Commutative Algebra

John Cremona
Notes by Florian Bouyer

Contents

Books: Introduction to Commutative Algebra by Atiyah and Macdonald. Commutative Algebra by Miles Reid.

1 Rings and Ideals

All rings R in this course will be commutative with a $1 = 1_R$.
We include the zero ring $0 = \{0\}$ with $1 = 0$. (in all other rings $1 \neq 0$)

Example. Algebraic geometry: $k[x_1, ..., x_n]$ with k a field. (The polynomial ring)
Number Theory: $\mathbb{Z}$, + rings of algebraic integers e.g. $\mathbb{Z}[i]$
Plus other rings from these by taking quotients, homomorphic images, localization,...

Ring homomorphisms: $R \to S$ (maps $1_R \mapsto 1_S$)

Subrings: $S \leq R$ ($\leq$ means subring) is a subset which is also a ring with the same operations and the same $1_S = 1_R$.

Ideals: $I \lhd R$: a subgroup such that $RI \subseteq I$

Quotient Ring: R/I the set of cosets of I in R $(x+I)$ with a natural multiplication $(x+I)(y+I) = xy + I$

Associated surjective homomorphism: $\pi : R \to R/I$ defined by $x \mapsto x + I$

1 to 1 correspondence: {ideals J of R with$J \geq I$} $\leftrightarrow$ {ideals $\tilde{J}$ of R/I} defined by $J \mapsto \tilde{J} = \pi(J) = \{x + I : x \in J\}$ and $\tilde{J} \mapsto J = \pi^{-1}(\tilde{J})$

More generally if $f : R \to S$ is a ring homomorphism then $\ker(f) = f^{-1}(0) \lhd R$ and $\operatorname{im}(f) = f(R) \leq S$ and $R/\ker(f) \cong \operatorname{im}(f)$ defined by $x + \ker(f) \mapsto f(x)$ and we have a bijection {ideals$J$ of $R, J \geq \ker(f)$} $\leftrightarrow$ {ideals $\widetilde{J}$ of $\operatorname{im}(f)$}.

Example. $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. $\ker(f) = n\mathbb{Z}, \operatorname{im}(f) = \mathbb{Z}/n\mathbb{Z}$. Ideal of $\mathbb{Z}/n\mathbb{Z}$ $\leftrightarrow$ideals of $\mathbb{Z}$,$\geq n\mathbb{Z}$ i.e. $m\mathbb{Z}/n\mathbb{Z}, m|n$

1.1 Special elements, special rings

Definition 1.1. $x \in R$ is a *zero-divisor* if $xy = 0$ for some $y \neq 0$

$x \in R$ is *nilpotent* if $x^n = 0$ for some $n \geq 1$ ($\Rightarrow x$ is a zero divisor except in 0 ring)

$x \in R$ is a *unit* if $xy = 1$ for some $y \in R$ (then y is uniquely determined by x and hence is denoted x^{-1})

The set of all units in R forms a group under multiplication and is called the *Unit Group.* Denoted $R^\times$ (or R^*)

R is an *integral domain* (or domain) if $R \neq 0$ and R has no zero divisors.

Principal ideals: Every element $x \in R$ generates an ideal $xR = (x) = \{xr : r \in R\}$. $(x) = R = (1) \iff x \in R^\times$. $(x) = \{0\} = (0) \iff x = 0$

A *field* is a ring in which every non-zero element is a unit. In a field k the only ideals are $(0) = \{0\}$ and $(1) = k$.

Example. $\mathbb{Z}, k[x_1, ..., x_n]$ are domains but not fields ($n \geq 1$).

$\mathbb{Q}, k(x_1, ..., x_n)$ are fields.

$$\mathbb{Z}/n\mathbb{Z} = \begin{cases} 0 & \text{if } n = 1 \\ \text{a field} & \text{if } n \text{ is prime} \\ \text{not a domain} & \text{if } n \text{ is not prime} \end{cases}$$

Definition 1.2. *Prime ideal:* $P \lhd R$ is prime if R/P is an integral domain. i.e. $P \neq R$ and $xy \in P \iff x \in P$ or $y \in P$

Maximal ideal: $M \lhd R$ is maximal if R/M is a field. i.e. $R \geq I \geq M \Rightarrow I = R$ or $I = M$

An ideal $I \lhd R$ is *proper* if $I \neq R$ ($\iff I$ does not contain $1 \iff I$ does not contain any units)

Every maximal ideal is prime, but not conversely in general.

Note. 0 (the 0 ideal) is prime $\iff R$ is a domain. 0 is maximal $\iff R$ is a field.

Example. $R = \mathbb{Z}$. 0 ideal is prime but not maximal. $p\mathbb{Z}$ (p is prime) is maximal.

If R is a PID (Principal Ideal Domain) then every non-zero prime is maximal:

Proof. $R \supseteq (y) \supseteq (x) = P \neq 0 \Rightarrow x = yz$ for some $z \in R$. P prime $\Rightarrow y \in P$ or $z \in P$. If $y \in P$ then $(y) = (x) = P$. On the other hand if $z \in P$ then $z = xt = ytz \Rightarrow z(1 - yt) = 0$, but $z \neq 0$ since $x \neq 0$ but R is a domain $\Rightarrow yt = 1 \Rightarrow (y) = R$ □

Definition 1.3. The set of all prime ideals of R is called the *spectrum* of R, written $\mathrm{Spec}(R)$

The set of all maximal ideals is $\mathrm{Max}(R)$ and is less important.

Let $f : R \to S$ be a ring homomorphism, and let P be a prime ideal of S then $f^{-1}(P)$ is a prime ideal of R. $R \xrightarrow{f} S \xrightarrow{\pi} S/P$ has kernel $f^{-1}(P)$ and S/P is a domain so $f^{-1}(P)$ is prime.
Alternatively: If $x, y \notin f^{-1}(P) \Rightarrow f(x), f(y) \notin P \Rightarrow f(xy) = f(x)f(y) \notin P \Rightarrow xy \notin f^{-1}(P)$.
Hence $f : R \to S$ induces a map $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ by $P \mapsto f^{-1}(P)$

e.g. If f is surjective we have a bijection between $\{\text{ideals of } R \geq \ker(f)\} \leftrightarrow \{\text{ideals of } S\}$ which restricts to $\mathrm{Spec}(R) \supseteq \{\text{primes ideals of } R \geq \ker(f)\} \leftrightarrow \{\text{prime ideals } S\} = \mathrm{Spec}(S)$ with $P \mapsto f^*(P)$. So f^* is injective

Example. If $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is the inclusion. $0 \in \mathrm{Max}(\mathbb{Q})$ but $f^{-1}(0) = 0 \notin \mathrm{Max}(Z)$

$\mathrm{Spec}(\mathbb{Z}) = \{0\} \cup \{p\mathbb{Z} : p \text{ prime}\}$,

$\mathrm{Spec}(\mathbb{Q}) = \{0\} = \mathrm{Spec}(k)$ for any field k

$\mathrm{Spec}\,\mathbb{C}[x]\,' =' \underset{0\,\text{ideal}}{\{\infty\}} \cup \underset{a \in \mathbb{C} \to (X-a)}{\mathbb{C}} = \mathbb{P}^1(\mathbb{C})$

$\mathrm{Spec}\,\mathbb{C}[x, y]\,' =' \underset{0}{\{\infty\}} \cup \underset{\text{e.g. lines } X+Y=0}{\{\text{irreducible curves in } \mathbb{C}^2\}} \cup \underset{(a,b) \leftrightarrow (X-a, X-b) = \{f : f(a,b) = 0\}}{\mathbb{C}^2}$

Theorem 1.4. *Every non-zero ring has a maximal ideal*

Proof. Uses Zorn's Lemma:

Lemma. *Let $S, \leq$ be a partially ordered set (so $\leq$ is transitive and antisymmetric $x \leq y$ and $y \leq x \iff x = y$)*

If S has the property that every totally ordered subset $T \subseteq S$ has an upper bound in S, then S has a maximal element.

We apply this to the set of all proper ideals in R. Let T be a totally ordered set of proper ideals of R. Set $I = \bigcup_{J \in T} J$. Claim: $I \lhd R$, $I \neq R$ then I is an upper bound for the set T so Zorn $\Rightarrow \exists$ maximal proper ideal.

1. Let $x \in I$, $r \in R \Rightarrow x \in J$ for some $J \in T \Rightarrow rx \in J \subseteq I \Rightarrow rx \in I$
2. Let $x, y \in I$ then $x \in J_1$ and $y \in J_2$. Either $J_1 \subseteq J_2 \Rightarrow x, y \in J_2 \Rightarrow x + y \in J_2 \subseteq I$ or similarly $J_2 \subseteq J_1$.

Notice that $1 \notin J \,\forall J$ hence $1 \notin \cup J$ so I is a proper ideal of R □

The same proof can be used to show

Corollary 1.5. *Every proper ideal I is contained in a maximal ideal (Apply theorem to R/I)*

Corollary 1.6. *Every non-unit of R is contained in a maximal ideal (can use corollary 1.5)*

Definition 1.7. A *local ring* is one with exactly one maximal ideal (it may have other prime ideals!)

Example. p prime number $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\} \underset{\geq \mathbb{Z}}{\leq} \mathbb{Q}$ has unique maximal ideal $p\mathbb{Z}_{(p)}$ with $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \equiv \mathbb{Z}/p\mathbb{Z} = \{\frac{a}{b} : p \mid a, p \nmid b\}$. $\mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)} = \{\frac{a}{b} : p \nmid a, p \nmid b\} =$ set of units in $\mathbb{Z}_{(p)}$ In general in a local ring R with maximal ideal M the set of units $R^\times = R \setminus M$. Note that (0) is a prime ideal of $\mathbb{Z}_{(p)}$

k field, $R = k[[x]] = \{\text{power series in } X \text{ with coefficients in } k\} = \{f = \sum_{i=1}^{\infty} a_i x^i : a_i \in k\}$. Can check f is a unit $\iff a_0 \neq 0$. f is not a unit $\iff a_0 = 0 \iff f \in (x) \Rightarrow (x) = M$ is the unique maximal ideal.

1.2 Two radicals: The nilradical $N(R)$ and the Jacobson radical $J(R)$

Definition 1.8. $N(R) = \{x \in R : x \text{ is nilpotent}\}$

Proposition 1.9.

1. $N(R) \lhd R$
2. $N(R/N(R)) = 0$

Proof.

1. (a) Let $x \in N(R), r \in R$. So $x^n = 0$ for some $n \geq 1 \Rightarrow (rx)^n = r^n x^n = 0 \Rightarrow rx \in N(R)$.

   (b) $x^n = 0$, $y^m = 0$ $(m, n \geq 1) \Rightarrow (x+y)^{m+n+1} = 0$, $cx^i y^j = 0$ since $i + j = m + n + 1 \Rightarrow$ either $i \geq n$ or $j \geq m$

2. Need to show that $R/N(R)$ has no non-zero nilpotents.

$$x^n + N(R) = (x + N(R))^n = 0 = 0 + N(R) \text{ (in } R/N(R))$$

$$\begin{aligned} &\Rightarrow \quad x^n \in N(R) \\ &\Rightarrow \quad (x^n)^m = 0 \\ &\Rightarrow \quad x^{mn} = 0 \\ &\Rightarrow \quad x \in N(R) \\ &\Rightarrow \quad x + N(R) = 0 \text{ in } R/N(R) \end{aligned}$$

□

Proposition 1.10. *$N(R)$ is the intersection of all the prime ideals of R*

Proof. Let $x \in N(R)$ so $x^n = 0$ but since $0 \in P \, \forall P \in \operatorname{Spec} R$ hence $x^n \in P \, \forall P \in \operatorname{Spec} R \Rightarrow x \in P$ since P is prime $\Rightarrow x \in \bigcap_{P \in \operatorname{Spec} R} P$

For the other way we use the contrapositive. Let $x \notin N(R)$. So $x, x^2, x^3, \ldots$ are all non-zero. Consider all ideals I which contain no power of x e.g. 0. In this collection there is a maximal element say P. Then $P \lhd R$ and $x \notin P$. We need to show that P is prime. Let $y, z \notin P$, then $P + (y) \supsetneq P$ and $P + (z) \supsetneq P$. By maximality of P each of $P + (y), P + (z)$ contains a power of x. Say $(p_1, P_2 \in P, y', z' \in R)$

$$\begin{aligned} x^n &= p_1 + yy' \\ x^m &= p_2 + zz' \\ &\Rightarrow \quad x^{m+n} = \underbrace{p_1p_2 + p_1zz' + p_2yy'}_{\in P} + yz(y'z') \\ &\Rightarrow \quad x^{m+n} \in P + (yz) \\ &\Rightarrow \quad P + (yz) \neq P \\ &\Rightarrow \quad yz \notin P \end{aligned}$$

□

Definition 1.11. $J(R) =$ intersection of all maximal ideals of R. $N(R) \subseteq J(R)$ (since maximals are primes)

Proposition 1.12. $x \in J(R) \iff 1 - xy \in R^\times \, \forall y \in R.$

Proof. " $\Rightarrow$ ": If $1 - xy \notin R^\times$ then $1 - xy \in M$ for some ideal maximal ideal $M \Rightarrow x \notin M$ (else $1 \in M$ contradicting maximality of M) $\Rightarrow x \notin J(R)$

" $\Leftarrow$ ":

$$\begin{aligned} x \notin J(R) &\Rightarrow x \notin M \text{ for some } M \\ &\Rightarrow M + (x) = R \\ &\Rightarrow 1 = m + xy\,(m \in M, y \in R) \\ &\Rightarrow 1 - xy = m \notin R^\times \end{aligned}$$

□

Example. $R = A\,[[x]]$ (A is a ring). $R^\times = \{\sum_{i=0}^\infty a_i x^i : a_0 \in A^\times\}$ (Exercise).
$\Rightarrow x \in J(R)$ since $1 - xf \in R^\times\ \forall x \in R$.

1.3 New ideals from old

Sum If $I, J \lhd R$ then $I + J = \{x + y : x \in I, y \in J\} \lhd R$. (The smallest ideal $\supseteq$ both I and J)

Intersection $I \cap J \lhd R$ (The largest ideal $\subseteq$ both I and J)

Product $IJ =$ ideal generated by all xy with $x \in I, y \in J = \{\sum_{i=1}^n x_i y_i : x_i \in I, y_i \in J\}$. $IJ \subseteq I \cap J$, equality does not hold in general.

Powers: I^n =ideal generated by all product $x_1 x_2 \dots x_n$ $(x_i \in I)$

Example. $R = \mathbb{Z}$.

- $(m) + (n) = (d)$ where $d = \gcd(m, n)$
- $(m) \cap (n) = (l)$ where $l = \operatorname{lcm}(m, n)$
- $(m)(n) = (mn)$
- $(m)^k = (m^k)$

$R = k[x_1, \dots, x_n]$. Let $M = (x_1, x_2, \dots, x_n) = (x_1) + (x_2) + \dots + (x_n)$. ($M = \ker(\phi : R \to k)$ where $\phi(f) = f(0, 0, \dots, 0)$) $R/M \cong k$
$M^2 = (\dots, x_i x_j, \dots) = \{$polynomials with 0 constant terms and 0 linear terms$\}$

These operation are commutative and associative, not all distributive.

- $I(J + K) = IJ + IK$

  Proof. Each side is generated by xy, xz for $x \in I, y \in J, z \in K$ □

- If $I + J = (1)$ then $I \cap J = IJ$

  Proof. Take $(I+J)(I\cap J) = I(I\cap J)+J(I\cap J) \subseteq IJ+JI = IJ$ so $I+J = (1)$ then $I\cap J \subseteq IJ$ □

Definition 1.13. I and J are *coprime/comaximal/relatively prime* if and only if $I + J = (1) \iff x + y = 1$ for some $x \in I, y \in J$.

Example. For $R = \mathbb{Q}[x, y]$ we have $(x)+(y) = (x, y) = \{$elements $f \in R$ such that $f(0, 0) = 0\} \neq (1)$. So (x) and (y) are distinct prime ideals but they are not coprime.

Lemma 1.14. *If I and J are coprime then I^m and J^n are coprime for any $n, m \geq 1$.*

Proof. $x + y = 1$ for certain $x \in I, y \in J$. Consider $1 = (x + y)^{m+n-1} \in I^m + J^n$ hence I^m and J^n are coprime. □

Chinese Remainder Theorem. *If $I_1, \dots, I_n$ are pairwise coprime ideals of R then*

$$\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$$

$$R/\prod_{i=1}^{n} I_i = \prod_{i=1}^{n}(R/I_i)$$

Proof. The first equation is true for $n = 2$. We are going to use induction so assume $n > 2$ and the statement is true for $n-1$. Let $J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$ by the induction hypothesis. We have $I_i + I_n = (1)$ for all $i = 1, \dots, n-1$. So take $x_i + y_i = 1$ for some $x_i \in I_i$ and $y_i \in I_n$ then $\underbrace{\prod_{i=1}^{n-1} x_i}_{\in J} = \prod_{i=1}^{n-1}(1-y_i) \equiv 1 \mod I_n$ so $J + I_n = (1)$. Hence $\prod_{i=1}^{n} I_i = JI_n = J \cap I_n = \bigcap_{i=1}^{n} I_i$

Define $\varphi : R \to \prod_{i=1}^{n} R/I_i$ by $x \mapsto (x + I_1, x + I_2, ..., x + I_n)$. Kernel is $\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$, now we just need to show surjectivity. The element $\prod_{i=1}^{n-1} x_i$ maps to $(0, \dots, 0, 1)$ (the x_i are taken from the first paragraph). By symmetry all "unit vectors" of $\prod(R/I_i)$ are in the image hence φ is surjective. Then we use the first isomorphism theorem to get $R/\prod I_i \to \prod(R/I_i)$ □

If ideals are not coprime, still get a ring homomorphism$R/\left(\bigcap_{i=1}^{n} I_i\right) \hookrightarrow \prod(R/I_i)$ but not surjective.

Proposition 1.15.

1. *If $I \subseteq \bigcup_{i=1}^{n} P_i$ with P_i prime, then $I \subseteq P_i$ for some i*
2. *If $P \supseteq \bigcap_{i=1}^{n} I_i$ and P is prime, then $P \supseteq I_i$ for some i*
3. *2. is also true with "="*

Proof.

1. We prove by induction if $I \nsubseteq P_i$ for all i then $I \nsubseteq \bigcup_{i=1}^{n} P_i$. In the case $n = 1$ it is obvious. So suppose $n > 1$ and the statement is true for $n-1$. Suppose $I \nsubseteq P_i \forall i$. Then by induction $I \nsubseteq \bigcup_{j \neq i} P_j$ hence $\exists x_i \in I$ such that $x_i \notin \bigcup_{j \neq i} P_j$ so for all $j \neq i$ we have $x_i \notin P_j$. If for some i we have $x_i \notin P_i$ then $x_i \in I \setminus \bigcup_{j=1}^{n} P_j$ and we are done. So assume $x_i \in P_i$ for all i. Let $y = \sum_{i=1}^{n} x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n \in I$. The ith term is in P_j for all $j \neq i$ but not in P_i. Given j we see that all but the jth term are in P_j so $y \notin P_j$, hence $y \notin \bigcup_{j=1}^{n} P_j$
2. Suppose $P \nsupseteq I_i \forall i$, then $\exists x_i \in I_i \setminus P$ for every i. Then $\prod x_i \in (\bigcap I_i) \setminus P$
3. If $P = \bigcap I_i$ then $P \supseteq I_i$ for some i by part 2 and $P = \bigcap I_i \subseteq I_i$ hence $P = I_i$

□

1.4 Quotients and radicals

Definition 1.16. Let I, J be ideals, define the *quotient* $(I : J) = \{x \in R \mid xJ \subseteq I\}$ (This is an ideal, but not exactly the same as in algebraic number theory)

Special case: $(0 : J) =$*annihilator of* $J = Ann(J)$

Example. IF $R = \mathbb{Z}$, $((15) : (6)) = (5)$. More generally if $m = \prod p_i^{ei}$ and $n = \prod p_i^{f_i}$ then $((m) : (n)) = (a)$ where $a = \prod p_i^{\max\{e_i - f_i, 0\}}$.

Fact.

1. *$I \subseteq (I : J)$ (since $IJ \subseteq I$)*
2. *$(I : J)J \subseteq I$*
3. *$((I : J) : K) = (I : JK) = ((I : K) : J)$*
4. *$(\bigcap I_i : J) = \bigcap (I_i : J)$*
5. *$(I : \sum J_i) = \bigcap(I : J_i)$*

Definition 1.17. Let I be an ideal, define the *radical* of I to be $r(I) := \{x \in R | x^n \in I \text{ for some } n \geq 1\}$

Special case: $r(0) = N(R)$

Given I, let $\varphi : R \to R/I$. Then $\varphi^{-1}(N(R/I)) = \{x \in R : \varphi(x)^n = 0 \text{ for some } n\} = r(I)$. Hence $r(I)$ is an ideal.

Example. $R = \mathbb{Z}$. If $m = \prod p_i^{k_i}, k_i \geq 1$ then $r((m)) = (\prod p_i)$

Fact.
1. *If $I \subseteq J$ then $r(I) \subseteq r(J)$.*
2. *$r(I) \supseteq I$ (take $n = 1$ in the definition)*
3. *$r(r(I)) = r(I)$ ($(x^m)^n = x^{mn}$)*
4. *$r(IJ) = r(I \cap J) = r(I) \cap r(J)$*
5. *$r(I) = (1) \iff I = (1)$ (use $1 \in r(I)$)*
6. *$r(I + J) = r(r(I) + r(J))$*
7. *$r(P^n) = P$ where P is a prime ideal and $n \geq 1$*
8. *$r(I) = \bigcap_{\substack{P \supseteq I \\ P \text{ prime}}} P$*

Proposition 1.18. *I, J are coprime if and only if $r(I), r(J)$ are coprime if and only if I^m, J^n are coprime for every/any $m, n \geq 1$*

Proof. I and J coprime then I^m, J^n coprime for all m, n was lemma 1.14 . If $\forall m, n$ I^m, J^n are coprime $\Rightarrow \exists m, n$ I^m, J^n are coprime is trivial.If $\exists m, n \geq 1$ such that I^m, J^n are coprime then $I + J \supseteq I^m + J^n = (1)$ hence $I + J = (1)$ (i.e they are coprime)

We now just need to prove I, J coprime $\iff r(I), r(J)$ are coprime

"$\Rightarrow$" obvious because $r(I) + r(J) \supseteq I + J = (1)$, so $r(I) + r(J) = (1)$

"$\Leftarrow$" $r(I + J) = r(r(I) + r(J)) = r((1)) = (1)$ hence by fact 5. we have $I + J = (1)$ □

1.5 Extension and Contractions

Definition 1.19. Let $f : R \to S$ be a ring homomorphism. For $I \lhd R$, let the *extension* of I, I^e be the ideal generated by $\{f(x) \in S \mid x \in I\}$. So $I^e = \{\sum_{\text{finite}} s_i f(x_i) \mid s_i \in S, x_i \in I\}$

For $J \lhd S$, let the *contraction* of J, $J^c = f^{-1}(J) \subseteq R$ (this is an ideal)

Example. If $R \hookrightarrow S$ then $J^c = J \cap R, I^e = \{\sum s_i x_i \mid s_i \in S, x_i \in I\} =$ the S-ideal generated by I

Fact. *If P is a prime ideal of S then P^c is a prime ideal of R (seen). This is not true for extensions:*

Example. $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. If we take $(5)^e = 5\mathbb{Z}[i] = (2 + i)(2 - i)\mathbb{Z}[i]$ is not a prime ideal.

Proposition 1.20. *Let $I \lhd R$ and $J \lhd S$*

1. *$I \subseteq I^{ec}$ (since $x \in f^{-1}(f(x))$)*
2. *$J \supseteq J^{ce}$ (easy)*
3. *$I^e = I^{ece}$ and $J^c = J^{cec}$*
4. *Let C = set of contracted ideals in R and E = set of extended ideals in S. Then $C = \{I \lhd R | I = I^{ec}\}$, $E = \{J \lhd S | J = J^{ce}\}$ and there is a bijection $C \to E$ given by e whose inverse is c.*

Proof. 1 and 2 are easy. For 3 we have $I^e \supseteq I^{ece}$ by 2 applied to $J = I^e$ but by 1 we have $I \subseteq I^{ec}$ and apply extension hence $I^e \subseteq I^{ece}$. 4 is easy to prove using 3 □

Example. Counter example to reverse inclusion of 1. $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $(2)^{ec} = \mathbb{Q}^c = \mathbb{Z} = (1) \neq (2)$

Theorem 1.21. *Let $f : R \to S$ be a ring homomorphism and $I \to I^e$ and $J \to J^c$ be the extension and contraction maps. Then*

- *Extension:*
  1. *$(I_1 + I_2)^e = I_1^e + I_2^e$*

2. $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$
3. $(I_1 I_2)^e = I_1^e I_2^e$
4. $(I_1 : I_2)^e \subseteq I_1^e : I_2^e$
5. $r(I)^e \subseteq r(I^e)$

- *Contraction:*

1. $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$
2. $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$
3. $(J_1 J_2)^c \supseteq J_1^c J_2^c$
4. $(J_1 : J_2)^c \subseteq J_1^c : J_2^c$
5. $r(J)^c = r(J^c)$

Proof. None of these is too hard to show □

Example. Counter example to show cases where equality does not hold

- Contraction 1: Take $f : k \hookrightarrow k[x]$ (with k any field), $J_1 = (x)$ and $J_2 = (x+1)$. Then $J_1^c = J_2^c = (0)$ but $J_1 + J_2 = (1)$ which contracts to (1).
- Extension 2: Take $f : \mathbb{Z}[x] \to \mathbb{Z}$ to be the "evaluation homomorphism" which maps $x \mapsto 2$. Let $I_1 = (x)$ and $I_2 = (2)$ then $I_1 \cap I_2 = (2x)$ so $(I_1 \cap I_2)^e = (2x)^e = 4\mathbb{Z}$ while $I_1^e = I_2^e = 2\mathbb{Z}$ so $I_1^e \cap I_2^e = 2\mathbb{Z}$
- Contraction 3: Take $f : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, $J_1 = (2+i), J_2 = (2-i)$. Then $J_1^c = J_2^c = (J_1 J_2)^c = (5)$
- Extension 4: Take $f : \mathbb{Z}[x] \to \mathbb{Z}$ to be the "evaluation homomorphism" which maps $x \mapsto 2$. Let $I_1 = (x)$ and $I_2 = (2)$ then $(I_1 : I_2) = I_1$ (since $x|2f \iff x|f$) so $(I_1 : I_2)^e = (x)^e = 2\mathbb{Z}$ while $I_1^e = I_2^e = 2\mathbb{Z}$ with quotient $\mathbb{Z}$
- Contraction 4: Take $f : \mathbb{Z} \hookrightarrow \mathbb{Z}[i], J_1 = (2+i), J_2 = (2-i)$. Then $J_1^c = J_2^c = (5)$ so $(J_1^c : J_2^c) = \mathbb{Z}$ but $(J_1 : J_2) = J_1$ which contracts to (5).
- Extension 5: Take $f : \mathbb{Z} \hookrightarrow \mathbb{Z}[i], I = 2\mathbb{Z}$. Then $r(I)^e = (2\mathbb{Z})^e = 2\mathbb{Z}[i]$ while $r((2)^e) = r(2\mathbb{Z}[i]) = (1+i)\mathbb{Z}[i]$

From the theorem we can see that the set of extended ideals of S is closed under the sum and product, while the set of contracted ideals of R is closed under intersection and radical.

2 Modules

Definition 2.1. An *R-module* is an abelian group M with a scalar multiplication $\underset{(r,m)\mapsto rm}{R \times M \to M}$ satisfying

1. $(r_1 + r_2)m = r_1 m + r_2 m$
2. $r(m_1 + m_2) = rm_1 + rm_2$
3. $r_1(r_2 m) = (r_1 r_2)m$
4. $1_R m = m$

For each $r \in R$ the map $M \to M, m \mapsto rm$ is an endomorphism of M (by 2.) 1,3,4 says $R \to \mathrm{End}(M)$ is a ring homomorphism

Example.
1. R itself is an R-module. So are all ideals of R
2. If R is a field k then an R-module is a k-vector space
3. Every abelian group A is a $\mathbb{Z}$-module
4. A $k[x]$-module is $k$vector space V together with a k-linear map $V \to V$ given the scalar multiplication by x
5. Let G be a finite group (abelian). Let $R = k[G]$ the group algebra. Then a $k[G]$ module is a representation of G.

Definition 2.2. An R-module homomorphism $f : M \to N$ is a map $M \to N$ which satisfies

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$
2. $f(rm) = rf(m)$

Where M, N are both R-module. f is called *R-linear*

$\mathrm{Hom}_R(M, N) = \{\text{all } R\text{-linear map } f : M \to N\}$ is another R-module with point-wise operations

Example. $\mathrm{Hom}_R(R, M) \cong M$ by $f \leftrightarrow f(1_R)$ since $f(r) = f(r \cdot 1) = rf(1)$

Definition 2.3. $N \subseteq M$ is a *submodule* if it is closed under addition and scalar multiplication, (in particular $0 \in N$). We will use $N \leq M$ as notation.

Example. R-submodules of R are the ideals of R.

Definition 2.4. *Quotient Modules:* If $N \leq M$ then M/N is again an R-module via $r(x+N) = rx+N$ (well-defined since $rN \subseteq N$)

Kernels and Cokernels: If $f \in \mathrm{Hom}_R(M, N)$ then $\ker(f) \leq M$, $\mathrm{im}(f) \leq N$ and $\mathrm{coker}(f) = N/\mathrm{im}(f)$

So f is injective $\iff \ker(f) = 0$. f is surjective $\iff \mathrm{coker}(f) = 0 \iff \mathrm{im}(f) = N$

First Isomorphism Theorem. *If $f \in \mathrm{Hom}_R(M, N)$ then $M/\ker(f) \cong \mathrm{im}(f)$ via $m+\ker(f) \mapsto f(m)$*

Definition 2.5. *Sums of Submodules:* Let $M_i \leq M$ for $i \in I$. Then $\sum_{i\in I} M_i = \{\text{all finite sums } \sum_{i\in I} m_i \text{ with } m_i \in M_i\} \leq M$

Intersection of Submodules: Let $M_i \leq M$ for $i \in I$. Then $\bigcap_{i\in I} M_i \leq M$

Second Isomorphism Theorem. *Let $N \leq M \leq L$ be submodules of R. Then*

$$\frac{L/N}{M/N} \cong \frac{L}{M}$$

Proof. The map $L/N \to L/M$ defined by $x + N \mapsto x + M$ ($x \in L$) is surjective with kernel M/N, then use the first isomorphism theorem. □

Third Isomorphism Theorem. *Let $M_1, M_2 \leq M$ be R-modules. Then*

$$\frac{M_1 + M_2}{M_1} \cong \frac{M_2}{M_1 \bigcap M_2}$$

Proof. The map $M \to M_1 + M_2 \to (M_1 + M_2)/M_1$ defined by $y \mapsto 0 + y \mapsto y + M_1$is surjective with kernel $M_1 \bigcap M_2$. Then use the first isomorphism theorem. □

Definition 2.6. *Product of Ideal and Modules:* Let $I \lhd R$ and M a R-module. Define the product of I and M to be $IM = \{\sum_{i=1}^{n} a_i m_i | a_i \in I, m_i \in M\} \leq M$.

A special case $I = (r)$ we write $rM = \{rm | m \in M\} \leq M$

Quotient: Let M, N be R-module such that they both are submodules of L, we define the quotient to be $(M : N) = \{r \in R : rN \subseteq M\} \lhd R$

Special case: $M = 0$, $(0 : N) = \{r \in R : rN = 0\} = \operatorname{Ann}_R(N) \lhd R$

$M$is a *faithful* R-module if $\operatorname{Ann}_R M = 0$

If $I \subseteq \operatorname{Ann}_R M$ then M may be regarded as an R/I-module via $(r + I)m = rm$. In particular taking $I = \operatorname{Ann}_R M$ we may view M as a faithful $R/\operatorname{Ann}_R M$-module.

Example. If A is an abelian group (hence a $\mathbb{Z}$-module) which is *p-torsion* (meaning $pA = 0$ for some prime p) then A is $\mathbb{Z}/p\mathbb{Z}$-module, i.e., a vector space over $\mathbb{F}_p$.

Definition 2.7. *Cyclic Submodules:* $x \in M$ an R-module generates $(x) = Rx = \{rx | r \in R\} \leq M$ is *the cyclic submodule* generated by x. In particular if $M = Rx$ for some x then M is *cyclic* and $M \cong R/\operatorname{Ann}_R x$ (as R-modules)

Finitely Generated Module: We say M is *finitely generated* (f.g.) if $M = \sum_{i=1}^{n} Rx_i$ for some finite collection $x_1, \ldots, x_n \in M$. More generally $\{x_i\}_{i \in I}$ generates M if every $x \in M$ is a finite R-linear collection of the $x_i \in M$.

Example. $M = R[x]$ is generated by $1, x, x^2, x^3, \ldots$ but M is <u>not</u> finitely generated.

Definition 2.8. Let M, N be R-modules. We define:

Direct Sum: $M \oplus N = \{(m, n) : m \in M, n \in N\}$ is an R-module with coordinate operations.

Direct Product: $M \times N = \{(m, n) : m \in M, n \in N\}$ is an R-module with coordinate operations.

Similarly if M_i $(i = 1, \ldots, n)$ are R-modules we can form $\oplus_{i=1}^{n} M_i = \{(m_1, \ldots, m_n) | m_i \in M_i \, \forall i \leq n\} = \prod_{i=1}^{n} M_i$

Infinite Direct Sum: If we start with $\{M_i\}_{i \in I}$ we define $\oplus_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i \, \forall i,$all but finitely many $m_i = 0\}$

Infinite Direct Product: If we start with $\{M_i\}_{i \in I}$ we define $\prod_{i=I} M_i = \{(m_i)_{i \in I} : m_i \in M_i \, \forall i\}$

Example. As an R-module $R[x] \cong \oplus_{i=0}^{\infty} R$ where the isomorphism is defined by $\sum_{i=0}^{d} r_i x^i \mapsto (r_0, r_1, r_2, \ldots, r_d, 0, 0, \ldots)$
$R[[x]] \cong \prod_{i=0}^{\infty} R$ (as R-modules)

Definition 2.9. *Free Modules*: M is *free* if $M \cong \oplus_{i \in I} M_i$ where each $M_i \cong R$.

A *finitely generated free module* $M \cong \underbrace{R \oplus \cdots \oplus R}_{n} = R^n$

Lemma 2.10. *M is finitely generated if and only if $M \cong$ a quotient of R^n for some n*

Proof. "⇒": If $x_1, \ldots, x_n$ generates M then map $R^n \to M$ by $(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i x_i$ is surjective (since M is finitely generated) so $R^n/\ker \cong M$

"⇐": R^n is finitely generated by $(1, 0, \ldots 0), (0, 1, 0, \ldots, 0), \ldots$ So R^n/K is finitely generated by images of these in R^n/K □

Proposition 2.11. *Let M be a finitely generated R-module, $J \lhd R$ and $\varphi \in \operatorname{End}_R(M) = \operatorname{Hom}_R(M, M)$. Suppose that $\varphi(M) \subseteq JM$. Then $\exists a_1, a_2, \ldots, a_n \in J$ such that*

$$\varphi^n + a_1 \varphi^{n-1} + a_2 \varphi^{n-2} + \cdots + a_n I_M = 0$$

in $\operatorname{End}_R(M)$ and I_M is the identity map $M \to M$

Proof. Let $x_1, \dots, x_n$ generate M. $\forall i \le n, \varphi(x_i) = \sum_{j=1}^n a_j x_j$ where $a_j \in J$.

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij} I) x_i = 0$$

for $i = 1, \dots, n$ where $\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$. We can rewrite this as $(I\varphi - A)X = 0$ where $A = (a_{ij}), I = (\delta_{ij}), X = (x_1, \dots, x_n)^T$. Multiply by $\mathrm{adj}(I\varphi - A)$ whose entries are all in $\mathrm{End}_R(M) \Rightarrow \det(I\varphi - A)x_i = 0 \, \forall i \Rightarrow \det(I\varphi - A) = 0 \in \mathrm{End}_R(M)$. If we multiply out $\det(I\varphi - A)$ to get the equation above. □

Applications:

1. $x \in \mathbb{C}$. If M is a non-zero finitely generated $\mathbb{Q}$-submodule of $\mathbb{C}$ such that $xM \subseteq M$ then x is algebraic.

   Corollary 2.12. *The set of all algebraic numbers in $\mathbb{C}$ forms a field.*

2. $x \in \mathbb{C}, M \subseteq \mathbb{C}$ a non-zero finitely generated $\mathbb{Z}$-submodule such that $xM \subseteq M \Rightarrow x$ is an algebraic integer

   Corollary 2.13. *The set of algebraic integers in $\mathbb{C}$ is a ring.*

Proof Of Applications and Corollary. $\alpha \in \mathbb{C}$ is algebraic $\iff$ $\exists$monic $f \in \mathbb{Q}[x]$ such that $\deg f = n \ge 1$ and $f(\alpha) = 0 \iff \exists M \subseteq \mathbb{C}$ a finitely generated $\mathbb{Q}$-submodule of $\mathbb{C}$ with $\alpha M \subseteq M$. (For $\Rightarrow$: $M = \mathbb{Q}[\alpha] = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\alpha^2 + \cdots + \mathbb{Q}\alpha^{n-1}$)

$\alpha \in \mathbb{C}$ is an algebraic integer $\iff$ $\exists$ monic $f \in \mathbb{Z}[x]$, such that $\deg f = n \ge 1$ and $f(\alpha) = 0 \iff M \subset \mathbb{C}$ a finitely generated $\mathbb{Z}$-module with $\alpha M \subseteq M$ (Again for $\Rightarrow$: $M = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$)

Let $R = \mathbb{Q}$ or $\mathbb{Z}$ and let α, β be {algebraic numbers or algebraic integers respectively}, then $\alpha \pm \beta, \alpha\beta$ are also {algebraic numbers, algebraic integers}. Let the polynomial of α be $f(x), \deg f = n$ and of β be $g(x), \deg g = m$ with $f, g \in R[x]$ monic. Let M be the R-submodule of $\mathbb{C}$ generated by $\alpha^i\beta^j, 0 \le i \le n-1, 0 \le j \le m-1$, i.e., $M = \sum_{i,j} R\alpha^i\beta^j$. Clearly $\alpha M \subseteq M$ and $\beta M \subseteq M$. Then $(\alpha \pm \beta)M \subseteq M$ and $\alpha\beta M \subseteq M$ quite clearly hence $\alpha \pm \beta$ are {algebraic numbers, algebraic integers}. Hence both sets are subrings of $\mathbb{C}$. If α is an algebraic number $\alpha \neq 0$ then α^{-1} is also algebraic (easy) so {algebraic numbers} is a subfield of $\mathbb{C}$. □

Corollary 2.14. *If M is an finitely generated R-module and $J \lhd R$ such that $JM = M$ then $\exists r \in R$ such that $rM = 0$ and $r \equiv 1 \mod J$ (i.e., $r - 1 \in J$)*

Proof. Apply the proposition with $\varphi =$ identity map. So the proposition tells us $(1 + a_1 + \cdots + a_{n-1})M = 0$ with $a_i \in J$. So let $r = 1 + a_1 + \cdots + a_{n-1}$. □

Corollary 2.15 (Nakayama's Lemma)**.** *If M is a finitely generated R-module and $I \lhd R$ such that $I \subseteq J(R)$. If $IM = M$ then $M = 0$*

Proof. By Corollary 2.14 $\exists r \in R$ such that $rM = 0$ and $r - 1 \in I \Rightarrow r - 1 \in J(R)$ but this implies (by Proposition 1.12)$r \in R^*$ so $M = r^{-1}rM = 0$ □

Corollary 2.16. *Let M be finitely generated and $I \lhd R$ such that $I \subseteq J(R)$. Let $N \le M$. If $M = IM + N$ then $M = N$.*

Proof. Apply Corollary 2.15 to M/N (which is still finitely generated), using $I(M/N) = (IM + N)/N \, (*)$, since $M = IM + N \Rightarrow I(M/N) = M/N \Rightarrow M/N = 0 \Rightarrow M = N$. To check $(*)$ holds we use the map $\phi : IM + N \to I(M/N)$ defined by $am + n \mapsto a(m + N)$. ϕ is clearly surjective and has kernel $= N$ (hence use the first isomorphism theorem) □

Corollary 2.17. *Let M be a finitely generated R-module, where R is a local ring with (unique) maximal ideal P and residue field $k = R/P$. Then*

1. *M/PM is a finite dimensional vector space over k*

2. $x_1, \dots, x_n$ *generates* M *as an* R*-module* $\iff$ $\overline{x_1}, \dots, \overline{x_n}$ *generates* M/PM *as a* k*-vector space. (Here* $\overline{x} = x + PM \in M/PM$*)*

Proof. 1. M/PM is an R-module which is annihilated by P hence is a module over $R/P = k$.

2. "$\Rightarrow$": Clear. $\overline{x} \in M/PM \Rightarrow \exists x_i \in R$ such that $x = \sum_{i=1}^n r_i x_i \Rightarrow \overline{x} = \sum_{i=1}^n r_i \overline{x_i}$. (Note that this also proves the finite dimensional claim of part 1)
"$\Leftarrow$": Let $x_1, \dots, x_n \in M$ be such that $\overline{x_1}, \dots, \overline{x_n}$ generates M/PM. Set $M = \sum_{i=1}^n Rx_i \leq M$. We want to show $M = N$. We are going to use Corollary 2.16, noting that $J(R) = P$, with $I = P$. Then we can apply the Corollary if $M = PM + N$. Let $x \in M$, then $\overline{x} \in M/PM$ so $\exists r_i$ such that $\overline{x} = \sum r_i \overline{x_i}$ in $M/PM \Rightarrow x - \sum r_i x_i \in PM \Rightarrow x \in N + PM$

□

Example. $R = \mathbb{Z}_{(5)} = \{\frac{a}{b} \in \mathbb{Q} \mid 5 \nmid b\}$. This is a local ring with maximal ideal $P = 5R$. We can check that $R/P \cong \mathbb{Z}/5\mathbb{Z}$. Let $M = \mathbb{Q}$, but $P\mathbb{Q} = \mathbb{Q} \Rightarrow \mathbb{Q}/P\mathbb{Q}$ is 0 but $\mathbb{Q}$ is not finitely generated as an R-module. (see exercise)

2.1 Exact Sequences

Definition 2.18. Let L, M, N be R-module. A sequence $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ of R-module homomorphism is *exact* if $\text{im}(\alpha) = \ker(\beta)$.
Note: This implies $\beta \cdot \alpha = 0$ ($\iff$ $\text{im}(\alpha) \subseteq \ker(\beta)$)

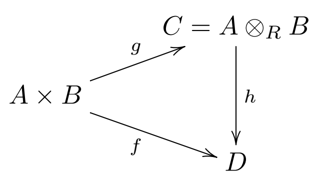
Example. Key Examples:

- $L \xrightarrow{\alpha} M \longrightarrow 0$ is exact $\iff \alpha$ is surjective
- $0 \longrightarrow M \xrightarrow{\alpha} N$ is exact $\iff \alpha$ is injective
- A longer sequence $\dots \longrightarrow M_{i-1} \xrightarrow{\alpha_{i-1}} M_i \xrightarrow{\alpha_i} M_{i+1} \xrightarrow{\alpha_{i+1}} \dots$ is exact $\iff$ $\ker(\alpha_i) = \text{im}(\alpha_{i-1}) \, \forall i$
- *Short Exact Sequence* $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ is exact $\iff$
  - α is injective ($L \hookrightarrow M$)
  - β is surjective (so $N \cong M/\ker\beta$)
  - $\text{im}(\alpha) = \ker(\beta)$
  - That is $L \cong \alpha(L) \leq M$ and $M/\alpha(L) \cong N$

2.2 Tensor products of modules

Let R be a ring. Given two R-modules, A, B we will define/construct an R-module $C = A \otimes_R B$ with the following properties

1. C is an R-module and there is an R-bilinear map $g : A \times B \to C$
2. (Universal property) For any R-bilinear map $f : A \times B \to D$ (with D any R-module) there is a *unique* R-linear map $h : C \to D$ such that $f = h \circ g$



These properties uniquely determine $A \otimes_R B$ up to unique isomorphism. This is because:

- Taking $D = C$ shows that $\text{id}_C : C \to C$ is the only map such that $g = \text{id}_C \circ g$

- If D also satisfies 1., 2. then $\exists h_1 : C \to D$ such that $f = h_1 \circ g$ and $\exists h_2 : D \to C$ such that $g = h_2 \circ f$. Then we see that $f = h_1 \circ h_2 \circ f \Rightarrow h_1 \circ h_2 = \mathrm{id}_D$ and $g = h_2 \circ h_1 \circ g \Rightarrow h_2 \circ h_1 = \mathrm{id}_C$

Existence:
We construct C as follows

- Take the free R-module F with $A \times B$ as generating set i.e. generators $(a, b) \,\forall a \in A, b \in B$. $F = \{\sum_{i=1}^{n} r_i(a_i, b_i) | r_i \in R, a_i \in A, b_i \in B\}$
- Factor out the submodule L consisting of all elements of the form $(r_1a_1 + r_2a_2, b) - r_1(a_1, b) - r_2(a_2, b)$ and $(a, r_1b_1 - r_2b_2) - r_1(a, b_1) - r_2(a, b_2) \,\forall r_1, r_2 \in R, a, a_1, a_2 \in A, b, b_1, b_2 \in B$
- Set $C = F/L$. Denote the image in F/L of (a, b) by $a \otimes b$. Then F/L is generated by $\{a \otimes b | a \in A, b \in B\}$ with "relations" $(r_1a_1 + r_2a_2) \otimes b = r_1(a_1 \otimes b) + r_2(a_2 \otimes b)$ and $a \otimes (r_1b_1 + r_2b_2) = r_1(a \otimes b_1) + r_2(a \otimes b_2)$ $(*)$

So each elements of $A \otimes_R B$ has the form $\sum_{i=1}^{n} r_i(a_i \otimes b_i)$. But (by $(*)$) we have $r(a \otimes b) = (ra) \otimes b = a \otimes (rb)$. Using this, every element of $A \otimes_R B$ is a finite sum of "atomic tensors" $a \otimes b$. Can we simplify these sums further? Not in general! e.g. $a_1 \otimes b_1 + a_2 \otimes b_2$ can not, in general, be rewritten as a single "atom" $a \otimes b$.

Example. If A, B are both cyclic R-modules, say $A = Rx, B = Ry$ then every $a \in A$ has the form $a = rx$ for some $r \in R$ and similarly every $b \in B$ has the form $b = sy$ for some $s \in R$. Then $a \otimes b = rx \otimes sy = rs(x \otimes y)$. A general element of $A \otimes_R B$ is thus a finite sum of $\sum_{i=1}^{n} t_i(x \otimes y) = t(x \otimes y)$ where $t = \sum_{i=1}^{n} t_i \in R$. Hence $A \otimes_R B$ is cyclic, generated by $x \otimes y$

Fact. *More generally if A, B are finitely generated by $x_1, \dots, x_n$ for A and $y_1, \dots, y_m$ for B. Then $(\sum r_i x_i) \otimes (\sum s_j y_j) = \sum_{i,j} (r_i s_j)(x_i \otimes y_j)$. Hence $A \otimes_R B$ is also finitely generated by $x_i \otimes y_j$*

Exercise. $R = k$ a field. $x_1, \dots, x_n$ a basis for A and $y_1, \dots, y_n$ a basis for B then the $x_i \otimes y_j$ are a basis for $A \otimes_k B$ and hence $\dim_k A \otimes_k B = mn = (\dim_k A)(\dim_k B)$

Similarly we can define $A \otimes_R B \otimes_R C$ for any three R-modules A, B, C and $A_1 \otimes_R A_2 \otimes_R \cdots \otimes_R A_n$ for any n R-modules $A_1, \dots, A_n$. We get nothing essentially new since $A \otimes_R B \otimes_R C$ turns out to be isomorphic to $(A \otimes_R B) \otimes_R C$ and to $A \otimes_R (B \otimes_R C)$

Lemma 2.19. *1.* $A \otimes_R B \cong B \otimes_R A$

2. $A \otimes_R R \cong A$

3. $(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C)$

Proof. 1. We have an R-bilinear map $A \times B \to B \otimes_R A$ via $(a, b) \mapsto b \otimes a$. (Since $(r_1a_1 + r_2a_2, b) \mapsto b \otimes (r_1a_1 + r_2a_2) = r_1(b \otimes a_1) + r_2(b \otimes a_2) \leftarrow r_1(a_1, b) + r_2(a_2, b)$). Hence there is a unique R-linear map $h_1 : A \otimes_R B \to B \otimes_R A$ with $a \otimes b \mapsto b \otimes a$. Similarly we get $h_2 : B \otimes_R A \to A \otimes_R B$ with $b \otimes a \mapsto a \otimes b$, hence $h_1 \circ h_2 = \mathrm{id}$ and $h_2 \circ h_1 = \mathrm{id}$

2. Define a map $A \times R \to A$ by $(a, r) \mapsto ra$. It is surjective (take $r = 1$) and R-bilinear, hence induces a map $f : A \otimes_R R \to A$ with $a \otimes r \mapsto ra$ surjective. Define $g : A \to A \otimes_R R$ by $g(a) = a \otimes 1 \in A \otimes_R R$. We can easily check that $f \circ g = \mathrm{id}_A$ and $g \circ f = \mathrm{id}_{A \otimes_R R}$.

3. Exercise

□

Definition 2.20. *Tensoring maps* (i.e., R-module homomorphism): Let $f : A_1 \to A_2, g : B_1 \to B_2$ be R-linear maps where A_1, A_2, B_1, B_2 are R-modules. Then there is an R-linear map $f \otimes g : A_1 \otimes_R B_1 \to A_2 \otimes_R B_2$ which sends $a \otimes b \mapsto f(a) \otimes g(b)$. This is induced by the R-bilinear map $A_1 \times B_1 \to A_2 \otimes_R B_2$ which sends $(a_1, b_1) \mapsto f(a_1) \otimes g(b_1)$

2.3 Restriction and Extension of Scalars

Or: How we usually think about tensor products Let $f : R \to S$ be a ring homomorphism. Then every S-module becomes an R-module via $rx = f(r)x$.

Example. Special Cases:

1. S is an R-module ($rs = f(r)s$)
2. R a subring of S and f the inclusion map $R \hookrightarrow S$. Then every S-module is an R-module too.

   Example. If K, L are fields with $K \subset L$ (i.e., L is an extension of K) then L-vector space is a K-vector space. (Restriction of scalars). In particular L is a vector space over K. $\dim_K L$ is the *degree* of the extension ($\leq \infty$).

   Standard Fact: If $L \supset K \supset F$ (fields) and L is a finite extension of K and K is finite over F then L is finite over F.

Proposition 2.21. *Let $f : R \to S$ be as above. If M is a finitely generated S-module and S is a finitely generated R-module then M is a finitely generated R-module.*

Proof. Straightforward □

We are now going to try to go the other way. Let $f : R \to S$ and M be an R-module. Let $M_S = S \otimes_R M$, this is an R-module. It can be made into an S-module via $s'(s \otimes m) = (s's) \otimes m$. (The R-module structure of M_S can be done in two ways $r(s \otimes m) = (f(r)s) \otimes m = s \otimes rm$). If $R = S$ and $f = \mathrm{id}$ we just get $R \otimes_R M \cong M$ $(= M_R)$

Definition 2.22. We say that M_S is obtained from M by *extension of scalars*

Remark. If $\{x_i\}_{i \in I}$ generates M as an R-module then $\{1 \otimes x_i\}_{i \in I}$ generates M_S as an S-module. i.e., $M = \sum_{i \in I} Rx_i \Rightarrow M_S = \sum_{i \in I} S(1 \otimes x_i)$. By abuse of notation we often just write $M_S = \sum_{i \in I} Sx_i$ where $\sum s_i x_i$ is shorthand for $\sum s_i \otimes x_i$.

Example.

1. $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}$. $\mathbb{Q}(i)$ is generated as $\mathbb{Q}$-module by $1, i$ hence $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R}$ is generated as an $\mathbb{R}$-module by $1 \otimes 1, i \otimes 1$. And we abbreviate $x(1 \otimes 1) + y(1 \otimes i)$ as $x + yi$ where $x, y \in \mathbb{R}$.
2. Let R and S be two ring with $f : R \to S$ is the "structure map" giving S the structure of an R-module. Then $R[x] \otimes_R S \cong S[x]$. Strictly: elements of the left side are polynomials in $x \otimes 1$
3. $R^n \otimes_R S \cong S^n$. If $e_1, \dots, e_n$are the "standard" generators $(1, 0, \dots, 0), \dots, (0, \dots 0, 1)$ for R^n then $R^n \otimes_R S$ is freely generated by $e_i \otimes 1$.

2.4 Algebras

Definition 2.23.

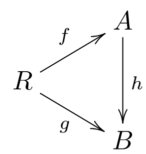
1. Let R be a ring. An *R-algebra* is a ring A with a ring homomorphism $f : R \to A$, which turns A into an R-module. (via $ra = f(r)a$)
2. Conversely if A is both a ring and an R-module ($(r, a) \mapsto r \cdot a$)then it is an R-algebra if the two structures of A are compatible, i.e.:
   - $(r_1 + r_2) \cdot a = r_1 \cdot a + r_2 \cdot a$
   - $r_1(r_2 \cdot a) = (r_1 r_2) \cdot a$
   - $1 \cdot a = a$
   - $r \cdot (a_1 a_2) = (r \cdot a_1)a_2 = a_1 \cdot (ra_2)$

We recover the structure map $f : R \to A$ by setting $f(r) = r \cdot 1_A \in A$.

To go from one definition to the other: $1 \Rightarrow 2$: Define $r \cdot a = f(r)a$ (show that this satisfy the axiom given).

$2 \Rightarrow 1$: Define $f(r) = r \cdot 1_a \in A$ (Show that this does give a ring homomorphism)

Definition 2.24. Let A, B be R-algebra with structure maps $f : R \to A, g : R \to B$. Then an *R-algebra homomorphism* from $A \to B$ is a map $h : A \to B$ which is both a ring homomorphism and R-linear such that $g = h \circ f$



$$
\begin{aligned}
h(a_1 + a_2) &= h(a_1) + h(a_2) \\
h(ra) &= rh(a) \, \forall a \in A, r \in R \\
&\iff h(f(r)a) = g(r)h(a) \\
&\iff h(f(r))h(a) = g(r)h(a) \\
&\iff h(f(r)) = g(r) \\
&\iff h \circ f = g
\end{aligned}
$$

What we have proved: A ring homomorphism $h : A \to B$ is an R-module homomorphism $\iff$ $h \circ f = g$

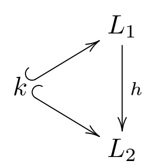
Special Cases:

1. $R = k$ a field, $A \neq 0$ then the structure map $f : k \to A$ must be injective ($f(1_k) = 1_A$ so $f \neq 0$). So A is a ring with k as a subring.

   Example. $A = k[X]$ is a k-algebra, $\mathbb{C}$ is an $\mathbb{R}$-algebra (and a $\mathbb{Q}$-algebra)

2. $R = \mathbb{Z}$. Any ring A is a $\mathbb{Z}$-algebra whose structure map is the unique ring homomorphism $\mathbb{Z} \to A$, $n \mapsto n \cdot 1_A = \underbrace{1 + 1 + \cdots + 1}_{n>0}$

3. k a field. Extension fields of k are k-algebra. If $k \subset L_1, k \subset L_2$ (L_1, L_2 are fields). Then a map $h : L_1 \to L_2$ is a k-algebra homomorphism if it is a ring homomorphism (necessarily injective) such that $h(x) = x \, \forall x \in k$.



2.5 Finite conditions

Let A be an R-algebra.

Definition 2.25. A is a *finite* R-algebra if it is finitely generated as an R-module, i.e., $\exists a_1, \ldots, a_2 \in A$ such that $A = Ra_1 + \cdots + Ra_n$

A is a *finitely generated* R-algebra if there is a surjective ring homomorphism $R[x_1, \ldots x_n] \to A$ for some n defined by $x_i \mapsto a_i$. Denote this by $A = R[a_1, \ldots, a_n]$. Hence every element of A is a polynomial in the finite set $a_1, \ldots, a_n$

Example. $A = R[x]$ is a finitely generated R-algebra (generator $= x$), but it is not a finite R-algebra since it is not finitely generated as an R-module. (it is generated by $1, x, x^2, \ldots$ but not by any finite set of polynomials)

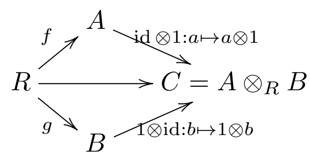
If $\alpha \in \mathbb{C}$ then $\mathbb{Q}[\alpha]$ is a finitely generated $\mathbb{Q}$-algebra, and is a finite $\mathbb{Q}$-algebra $\iff$ α is an algebraic number.

$A = \mathbb{Z}[\alpha]$ is finitely generated $\mathbb{Z}$-algebra, and is a finite $\mathbb{Z}$-algebra $\iff$ α is an algebraic integer.

2.6 Tensoring Algebras

Let A, B be R-algebras with structure maps $f : R \to A, g : R \to B$. The R-module $C = A \otimes_R B$ may be turned into a ring and hence an R-algebra by setting $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$. (extended by linearity)

Proof that this is well defined and turns $A \otimes_R B$ into a ring. Map $A\times B\times A\times B \to C$ by $(a_1, b_1, a_2, b_2) \mapsto a_1a_2 \otimes b_1b_2$. This is clearly R-multilinear and hence induces an R-linear map from $(A \otimes_R B) \otimes_R (A \otimes_R B) \to C$, i.e, $C \otimes_R C \to C$ is a well defined map, which in turns gives our multiplication. $1_C = 1_A \otimes 1_B$ and $0_C = 0_A \otimes 0_B$. Checking C is a ring is straightforward. The structure map $R \to C$ is $r \mapsto r \cdot (1 \otimes 1) = 1 \otimes g(r) = f(r) \otimes 1$



□

3 Localization

Rings and Modules of Quotients Recall: If R is an integral domain then we construct its field of fractions as follows: take the set of ordered pairs $(r,s), r \in R, s \in R \setminus \{0\}$ with equivalence relation $(r_1,s_1) \sim (r_2,s_2) \iff r_1s_2 = r_2s_1$. Denote the class of (r,s) by $\frac{r}{s}$. Define ring operations by via the usual formulas $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2+r_2s_1}{s_1s_2}$. Lots of checking of well-defined-ness and axioms shows that this is a field K. $0 = \frac{0}{1}, 1 = \frac{1}{1}, \frac{r}{s} = 0 \iff r = 0$ so we get $R \hookrightarrow K$ by $r \mapsto \frac{r}{1}$, so if $\frac{r}{s} \neq 0 \Rightarrow \frac{s}{r} \in K$ and $\frac{r}{s}\frac{s}{r} = \frac{1}{1}$

Definition 3.1. A *multiplicatively closed set* (MCS) in a ring R is a subset S of$R$ such that:

1. $1 \in S$
2. $s_1, s_2 \in S \Rightarrow s_1s_2 \in S$

   We'll often assume $0 \notin S$

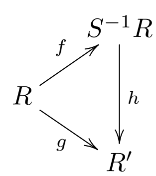
Example. If R is an integral domain, $S = R \setminus \{0\}$.
R any ring, P prime ideal of R, $S = R \setminus P$

Given a MCS S take the set of pairs $R \times S$ with the relation: $(r_1,s_1) \sim (r_2,s_2) \iff \exists s \in S$ such that $s(r_1s_2 - r_2s_1) = 0$. This is an equivalence relation: Reflexivity and Symmetry are trivial. For Transitivity: $(r_1,s_2) \sim (r_2,s_2)$ and $(r_2,s_2) \sim (r_3,s_3) \Rightarrow \exists s,t \in S$ such that $s(r_1s_2 - r_2s_1) = 0, t(r_2s_3 - r_3s_2) = 0 \Rightarrow s_2st(r_1s_3 - r_3s_1) = sts_1r_2s_3 - sts_3r_2s_1 = 0$.

Let $S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\}$ where $\frac{r}{s}$ is the equivalence class of (r,s). So $\frac{r_1}{s_1} = \frac{r_2}{s_2} \iff s(r_1s_2 - r_2s_1) = 0$ for some $s \in S$. This forms a ring under the usual addition and multiplication of fractions. (Check ring axioms + well-defined-ness). $0_{S^{-1}R} = \frac{0}{1}$, $1_{S^{-1}R} = \frac{1}{1}$ and we have a ring homomorphism $f : R \to S^{-1}R$ defined by $r \mapsto \frac{r}{1}$ which is not injective in general. $\frac{r_1}{1} = \frac{r_2}{1} \iff \exists s \in S$ such that $s(r_1 - r_2) = 0$, i.e., $r_1 - r_2 \in \{r \in R : rs = 0 \text{ for some } s \in S\} = \ker(f) \lhd R$.

Note. $f(s)$ is a unit in $S^{-1}R$: since $f(s) = \frac{s}{1}$ and $\frac{s}{1}\frac{1}{s} = \frac{1}{1} = 1$.

Proposition 3.2. *Let S be a MCS in R and $f : R \to S^{-1}R$ as above. If $g : R \to R'$ is a ring homomorphism such that $g(s)$ is a unit in R' for all $s \in S$ then there is a unique map $h : S^{-1}R \to R'$ such that $g = h \circ f$*



"g factors through h"

Proof. Uniqueness: Suppose such an h exists. Let $\frac{r}{s} \in S^{-1}R$, $\frac{s}{1}\frac{r}{s} = \frac{r}{1} \Rightarrow h(\frac{s}{1})h(\frac{r}{s}) = h(\frac{r}{1})$ but $h(\frac{r}{1}) = h(f(r)) = g(r) \Rightarrow g(s)h(\frac{r}{s}) = g(r) \Rightarrow h(\frac{r}{s}) = g(r)g(s)^{-1}$

Existence: Define $h : S^{-1}R \to R'$ by $h(\frac{r}{s}) = g(r)g(s)^{-1}$. It it well-defined? $\frac{r_1}{s_1} = \frac{r_2}{s_2} \Rightarrow s(r_1s_2 - r_2s_1) = 0$ for some $s \in S \Rightarrow g(s)(g(r_1)g(s_2) - g(r_2)g(s_1)) = 0 \Rightarrow g(r_1)g(s_2) = g(r_2)g(s_1)$ (Since $g(s)$ is a unit) $\Rightarrow g(r_1)g(s_1)^{-1} = g(r_2)g(s_2)^{-1}$ (again because $g(s_1)$ and $g(s_2)$ are units). It is easy to check that h is a ring homomorphism. $h(f(r)) = h(\frac{r}{1}) = g(r)g(1)^{-1} = g(r)\ \forall r \in R \Rightarrow h \circ f = g$ □

So the pair $(S^{-1}R, f)$ with $f : R \to S^{-1}R$ is determined up to isomorphism by:

1. $s \in S \Rightarrow f(s)$ is a unit
2. $f(r) = 0 \iff rs = 0$ for some $s \in S$
3. $S^{-1}R = \{f(r)f(s)^{-1} | r \in R, s \in S\}$

Example. 1. $P \lhd R$ prime ideal and $S = R \setminus P$. Set $R_P = S^{-1}R$ in this case. "*the localization of R at P*". $f : R \to R_P$, $r \mapsto \frac{r}{1}$, the extension of P to R_P is $PR_P = \{\frac{r}{s} : r \in P, s \notin P\}$ which is the set of non-units in R_P. So this is the unique maximal ideal in R_P, so R_P is a local ring.
Special Case:

(a) R an integral domain, $P = 0$ then R_P is the field of fractions of R. (e.g., $R = \mathbb{Z}$ then $R_P = \mathbb{Q}$)

(b) $R = \mathbb{Z}$, $P = p\mathbb{Z}$ (p a prime number) $\Rightarrow R_P = \mathbb{Z}_{(p)} = \{\frac{r}{s} \in \mathbb{Q} : r \in \mathbb{Z}, s \in \mathbb{Z} \setminus p\mathbb{Z}\} \subseteq \mathbb{Q}$
Let $f \in \mathbb{Z}$. Write $f(p)$ to be the image of f in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Then p is a zero of $f \iff f(p) = 0 \iff f \in p\mathbb{Z}$. What about $f \in \mathbb{Q}$? Write $f = \frac{r}{s}$, $f(p) = \begin{cases} r(p)s(p)^{-1} & \text{if } p \nmid s \ (\iff s(p) \neq 0) \\ \infty & \text{otherwise} \end{cases}$. So f gives a function on $\operatorname{Spec} \mathbb{Z}$ with $f(p) \in \begin{cases} \mathbb{F}_p \cup \{\infty\} & \text{if } p \text{ is a prime} \\ \mathbb{Q} & \text{if } p = 0 \end{cases}$

(c) $R = k[x_1, \dots, x_n]$ where k is an algebraically closed field (e.g., $k = \mathbb{C}$). $M \lhd R, M = (x_1 - a_1, \dots, x_n - a_n)$ where $(a_1, a_2, \dots, a_n) := \underline{a} \in k^n$.
Note. i. M is $\ker(\text{eval}_{\underline{a}} : R \to k$ defined by $f \mapsto f(\underline{a})) \Rightarrow M$ is maximal since $R/M \cong k$
ii. Every maximal ideal of R has this form (by the Hilbert's Nullstellensatz)
$R \subset R_M \subset k(x_1, \dots, x_n)$ and $R_M = \{\frac{f}{g} : f, g \in R, g(\underline{a}) \neq 0\}$ = subring of $k(x_1, \dots, x_n)$ consisting of rational functions which are "defined at $\underline{a}$". The unique maximal ideal in R_m is $MR_M = \{\frac{f}{g} : f(\underline{a}) = 0, g(\underline{a}) \neq 0\}$. Finally $R_M/MR_M \cong k = R/M$

2. $0 \in S \Rightarrow S^{-1}R = 0$ (The zero ring)

3. If $S \subset R^\times$ then $f : R \to S^{-1}R$ is an isomorphism (and conversely)

4. $f \in R, S = \{1, f, f^2, \dots\}$ then $S^{-1}R$ is denoted $R_f = \{\frac{r}{f^n} | r \in R, n \geq 0\}$

Example. $R = \mathbb{Z}, f = 2$, $R_f = \mathbb{Z}[\frac{1}{2}]$

3.1 Localization of Modules

Given an R-module M and a multiplicatively closed set $S \subset R$, let $S^{-1}M = \{$equivalence classes: $\frac{m}{s}$ of pairs (m, s) with $m \in M, s \in S$ modulo the relation $(m, s) \sim (m', s') \iff r(sm' - s'm) = 0$ for some $t \in S\}$. Define $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$ and $\frac{r}{s_1}\frac{m}{s_2} = \frac{rm}{s_1 s_2}$. This turns $S^{-1}M$ into an $S^{-1}R$-module.

Also if $\phi : M \to N$ is an R-linear map then we define $S^{-1}\phi : S^{-1}M \to S^{-1}N$ by $(S^{-1}\phi)(\frac{m}{s}) = \frac{\phi(m)}{s}$. This is an $S^{-1}R$-linear map.

If we have $M_1 \xrightarrow{\psi} M_2 \xrightarrow{\phi} M_3$ is a sequence of R-linear map then $S^{-1}(\phi\psi) = (S^{-1}\phi)(S^{-1}\psi) : S^{-1}M_1 \to S^{-1}M_3$ since they both map $\frac{m}{s} \to \frac{\phi(\psi(m))}{s} \forall \frac{m}{s} \in S^{-1}M_1$

Proposition 3.3. *If $M_1 \xrightarrow{\psi} M_2 \xrightarrow{\phi} M_3$ is an exact sequence of R-modules then $S^{-1}M_1 \xrightarrow{S^{-1}\psi} S^{-1}M_2 \xrightarrow{S^{-1}\phi} S^{-1}M_3$ is an exact sequence of $S^{-1}R$-modules.*

Proof. We need to prove that: $\operatorname{im}\psi = \ker\phi \Rightarrow \operatorname{im}(S^{-1}\psi) = \ker(S^{-1}\phi)$
$\operatorname{im}\psi \subseteq \ker\phi \Rightarrow \phi\psi = 0 \Rightarrow (S^{-1}\phi)(S^{-1}\psi) = S^{-1}(\phi\psi) = S^{-1}0 = 0 \Rightarrow \operatorname{im}(S^{-1}\psi) \subseteq \ker(S^{-1}\phi)$
Conversely: Let $\frac{m_2}{s} \in \ker(S^{-1}\phi)$. Then $0 = \frac{\phi(m_2)}{s}$ so $\exists t \in S$ such that $t\phi(m_2) = 0 \Rightarrow \phi(tm_2) = 0$. So $\exists m_1 \in M_1$ such that $tm_2 = \psi(m_1)$. Now $\frac{m_1}{ts} \overset{S^{-1}\psi}{\mapsto} \frac{\psi(tm_1)}{ts} = \frac{tm_2}{ts} = \frac{m_2}{s}$. So $\frac{m_2}{s} \in \operatorname{im}(S^{-1}\psi)$ as required. □

Special Case: $M_1 = 0$, i.e., ϕ injective: If $M \leq N$ then $S^{-1}M \leq S^{-1}N$

Corollary 3.4. *Let N, N_1, N_2 be R-modules of M. Then:*

1. *$S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2$ (as submodules of $S^{-1}M$)*

2. *$S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$ (as submodules of $S^{-1}M$)*

3. *$S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$*

Proof. 1. Trivial: Both sides consist of elements of $\frac{x_1+x_2}{s} = \frac{x_1}{s} + \frac{x_2}{s}$ ($x_i \in N_i, s \in S$), and $\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{s_2x_1+s_1x_2}{s_1s_2}$, the numerator is in $N_1 + N_2$ and denominator in S, hence the whole fraction is in $S^{-1}(N_1 + N_2)$

2. Exercise

3. Apply the proposition to the short exact sequence $0 \to N \to M \to M/N \to 0$ to get that $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ is exact then by first isomorphism theorem $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$

□

Proposition 3.5. *$S^{-1}M \cong S^{-1}R \otimes_R M$ via the map $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$. That is $S^{-1}M$ is obtain via "extension of scalars" using the standard map $f : R \to S^{-1}R$ as the structure map*

Proof. Map $S^{-1}R \times M \to S^{-1}M$ by $(\frac{r}{s}, m) \mapsto \frac{rm}{s}$. This is bilinear so it induces a well defined map $g : S^{-1}R \otimes_R M \to S^{-1}M$ as in the theorem. We check g is an isomorphism.

g is surjective: $g(\frac{1}{s} \otimes m) = \frac{m}{s}$

Observe that every element of $S^{-1}R \otimes_R M$ has the form $\frac{1}{s} \otimes m$ since $\sum_{i=1}^n \frac{r_i}{s_i} \otimes m_i = \sum_{i=1}^n \frac{r_i'}{s} \otimes m_i$ where $s = s_1s_2 \dots s_n$. But $\sum_{i=1}^n \frac{r_i'}{s} \otimes m_i = \sum_{i=1}^n \frac{1}{s} \otimes r_i'm_i = \frac{1}{s} \otimes (\sum_{i=1}^n r_i'm_i)$. Now we show g is injective. Suppose $g(\frac{1}{s} \otimes m) = 0 \Rightarrow \frac{m}{s} = 0 \Rightarrow \exists t \in S$ such that $tm = 0$. Now $\frac{1}{s} \otimes m = \frac{t}{ts} \otimes m = \frac{1}{ts} \otimes tm = \frac{1}{ts} \otimes 0 = 0$. Hence g is injective. □

Proposition 3.6. *Let M, N be R-modules and S a MCS. Then $S^{-1}M \otimes_{s^{-1}R} S^{-1}N \cong S^{-1}(M \otimes_R N)$ (as $S^{-1}R$-modules)*

Proof.

$$\begin{aligned}
S^{-1}M \otimes_{S^{-1}R} S^{-1}N &\cong (M \otimes_R S^{-1}R) \otimes_{S^{-1}R} S^{-1}N \text{ by the preceding proposition} \\
&\cong M \otimes_R (S^{-1}R \otimes_{S^{-1}R} S^{-1}N) \text{ by associativity} \\
&\cong M \otimes_R S^{-1}N \text{ by Lemma 2.19} \\
&\cong M \otimes_R (S^{-1}R \otimes_R N) \text{ by preceding proposition} \\
&\cong S^{-1}R \otimes_R (M \otimes_R N) \text{ rearranging terms} \\
&\cong S^{-1}(M \otimes_R N) \text{ by preceding proposition}
\end{aligned}$$

□

Special Case: Let $P \lhd R$ be a prime ideal. Let $S = R \setminus P$ and denote $S^{-1}M$ by M_P. (which is a module over the local ring $R_P = S^{-1}R$). Then $M_P \otimes_{R_P} N_P \cong (M \otimes_R N)_P$

3.2 Local Properties

Definition 3.7. A property of R-modules is called *local* if: M has the property if and only if M_P has the property $\forall P \in \operatorname{Spec} R$

Proposition 3.8 (Being zero is a local property)**.** *Let M be an R-module. Then the following are equivalent:*

1. *$M = 0$*
2. *$M_P = 0$ for all prime $P \lhd R$*
3. *$M_P = 0$ for all maximals $P \lhd R$*

Proof. 1⇒2⇒ 3 is trivial. To show $3 \Rightarrow 1$, suppose $M \neq 0$. Let $x \in M, x \neq 0$, set $I = \operatorname{Ann}_R x = \{r \in R : rx = 0\} \lhd R, \neq R$ (as $1 \notin I$), so there exists a maximal ideal $P \supseteq I$. Then $\frac{x}{1} \in M_P$ is non-zero: for $\frac{x}{1} = 0 \iff sx = 0$ for some $s \in R \setminus P$, which is a contradiction. □

Proposition 3.9. *Let $\phi : M \to N$ be a homomorphism of R-modules. The following are equivalent:*

1. *ϕ is injective*

2. $\phi_P : M_P \to N_P$ *is injective for all primes* P

3. $\phi_P : M_P \to N_P$ *is injective for all maximals* P

Moreover the same holds with "injective" replaced by "surjective" throughout.

Proof. Surjective case: $1 \Rightarrow M \overset{\phi}{\to} N \to 0$ is exact $\Rightarrow M_P \overset{\phi_P}{\to} N_P \to 0$ is exact for all primes $P \Rightarrow \phi_P$ is surjective for all $P \Rightarrow 2$.

$2 \Rightarrow 3$ is trivial

$3 \Rightarrow 1$: Let $N' = \phi(M) \leq N$. Then $M \to N \to N/N' \to 0$ is exact. $\Rightarrow M_P \overset{\phi_P}{\to} N_P \to (N/N')_P \to 0$ is exact $\forall$ maximal $P \Rightarrow (N/N')_P = 0$ for all maximal $P \Rightarrow N/N' = 0$ (by previous proposition) $\Rightarrow N = N'$ hence ϕ is surjective.

(Injective case uses the same argument with the exact sequence $0 \to M \to N$) □

3.3 Localization of Ideals

R is a ring, S a multiplicatively closed set $\subset R$, $f : R \to S^{-1}R$ defined by $r \mapsto \frac{r}{1}$. Recall that for $I \lhd R$ we have $I^e = S^{-1}I = \{\frac{r}{s} : r \in I, s \in S\} \lhd S^{-1}R$. (We will use $I \lhd R$ and $J \lhd S^{-1}R$)

Note. Any finite sum $\sum \frac{r_i}{s_i}$ can be put over a common denominator

Proposition 3.10. *1. Every ideal* $J \lhd S^{-1}R$ *is the extension of an ideal* $I \lhd R$. *(Namely* $J = J^{ce}$*)*

2. *If* $I \lhd R$ *then* $I^{ec} = \cup_{s\in S}(I : s)$*; hence* $I^e = (1)$ *if and only if* $I \cap S \neq \emptyset$.

3. *If* $I \lhd R$ *then* I *is the contraction of some ideal* $J \lhd S^{-1}R$ *if and only if no element of* S *is a zero divisor in* R/I.

4. *The correspondence* $P \leftrightarrow S^{-1}P$ *gives an order-preserving bijection between the prime ideals* P *of* R *which do not meet* S *and the prime ideals* $S^{-1}P$ *of* $S^{-1}R$.

5. S^{-1} *commutes with sums, products, intersections and radicals:*

   (a) $S^{-1}(I_1 + I_2) = S^{-1}I_1 + S^{-1}I_2$
   (b) $S^{-1}(I_1 I_2) = (S^{-1}I_1)(S^{-1}I_2)$
   (c) $S^{-1}(I_1 \cap I_2) = S^{-1}I_1 \cap S^{-1}I_2$
   (d) $S^{-1}(r(I)) = r(S^{-1}I)$

Proof. 1. We always have $J \supseteq J^{ce}$. We prove the containment the other way, let $\frac{r}{s} \in J \lhd S^{-1}R \Rightarrow \frac{r}{1} \in J \Rightarrow r \in J^c \Rightarrow \frac{r}{s} = \frac{1}{s}\frac{r}{1} \in (J^c)^e$. Hence $J = J^{ec}$.

2.

$$\begin{aligned} r \in I^{ec} = (S^{-1}I)^c \quad &\iff \quad \frac{r}{1} = \frac{a}{s} \text{ for some } a \in I, s \in S \\ &\iff \quad t(sr - a) = 0 \text{ for some } a \in I, s, t \in S \\ &\iff \quad rs_1 \in I \text{ for some } s_1 \in S \\ &\iff \quad r \in (I : s_1) \text{ for some } s_1 \in S \\ &\iff \quad r \in \cup_{s\in S}(I : S) \end{aligned}$$

So $\underbrace{I^e = (1) \iff I^{ec} = (1)}_{I^e = I^{ece}} \iff 1 \in \cup_{s\in S}(I : s) \iff I \cap S \neq \emptyset$

3. I is a contraction $\iff I^{ec} \subseteq I \iff (sr \in I \text{ for some } s \in S \Rightarrow r \in I) \iff (\bar{s}\bar{r} = 0 \text{in } R/I$ for some $s \in S \Rightarrow \bar{r} = 0) \iff \forall s \in S, \bar{s}$ is not a zero divisor in R/I

4. One way is clear: If Q is a prime of $S^{-1}R$ then Q^c is a prime of R. Conversely: let P be a prime of $R \Rightarrow R/P$ is a domain. Now $\bar{S}^{-1}(R/P) \cong S^{-1}R/S^{-1}P$ (where $\bar{S}$ is the image of S in R/P). But $\bar{S}^{-1}(R/P)$ is a subring of the field of fractions of R/P, so is either 0 or an integral domain. If 0 then $S^{-1}P = S^{-1}R = (1)$. If $\neq 0$ then $S^{-}P$ is a prime ideal of $S^{-1}R$. The first case occurs $\iff 0 \in \bar{S} \iff S \cap P \neq \emptyset$.

5. Easy Exercise

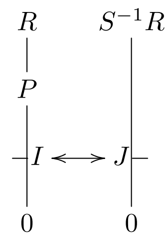
$\square$

Remark. Here's a quick proof that $f \in R$ not nilpotent $\Rightarrow \exists P$ with $f \notin P$ and P prime.

Take $S = \{1, f, f^2, \dots\} \not\ni 0 \Rightarrow S^{-1}R$ is a non-zero ring, so it has a maximal ideal $Q \Rightarrow Q^c = P$ is a prime of $R, P \cap S = \emptyset \Rightarrow f \notin P$.

Corollary 3.11. $N(S^{-1}R) = S^{-1}(N(R))$

Corollary 3.12 (Special case when $S = R \setminus P, P$ prime)**.** *$I \cap S = \emptyset \iff I \subseteq P$. Hence the proper ideals of R_P are in bijection with the ideals of R which are contained in P.*



Corollary 3.13. *The field of fractions of the domain R/P (P is prime) is isomorphic to the residue field of R_P*

Proof. $S = R \setminus P$. The residue field of R_P is $R_P/S^{-1}P = S^{-1}R/S^{-1}P = \bar{S}^{-1}(R/P) =$ field of fraction of R/P since $\bar{S} = (R/P) \setminus \{0\}$. $\square$

Corollary 3.14. *If $P_1 \subset P_2$ are primes of R then $(R/P_1)_{P_2} = R_{P_2}/{P_1}_{P_2}$ - a ring whose prime correspond to primes of R <u>between</u> P_1 and P_2*

Geometrical Interlude I

Let k be an algebraically closed field (e.g. $k = \mathbb{C}$). Let k^n be affine n-space over k: $\{\underline{a} = (a_1, \dots, a_n) : a_j \in k\}$. Algebraic geometry studies solutions to polynomial equations $S = \{f_j(x_1, \dots, n_n)\} \subseteq k[x_1, \dots, x_n]$. $V(S) = \{\underline{a} \in k^n : f_j(\underline{a}) = 0 \, \forall f_j \in S\}$.

Definition. The set $V(S)$ is an *affine algebraic set*

Clearly $V(S) = V(I)$ where I is the ideal of $k[x_1, \dots, x_n]$ generated by S and $V(I) = V(r(I))$, since $f \in r(I) \iff f^n \in I$ $(n \geq 1)$

Hilbert Basis Theorem. *Every ideal $I \lhd k[x_1, \dots, x_n]$ is finitely generated*

Proof. Later □

If $I = (f_1, \dots, f_k)$ then $V(I) = V(\{f_1, \dots, f_k\})$. It is not hard to check that:

- $V(0) = k^n$
- $V(1) = \emptyset$
- $V(\cup_j S_j) = \cap_j V(S_j)$
- $V(IJ) = V(I) \cup V(J)$

Hence the collection of all algebraic subsets of k^n is closed under intersections and finite unions, so they form the closed sets of a topology on k^n called the *Zariski topology* on k^n.

In the other direction: let $S \subset k^n$ and define $I(S) = \{f \in k[x_1, \dots, x_n] : f(\underline{a}) = 0 \, \forall \underline{a} \in S\}$, which is an ideal of $k[x_1, \dots, x_n]$, and in fact $r(I(S)) = I(S)$.

Fact. $V(I(S)) = \overline{S}$ *(for $S \subset k^n, \overline{S}$ is the closure of S in k^n)*

Fact. $I(V(J)) = r(J)$ *for $J \lhd k[x_1, \dots, x_n]$. This is called "Hilbert's Nullstellensatz", we will prove this later.*

The conclusion is that V and I gives (inclusion order-reversing) bijections between radical ideals of $k[x_1, \dots, x_n]$ and closed subsets of k^n.

Definition 3.15. An algebraic set is *irreducible* if it is not the union of two proper closed subsets. ($\iff$ any two non-empty open subsets intersects non-trivially). These are $V(P)$ for P a prime ideal of $k[x_1, \dots, x_n]$. Irreducible algebraic sets are often called *algebraic varieties*

Example. **$n = 1$:** $k^n = k^1 = k$. Now $k[x]$ is a UFD so the primes are (0) and $(x - a)$ with $a \in k$ (since k is algebraically closed). Note $(x - a)$ are maximals and correspond to points of k while (0) is not maximal and correspond to the whole of k. The closed sets are k itself and all the finite subsets of k. (So every infinite subset of k is dense)

$n = 2$: $k[x_1, x_2] = k[x, y]$. Primes have 3 types:

- $(0) \leftrightarrow V(0) = k^2$
- $P = (f(x, y)) \leftrightarrow V(f) =$ irreducible curves in k^2 (f irreducible). e.g., $V(x^2 + y^2 - 1) =$ circle in k^2
- $M = (x - a, y - b) \leftrightarrow V(M) = \{(a, b)\}$ singleton in k^2 $(a, b \in k)$

Coordinate rings (of algebraic sets)

Every element $f \in k[x_1, \dots, x_n]$ defines a polynomial function $k^n \to k$ (defined by $\underline{a} \mapsto f(\underline{a})$). f, g agree on $V(I) \iff f - g \in I(V(I))$. Without loss of generality we can assume $I = r(I)$ so f, g agree on $V(I) \iff f - g \in I$.

Definition. Define $k[V] = k[x_1, \dots, x_n]/I$. Then $k[V]$ is the ring of polynomial function on V. This is called the *coordinate ring of V*.

Ideals of $k[V] \leftrightarrow$ ideals J with $I \subseteq J \lhd k[x_1, \dots, x_n]$. $M_{\underline{a}} =$ Maximal ideals of $k[V] \leftrightarrow$ maximal ideals $M \supseteq I$, i.e., $M = (x_1 - a_1, \dots, x_n - a_n)$ with $\underline{a} = (a_1, \dots, a_n) \in V$. $M_{\underline{a}} = \{\overline{f} \in k[V] : f(\underline{a}) = 0\}$ =kernel of map $k[V] \to k$ defined by $\overline{f} \mapsto f(\underline{a})$.

If V is a variety then $k[V]$ is an integral domain, (since $V = V(P)$ so $K[V] = k[x_1, \dots, k_n]/P$ where P is prime)

We have a correspondence between

- Algebraic sets (or varieties) in k^n
- finitely generated k-algberas (or domains)

This correspondence extends to one which takes polynomial maps between algebraic sets to morphism of k-algebras.

4 Integral Dependence

Definition 4.1. Let A be a subring of the ring B. An element $b \in B$ is *integral over A* if it satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0, a_i \in A \tag{4.1}$$

Let $f(x) = x^2 + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$. If $a \in A$ then a is a root of $x - a$, so a is integral over A

Example. $A = \mathbb{Z}, B = \mathbb{C}$, $z \in \mathbb{C}$ is integral over $\mathbb{Z} \iff z$ is an algebraic integer

$A = \mathbb{Q}, B = \mathbb{C}$ gives algebraic numbers

$A = \mathbb{Z}, B = \mathbb{Q}, z \in \mathbb{Q}$ integral over $\mathbb{Z} \iff z \in \mathbb{Z}$, i.e., let $x = \frac{r}{s}, r, s \in \mathbb{Z}$ coprime. If $\left(\frac{r}{s}\right)^n + \cdots + a_0 = 0$ then $r^n + a_{n-1}r^n s + \cdots + a_0 s^n = 0 \Rightarrow s | r^n \Rightarrow s = \pm 1, x \in \mathbb{Z}$.

A is a UFD, B its field of fraction gives similar result as the previous example.

Theorem 4.2. *Let A be a subring of B, $b \in B$. Then the following are equivalent:*

1. *b is integral over A*
2. *$A[b]$ is a finitely generated A-module*
3. *B contains a subring $C \supseteq A[b]$ which is finitely generated as an A-module*
4. *There exists a faithful $A[b]$-module M which is finitely generated as an A-module*

Proof. $1 \Rightarrow 2$: If b satisfies equation (4.1) then $A[b]$ is generated by $1, b, \ldots, b^{n-1}$ since equation (4.1) $\Rightarrow b^n = -(a_{n-1}b^{n-1} + \cdots + a_0)$

$2 \Rightarrow 3$: Take $C = A[b]$

$3 \Rightarrow 4$: $M = C$. This is a faithful $A[b]$-module as $A[b]$ is a subring C and $1 \in C$. So if $rx = 0 \, \forall r \in A[b], x \in M = C$ then $r1 = 0$, hence $r = 0$.

$4 \Rightarrow 1$: Given M as in 4. let $m_1, \ldots, m_n$be generators of M as an A-module. Let $\phi : M \to M$ be the map defined by $x \mapsto bx$. This is A-linear so $\phi \in \mathrm{End}_A(M)$. Hence there exists $a_0, \ldots, a_{n-1} \in A$ such that $\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 = 0$ (in $\mathrm{End}_A(M)$), i.e., $(\phi^n + \cdots + a_0)y = 0 \, \forall y \in M \Rightarrow (b^n + a_{n-1}b^{n-1} + \cdots + a_0)y = 0 \, \forall y \in M \underset{M \text{ faithful}}{\Rightarrow} b^n + a_{n-1}b^{n-2} + \cdots + a_0 = 0$ ☐

Corollary 4.3. *For all $n \geq 1$, if $b_1, \ldots, b_n \in B$ are all integral over A then $A[b_1, \ldots, b_n]$ is finitely generated as an A-module.*

Proof. We prove this using induction on n.

$n = 1$: Use the previous theorem.

In general: Let $A_1 = A[b_1, \ldots, b_{n-1}]$. Then A_1 is finitely generated as an A module. $A[b_1, \ldots, b_n] = A_1[b_n]$, but b_n is integral over A_1, hence $A_1[b_n]$ is finitely generated as an A_1-module, so $A_1[b_n]$ is finitely generated as an A-module ☐

Corollary 4.4. *Let $C = \{b \in B | b$ integral over $A\} \subseteq B$. Then C is a subring of B containing A.*

Proof. We need to show that for all $x, y \in C$ then $x \pm y, xy \in C$. Since $x, y \in C$ by the previous corollary we know $A[x, y]$ is finitely generate as an A-module and it contains $x \pm y, xy$. By the previous theorem (3.⇒1.) all elements of $A[x, y]$ are integral over A ☐

Definition 4.5. Using the notation of Corollary 4.4, C is the *integral closure* of A in B.

If $C = B$ we say B is *integral* over A

If $C = A$ we say A is *integrally closed* in B

Example. $\mathbb{Z}$ is integrally closed over $\mathbb{Q}$

The integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is the ring of algebraic integers.

Definition 4.6. If A is an integral domain, we say that A is *integrally closed* if A is integrally closed in its field of fractions.

Example. $\mathbb{Z}$ is integrally closed

Any UFD is integrally closed

Corollary 4.7. *If $A \subseteq B \subseteq C$ then C is integral over $A \iff B$ is integral over A and C is integral over B*

Proof. "$\Rightarrow$": Obvious

"$\Leftarrow$": Let $c \in C$. Then $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$, $b_i \in B$. Define $B_0 := A[b_0, \ldots, b_{n-1}]$. Then c is integral over B_0 and B_0 is finitely generated as an A-module. By the theorem c is integral over A $\square$

Corollary 4.8. *The integral closure of A in B is integrally closed in B*

Proof. Trivially follows from previous corollary $\square$

Example. Let K be a number field (that is a field containing $\mathbb{Q}$ with finite degree). Then the integral closure of $\mathbb{Z}$ in K is the ring of algebraic integers of K, called the *ring of integers.* That is, the ring of integers is $K \cap \{\text{ring of all algebraic integers}\}$. We will denote this $\mathcal{O}_K$ (or $\mathbb{Z}_K$). e.g.:

- $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$ (the Gaussian integers)
- $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_K$ contains $\mathbb{Z}[\sqrt{-3}]$. In fact $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$
- $K = \mathbb{Q}(\sqrt[3]{10})$. The integral closure of $\mathbb{Z}$ in K is $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}]$

Proposition 4.9. *Let B be an integral extension of A. Then:*

1. *For all $J \lhd B$, $I = J^c = J \cap A$ we have B/J is integral over A/I*
2. *If S is a multiplicatively closed set in A then $S^{-1}B$ is integral over $S^{-1}A$.*
   Special Case: *P a prime of A, $S = A \setminus P \Rightarrow B_P$ is integral over A_P*

Proof. Let $b \in B$ satisfy $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ (in B) $\Rightarrow \bar{b}^n + \bar{a_1}\bar{b}^{n-1} + \cdots + \bar{a_n} = 0$ (in B/J)$\Rightarrow \bar{b}$ is integral over A/I

$\frac{b}{s} \in S^{-1}B \Rightarrow \left(\frac{b}{s}\right)^n + \frac{a_1}{s}(\frac{b}{s})^{n-1} + \cdots + \frac{a_{n-1}}{s^{n-1}}(\frac{b}{s}) + \frac{a_n}{s^n} = 0 \Rightarrow \frac{b}{s}$ is integral over $S^{-1}A$ $\square$

Lemma 4.10. *Let B be an integral extension of A, with A and B both domains. Then B is a field if and only if A is a field*

Proof. Assume A is a field. Let $b \in B, b \neq 0$. Let $b^n + a_1 b^{n-1} + \cdots + a_{n-1}b + a_n = 0$ be an integral equation of minimal degree n. Then $a_n \neq 0$ so a_n^{-1} exists in A. Hence the equation can be rewritten as $b(b^{n-1} + \cdots + a_{n-1}) = -a_n \Rightarrow b^{-1} = -a_n^{-1}(b^{n-1} + \cdots + a_{n-1}) \in B$. Hence b as an inverse, so B is a field.

Conversely suppose B is a field. Let $a \in A, a \neq 0$. Then a^{-1} exists in B. So there is an equation: $(a^{-1})^n + a_1(a^{-1})^{n-1} + \cdots + a_n = 0$ ($a_i \in A$), which can be rearranged to give $a^{-1} = -(a_1 + a_2 a + \cdots + a_n a^{n-1}) \in A$. $\square$

Lemma 4.11. *Let B be an integral extension of A. Let $Q \lhd B$ be prime and $P = Q \cap A$, a prime of A. Then P is maximal if and only if Q is maximal*

Proof. By Proposition 4.9 B/Q is integral over A/P so by Lemma 4.10 Q is maximal $\iff B/Q$ is a field $\iff A/P$ is a field $\iff P$ is maximal $\square$

Theorem 4.12. *Let B be an integral extension of A and P a prime of A. Then:*

1. *There exists a prime Q of B with $P = Q \cap A$*
2. *If Q_1, Q_2 are primes of B with $Q_1 \cap A = P = Q_2 \cap A$ and $Q_1 \supseteq Q_2$ then $Q_1 = Q_2$.*

Proof. Consider the following commutative diagram:

$$\begin{array}{ccc} A & \xhookrightarrow{\text{int}} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_P & \xhookrightarrow{\text{int}} & B_P \end{array}$$

Let M be a maximal ideal in B_P. Let $Q = \beta^{-1}(M)$, a prime in B. Now $Q \cap A = P$ since $M \cap A_P$ is maximal in A_P (Lemma 4.11) but A_P has only one maximal ideal namely PA_P, which contracts to P: $\alpha^{-1}(M \cap A_P) = P = A \cap \beta^{-1}(M) = A \cap Q$.

Let Q_1 and Q_2 be as in the statement. Then let $N_1 = Q_1 B_P$ and $N_2 = Q_2 B_P$ their extension in B_P. These are primes of B_P (by Proposition 3.10, and the fact that $Q_j \cap S = \emptyset$ where $S = A \setminus P$).

Claim: N_1, N_2 are maximal.

This follow from $N_j \cap A_P$ are maximal (using Lemma 4.11), but $N_1 \cap A_P = N_2 \cap A_P = PA_P$ since both contract to P. Hence each N_j is maximal. But if $Q_1 \supseteq Q_2 \Rightarrow N_1 \supseteq N_2 \Rightarrow N_1 = N_2 \Rightarrow Q_1 = \beta^{-1}(N_1) = \beta^{-1}(N_2) = Q_2$ □

Example (Counter-Example showing the requirement of part 2). $A = \mathbb{Z}, B = \mathbb{Z}[i], P = 5\mathbb{Z}$, then if we let $Q_1 = (2+i), Q_2 = (2-i)$ we find $Q_1 \cap \mathbb{Z} = 5\mathbb{Z}$ and $Q_2 \cap \mathbb{Z} = 5\mathbb{Z}$

The "Going Up" Theorem. *Consider the following set-up.*

$$\begin{array}{lcl} B & & Q_1 \subseteq \cdots \subseteq Q_m \textit{(primes of } B) \\ \text{int}\uparrow & & \\ A & & P_1 \subseteq P_2 \subseteq \cdots \subseteq P_m \subseteq \cdots \subseteq P_n \ \textit{(primes of } A) \end{array}$$

with $Q_i \cap A = P_i$ (for all $1 \le i \le m$). With that set-up there exists $Q_{m+1}, \ldots, Q_n$ primes of B with $Q_m \subseteq Q_{m+1} \subseteq \cdots \subseteq Q_n$ and $Q_i \cap A = P_i$ (for $m+1 \le i \le n$)

Proof. By induction we reduce to the case $m = 1, n = 2$. That is we must find Q_2 such that $Q_1 \subseteq Q_2$ and $Q_2 \cap A = P_2$. (where $P_1 \subseteq P_2$ and $Q_1 \cap A = P_1$)

Let $\bar{A} = A/P_1, \bar{B} = B/Q_1$. Then $\bar{B}$ is integral over $\bar{A}$ (by Proposition 4.9) and P_2/P_1 is a prime of $\bar{A}$ so there exists a prime of $\bar{B}$ above it. This prime has the form Q_2/Q_1 with $Q_2 \supseteq Q_1$ and Q_2 a prime of B. Then $(Q_2/Q_1) \cap \bar{A} = P_2/P_1 \Rightarrow Q_2 \cap A = P_2$ □

4.1 Valuation Rings

Definition 4.13. A *valuation ring* is an integral domain R such that for every $x \in K$ (the field of fractions of R) either $x \in R$ or $x^{-1} \in R$

Example. $\mathbb{Z}$ is not a valuation ring ($\frac{2}{3} \notin \mathbb{Z}, \frac{3}{2} \notin \mathbb{Z}$)

$\mathbb{Z}_{(p)}$ is a valuation ring

$R = K$: any field is a valuation ring.

Proposition 4.14. *Let R be a valuation ring with field K. Then:*

1. *R is a local ring*
2. *$R \subseteq R' \subseteq K \Rightarrow R'$ is a valuation ring*
3. *R is integrally closed*

Proof. 2. trivial

1. The units of R are the (non-zero) $x \in K$ with both $x, x^{-1} \in R$. Let $M = \{$non-units in $R\} = \{x \in R : x^{-1} \notin R\} \cup \{0\}$. We'll show that $M \lhd R$, then it's the unique maximal ideal of R. Let $x \in M, r \in R$. Then rx is not a unit since otherwise $x^{-1} = r(rx)^{-1} \in R$, contradiction, i.e., $rx \in M$. Let $x, y \in M$ be non-zero. Then either $\frac{x}{y} \in R$ or $\frac{y}{x} \in R$. If $\frac{x}{y} \in R$ then $x + y = y(\frac{x}{y} + 1) \in M$. Otherwise if $\frac{y}{x} \in R$ then $x + y = x(1 + \frac{y}{x}) \in M$

3. Let $x \in K$ be integral over R. Then $x^n + r_1 x^{n-1} + \cdots + r_n = 0$ $(r_i \in R)$. If $x \in R$ there is nothing to prove. If $x^{-1} \in R$ then $x + (r_1 + r_2 x^{-1} + \cdots + r_n (x^{-1})^{n-1}) = 0 \Rightarrow x \in R$ □

Definition 4.15. Let K be a field. A *discrete valuation* on K is a function $v : K^* \to \mathbb{Z}$ such that:

1. $v(xy) = v(x) + v(y) \, \forall x, y \in K^*$
2. $v(x+y) \ge \min\{v(x), v(y)\} \, \forall x, y \in K^*$ with $x + y \ne 0$

We extend v to a function $K \to \mathbb{Z} \cup \{\infty\}$ by setting $v(0) = \infty$. Now 1., 2. holds for all $x, y \in K$ with the obvious conventions.

Example 4.16. $K = \mathbb{Q}$, p a prime number, $v = \text{ord}_p$ defined as follows: for $x \in \mathbb{Q}^*$ write $x = p^n \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $p \nmid a, b$ and $n \in \mathbb{Z}$. Set $\text{ord}_p(x) = n$.

Associated to every discrete valuation of K there is a valuation ring R_v. $R_v = \{x \in K : v(x) \geq 0\}$. Clearly R_v is a ring (by 1. and 2.). Also R_v is a valuation ring since $v(x^{-1}) = -v(x)$ for all $x \in K^*$.

Definition 4.17. These R_v are called *discrete valuation ring* (DVR)

Example. $K = \mathbb{Q}$ has a DVR for each prime p, namely $v = \text{ord}_p$ then $R_v = \mathbb{Z}_{(p)}$.

Note. $\cap_p \mathbb{Z}_{(p)} = \mathbb{Z}$

Exercise. Every valuation ring of $\mathbb{Q}$ is $\mathbb{Q}$ itself or $\mathbb{Z}_{(p)}$ for some prime p.

Example. Let $K = k(x)$ where k is a field. K is the field of fractions of $k[x]$. Let $p(x)$ be a monic irreducible polynomial in $k[x]$. Every element of K^* can be written as $p^n \frac{a}{b}$ where $a, b \in k[x]$ and $p \nmid a, b$ with $n \in \mathbb{Z}$. In this case n is uniquely determined. Define $\text{ord}_p(p^n \frac{a}{b}) = n$, just as for $K = \mathbb{Q}$ this is a discrete valuation. The associated valuation ring is $\{\frac{f(x)}{g(x)} \in k[x] : p(x) \nmid g(x)\}$

e.g. $K = \mathbb{C}(x)$. The monic irreducible monic polynomial are $p(x) = x - a$ ($x \in \mathbb{C}$). Then

$$\text{ord}_p(h) = \begin{cases} n > 0 & \text{if } h \text{ has a zero of order } n \text{ at } a \\ n < 0 & \text{if } h \text{ has a pole of order } n \text{ at } a. \\ 0 & \text{if neither} \end{cases}$$

e.g. $K = k(x)$. Define $v(\frac{f}{g}) = \deg(g) - \deg(f)$ then v is a discrete valuation. Note $k(x) = k(\frac{1}{x})$. This v is just $\text{ord}_{1/x}$

Let v be a discrete valuation on K such that $v : K^* \to \mathbb{Z}$ is surjective. (This only involves rescaling v, unless v is identically 0). Let $\pi \in K$ be such that $v(\pi) = 1$.

$R_v = \{x \in K : v(x) \geq 0\}$ - $M_v \cup U_v$

$M_v = \{x \in K : v(x) > 0\}$ - maximal ideal of R_v

$U_v = \{x \in K : v(x) = 0\}$ - set of units in R_v

If $x, y \in R_v$ then $x|y \iff \frac{y}{x} \in R_v \iff v(\frac{y}{x}) \geq 0 \iff v(y) \geq v(x)$. So if x_n is an element with $v(x_n) = n$ (for all $n \in \mathbb{Z}$) then $x_n | x_{n+1}$ $\forall n$ hence $R_v \supset (x_1) \supset (x_2) \supset \ldots$

Every $x \in R \setminus \{0\}$ can be written uniquely as $x = \pi^n u$ where $n = v(x) \geq 0$ and $u \in U_v$. (Since if $n = v(x)$ then $u = \pi^{-n} x \Rightarrow v(u) = -n + v(x) = 0 \Rightarrow u \in U_v$), i.e., R_v is a UFD with only one prime, namely π.

Every ideal in R_v is principal: the only non-zero ideals are (π^n), $n \geq 0$. $M_v = (\pi)$ since $x \in M_v \iff v(x) \geq 1 = v(\pi) \iff \pi | x$. If $I \lhd R_v, I \neq 0$ let $n = \min\{v(x) : x \in I\}$. Then $I = (\pi^n)$ since $\exists x \in I$ with $v(x) = n$ $\forall y \in I$, $v(y) \geq n \Rightarrow x|y$ so $I = (x)$, and $v(x) = v(\pi^n) \Rightarrow x = \pi^n u \Rightarrow (x) = (\pi^n) = (\pi)^n$.

Geometrically Interlude II: Hilbert's Nullstellensatz.

Algebraic form of Nullstellensatz. *Let k be a field and let F be a field which is a finitely generated k-algebra. Then F is a finite algebraic extension of k. In particular if k is algebraically closed then $F = k$.*

Weak form of Nullstellensatz. *Let k be an algebraically closed field and $I \lhd k[x_1, \dots, x_n]$. If $I \neq (1)$ then $V(I) \neq \emptyset$ (i.e., $\exists \underline{a} \in k^n$ such that $f(\underline{a}) = 0 \,\forall f \in I$)*

Corollary 4.18. *The maximal ideals in $k[x_1, \dots, x_n]$ (k algebraically closed) are precisely the ideals $M_{\underline{a}} = (x_1 - a_1, \dots, x_n - a_n)$, $\underline{a} \in k^n$*

Strong form of Nullstellensatz. *Let k be an algebraically closed field and $I \lhd k[x_1, \dots, x_n]$. Then $I(V(I)) = r(I)$ (i.e., if $g(\underline{a}) = 0$ whenever $f(\underline{a}) = 0 \,\forall f \in I$ then $g^N \in I$)*

Proof that Algebraic form $\Rightarrow$ Weak form. Let k be a algebraically closed field and $I \underset{\neq}{\lhd} k[x_1, \dots, x_n] \Rightarrow I \subseteq M$ a maximal ideal. Consider $k \to k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/M$. Now $k[x_1, \dots, x_n]/M$ is a field which is a finitely generated k-algebra. By the Algebraic form the composite of the previous map is surjective ($k[x_1, \dots, x_n]/M \cong k$ as k is algebraically closed), so for all i, $\exists a_i \in k$ such that $x_i - a_i \in M$. So $M \supseteq (x_1 - a_1, \dots, x_n - a_n) = M_{\underline{a}}$. But $M_{\underline{a}}$ is maximal so $M = M_{\underline{a}}$. Now for all $f \in I \Rightarrow f \in M \Rightarrow f(\underline{a}) = 0$ □

Proof that Weak form $\Rightarrow$ Strong form. $I \lhd k[x_1, \dots, x_n]$. We know that $I(V(I)) \supseteq r(I)$ since $g \in r(I) \Rightarrow g^N \in I \Rightarrow g^N(\underline{a}) = 0 \,\forall \underline{a} \in V(I) \Rightarrow g(\underline{a}) = 0 \Rightarrow g \in I(V(I))$.

Conversely let $g \in I(V(I))$, then $(*)$ $(f(\underline{a}) = 0 \,\forall f \in I) \Rightarrow g(\underline{a}) = 0$.

Extend the ring $k[x_1, \dots, x_n]$ by adding a new variable y to get $k[x_1, \dots, x_n, y]$. In $k[x_1, \dots, x_n, y]$ form the ideal J generated by all $f \in I$ and $1 - g(x_1, \dots, x_n)y$, i.e., $J = (1 - g(x)y) + I \cdot k[x_1, \dots, x_n, y]$. Now $V(J) = \emptyset$ (in k^{n+1}) since if $(a_1, \dots, a_n, b) \in V(J)$ then

1. $f(a_1, \dots, a_n) = 0 \,\forall f \in I$
2. $1 - g(a_1, \dots, a_n)b = 0$

This is clearly a contradiction to $(*)$. So by the Weak form, we have $J = k[x_1, \dots, x_n, y]$, i.e., $1 \in J$. So

$$1 = h(x_1, \dots, x_n, y)(1 - g(x_1, \dots, x_n)y) + \sum_j h_j(x_1, \dots, x_n, y) f_j(x_1, \dots, x_n) \; f_j \in I.$$

Substitute $y = \frac{1}{g(x_1, \dots x_n)}$ to get an equation in $k(x_1, \dots, x_n)$.

$$1 = \sum_j h_j(x_1, \dots, x_n, \frac{1}{g(x_1, \dots, x_n})f_j(x_1, \dots, x_n)$$

The RHS is a rational function whose denominator is a power of g. So for large enough $N \geq 0$:

$$g^N = \sum_j \tilde{h}_j(x_1, \dots, x_n) f_j(x_1, \dots, x_n) \in I$$

for some $\tilde{h}_j \in k[x_1, \dots, x_n]$. Hence $g \in r(I)$ □

Proof of Algebraic Form of Nullstellensatz. $F = k[x_1, x_2, \dots, x_n]$ (where $x_i \in F$ are the generators of F) is a field. We must show that each x_i is algebraic over k. We are going to use induction on n

$n = 1$: $F = k[x_1]$. Write x_1^{-1} as a polynomial in x_1, then we can get an equation for x_1 over k. (Alternative: if x_1 were not algebraic then $k[x_1]$ is a polynomial ring, not a field)

Inductive Step: $F = k(x_1)[x_2, \dots, x_n]$ (since F is a field) is a finitely generated algebra over $k(x_1)$ with only $n - 1$ generators. So each x_j for $j \geq 2$ is algebraic over $k(x_1)$. If we can show that x_1 is algebraic over k then we are done. For all $j \geq 2$, we have a polynomial equation for x_j over $k(x_1)$. Let $f \in A := k[x_1]$ be a common denominator for all coefficient for all these polynomials. Consider the ring $A_f = S^{-1}A$ where $S = \{1, f, f^2, f^3, \dots\}$. All the $n - 1$ polynomials are monic in with coefficients in A_f. Hence each x_j ($j \geq 2$) is integral over A_f. It follows that F is integral over A_f

since $F = A[x_2, \ldots, x_n] = A_f[x_2, \ldots, x_n]$. By Lemma 4.10, since F is a field, so is A_f. Let $K = k(x_1)$, a subfield of F, the field of fractions of both A and A_f. Now $A = k[x_1] \subseteq A_f \subseteq K = k(x_1)$ and A_f a field implies that $A_f = K$ (since K is the smallest field containing A, being its field of fractions)

If x_1 were not algebraic over k then $A = k[x_1]$ would be the polynomial ring in one variable over k and $k(x_1) = K$ its field of fractions. Take any irreducible $g \in k[x_1]$ with $g \nmid f$, then $\frac{1}{g} \notin A_f$. (NB: $k[x_1]$ would have infinitely many irreducible) This leads to a contradiction hence x_1 is algebraic

□

5 Noetherian and Artinian modules and rings

Proposition 5.1 (Definition)**.** *An R-module M is* Noetherian *if it satisfies one of the following equivalent conditions:*

1. ACC (Ascending Chain Condition)*: any ascending chain $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ of submodules of M terminates, i.e., for some n we have $M_n = M_{n+1} = \dots$*

2. *Every non-empty collection of submodules of M has a maximal element*

3. *Every submodule of M is finitely generated*

Definition 5.2. A ring R is *Noetherian* if it is so as an R-module, i.e., the ideals of R satisfies ACC and every ideal if finitely generated.

Proposition 5.3 (Definition)**.** *An R-module M is* Artinian *if it satisfies the following equivalent conditions*

1. DCC (Descending Chain Condition): *any descending chain $M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$ of submodule of M terminates, i.e., for some n we have $M_n = M_{n+1} = \dots$*

2. *Every non-empty collection of submodules has a minimal element*

Proof of Proposition5.1. 1) $\iff$ 2): If we had an infinite AC $M_1 \subsetneqq M_2 \subsetneqq M_3 \subsetneqq \dots$ then $\{M_n : n \geq 1\}$ has no maximal elements. Conversely if S is a non-empty set of submodules of M with no maximal elements, then pick $M_1 \in S$, $\exists M_2 \supsetneqq M_1, \exists M_3 \supsetneqq M_2, \dots$

2) $\Rightarrow$ 3): Let S be the set of finitely generated submodules of N, where $N \leq M$. $0 \in S$ so S has a maximal elements, say N_0. So $N_0 \leq N$ and N_0 is finitely generated, if $N_0 \neq N$ take $x \in N \setminus N_0$, then $N_0 + Rx \supsetneqq N_0$ and is finitely generated, contradiction.

3) $\Rightarrow$ 1): Given $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$, let $N = \cup_{n=1}^{\infty} M_n$. Then N is a submodule of M. Let $x_1, \dots, x_n$ generate N. For large enough k, M_k contains contain all of the x_i. Then $M_k = N = M_{k+1} = M_{k+1} = \dots$ □

Note that the proof of 1) $\iff$ 2) can easily be adapted to prove Proposition 5.3

Example.

1. Every finite $\mathbb{Z}$-module is both Noetherian and Artinian

2. If R is a field k then R-modules are k-vector spaces and they are Noetherian $\iff$ they are finite dimensional $\iff$ they are Artinian.

3. $\mathbb{Z}$ is a Noetherian ring (every ideal is generated by 1 element) but is not Artinian: $\mathbb{Z} \supset (2) \supset (4) \supset (8) \supset \dots \supset (2^n) \supset \dots$.

4. $R = k[x_1, x_2, \dots]$ polynomials in a countable (non-finite) number of variables. R is neither Noetherian nor Artinian: $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \dots$ and $(x_1) \supset (x_1^2) \supset (x_1^3) \supset \dots$

Proposition 5.4. *If $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ is a short exact sequence of R-modules then M_2 is Noetherian $\iff$ both M_1, M_3 are. Similarly M_2 is Artinian $\iff$ both M_1, M_3 are.*

Proof. The proof for both cases are the similar, so we are just going to prove the Artinian case.

"$\Rightarrow$" : Suppose M_2 is Artinian. Any Descending Chain in M_1maps isomorphically under α to a Descending Chain in M_2 which terminates. Similarly any Descending Chain in M_3 lifts to a Descending Chain in M_2 via β^{-1} , hence terminates

"$\Leftarrow$": Suppose M_1, M_3 Artinian. Let $N_1 \supseteq N_2 \supseteq N_3 \supseteq \dots$ be a Descending Chain in M_2. Then $\alpha^{-1}(N_1) \supseteq \alpha^{-1}(N_2) \supseteq \dots$ is a Descending Chain in M_1,hence stops, and $\beta(N_1) \subseteq \beta(N_2) \subseteq \dots$ is a Descending Chain in M_3, hence stops. So there exists n such that $\alpha^{-1}(N_n) = \alpha^{-1}(N_{n+1}) = \dots$ and $\beta(N_n) = \beta(N_{n+1}) = \dots$. This implies $N_n = N_{n+1}$ since let $x \in N_n$, then $\beta(x) \in \beta(N_n) = \beta(N_{n+1}) \Rightarrow \exists y \in N_{n+1}$ with $\beta(x) = \beta(y)$. So $x - y \in \ker(\beta) = \mathrm{im}(\alpha)$, so $x - y = \alpha(z)$ for some $z \in M_1$ and since $\alpha(z) = x - y \in N_n, z \in \alpha^{-1}(N_n) = \alpha^{-1}(N_{n+1}) \Rightarrow \alpha(z) \in N_{n+1}$ so $x = y + \alpha(z) \in N_{n+1}$. □

Corollary 5.5. *Any finite sum of Noetherian (respectively Artinian) modules is again Noetherian (respectively Artinian)*

Proof. The sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ is exact. □

Note. A subring of a Noetherian ring is not necessarily Noetherian, e.g. $R = k[x_1, x_2, \dots] \subset k(x_1, x_2, \dots)$.

Corollary 5.6. *If R is Noetherian and M is a finitely generated R-module then M is Noetherian. Same for Artinian.*

Proof. $R^n = R \oplus R \oplus \cdots \oplus R$ is a Noetherian R-module, since R is. Every finitely generated R-module $M = Rx_1 + \cdots + Rx_n$ is the homomorphic image of some R^n, i.e., $0 \to \ker \to R^n \to M \to 0$ is exact. □

Later we'll prove that R Noetherian $\Rightarrow$ $R[x]$ is Noetherian (Hilbert Basis Theorem). Hence $R[x_1, \dots, x_n]$ is Noetherian, e.g, $R = k$ a field. Hence any finitely generated R-algebra is Noetherian.

5.1 Noetherian Rings

Lemma 5.7. *If R is a Noetherian ring and $f : R \to S$ a surjective ring homomorphism then S is Noetherian*

Proof. $R/\ker(f) \cong S \Rightarrow S$ is Noetherian as an R-module$\Rightarrow S$ is Noetherian. □

Lemma 5.8. *Let $R \leq S$ with R Noetherian. If S is finitely generated as an R-module then S is Noetherian.*

Proof. S is Noetherian as R-module by Corollary 5.6 hence is also Noetherian as S-module. □

Example. $\mathbb{Z}$ is Noetherian $\Rightarrow$ any ring which is finitely generated as $\mathbb{Z}$-module is Noetherian.
$\mathbb{Z}[\alpha]$ with α an algebraic integer is Noetherian

Lemma 5.9. *If R is a Noetherian ring and S a multiplicatively closed set in R then $S^{-1}R$ is Noetherian.*

Proof. By Proposition 3.10 there is a bijection, preserving inclusion, between the set of ideals of $S^{-1}R$ and a subset of the ideals of R. So Ascending Chain Condition for $R \Rightarrow$ Ascending Chain Condition for $S^{-1}R$ □

Corollary 5.10. *If R is Noetherian and $P \lhd R$ prime then R_P is a Noetherian local ring*

Hilbert Basis Theorem. *If R is a Noetherian ring then so is $R[x]$*

Proof. Let $J \lhd R[x]$. For $n \geq 0$ let I_n be the ideal of R consisting of all leading coefficients of $f \in J$ with $\deg(f) = n$ and 0. It is easy to check that I_n is an ideal. Then $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ since $\deg(f) = n \Rightarrow \deg(xf) = n + 1$ and they have the same leading coefficients. By Ascending Chain Condition for R there exists n such that $I_n = I_{n+1} = \dots$. Let $f_{1,n}, f_{2,n}, \dots, f_{k_n,n} \in J$ be polynomials of degree n whose leading coefficients generates I_n. For each $0 \leq m < n$ let $f_{1,m}, \dots, f_{k_m,m}$ $(k_m \geq 0)$ be polynomials in J of degree m whose leading coefficients generates I_m. (Use $k_m = 0$ if $I_m = 0$)
Claim: J is generated by all $f_{i,m}$, with $m \leq n, i \leq k_m$.
Let $g \in J$. Proceed by induction on $\deg(g)$. Our base case is the 0 polynomial, since this is trivial.

Case 1. $\deg(g) \geq n$: Then the leading coefficient of g are in $I_n \Rightarrow \exists r_1, \dots r_{k_n} \in R$ such that $\mathrm{lc}(g) = \mathrm{lc}(\sum_{i=1}^{k_n} r_i f_{i,n})$ where $\mathrm{lc}(f)$ = leading coefficient of f. $\Rightarrow$ leading term of g = leading term of $(g_1 = \sum r_i x^{\deg(g)-n} f_{1,n})$, $g_1 \in (f_{i,j})$. So $g_2 = g - g_1$ has $\deg(g_2) < \deg(g_1)$. By induction $g_2 \in (f_{i,j})$ so $g \in (f_{i,j})$

Case 2. $\deg(g) = m < n$: Now an R-linear combination of $f_{i,m}$ $(1 \leq i \leq k_m)$ has the same leading term as g. The rest is as in Case 1.

Hence J is generated by the finite set $\{f_{i,j} : 1 \leq i \leq k_m, 0 \leq j \leq n\}$. Hence every ideal in $R[x]$ is finitely generated, so $R[x]$ is a Noetherian ring □

Corollary 5.11. *If R is Noetherian so is $R[x_1, x_2, \ldots, x_n]$ for all $n \geq 1$*

Proof. Since $R[x_1, \ldots, x_{n-1}][x_n] = R[x_1, x_2, \ldots, x_n]$ □

In particular if k is a field then $k[x_1, \ldots, x_n]$ is Noetherian. Hence any system of polynomial equation has the same set of zeros as a finite system

Corollary 5.12. *If R is Noetherian then so is any finitely generated R-algebra.*

Proof. Any finitely generated R-algebra is of the form $R[\alpha_1, \ldots, \alpha_n]$ - a quotient of $R[x_1, \ldots, x_n]$ □

Example. Any finitely generated k-algebra (k a field) is Noetherian.

Any finitely generated $\mathbb{Z}$-algebra is Noetherian. (e.g., the ring of integers in a number field is Noetherian: NB theses do not all have the form $\mathbb{Z}[\alpha]$ with a single generator)

6 Primary Decomposition

In general rings we don't have a factorization theory which expresses elements as products of prime powers. Instead we make do with writing ideals as intersections of primary ideals.

Definition 6.1. A *primary* ideal $Q \lhd R$ is a proper ideal such that $xy \in Q \Rightarrow x \in Q$ or $y^n \in Q$ for some $n \geq 1$, i.e., $xy \in Q \Rightarrow$ either $x \in Q$ or $y \in r(Q)$.

Equivalently: $R/Q \neq 0$ and every zero-divisor is nilpotent.

Proposition 6.2. *1. Every prime ideal is primary.*

2. The contraction of a primary is primary.

3. If Q is primary then $r(Q)$ is prime. It is the smallest prime containing Q.

Proof. 1. Clear from the definition ($n = 1$)

2. Let $f : A \to B$ be a ring homomorphism, $Q \lhd B$ primary $\Rightarrow Q^c = f^{-1}(Q) \lhd A$ is primary. To see this: $1 \notin Q^c$ since $f(1) = 1 \notin Q$, hence $A/Q^c \neq 0$. Also note that f induces an injective map $A/Q^c \hookrightarrow B/Q$ so A/Q^c also has the property that zero-divisors are nilpotent.

3. Let $P = r(Q)$. Suppose $xy \in P$. Then $x^n y^n \in Q$ (for some $n \geq 1$) so either $x^n \in Q$ or $(y^n)^m \in Q$ (for some $m \geq 1$), so either $x \in P$ or $y \in P$. For the last sentence use the fact that the radical of I is the intersection of prime ideals containing I

□

Definition 6.3. If Q is primary and $r(Q) = P$ we say that Q is *P-primary*

Example. 1. In $\mathbb{Z}$ the primary ideals are (0) and (p^n), p prime, $n \geq 1$.

2. $R = k[x, y]$. Let $Q = (x, y^2) \Rightarrow P = r(Q) = (x, y)$. $P^2 = (x^2, xy, y^2) \subsetneqq Q \subsetneqq P$. Now $R/Q \cong k[y]/(y^2)$ in which we see that {nilpotent} = {zero-divisors} = {multiples of y}. This is an example of a primary which is not a prime power.

3. An example of prime power needs not be primary. Let $R = k[X, Y, Z]/(XY - Z^2) = k[x, y, z]$ where x, y, z satisfies the relation $xy = z^2$. Let $P = (x, y)$, then $R/P \cong k[X, Y, Z]/(X, Y) \cong k[Y] \Rightarrow P$ prime. Now $xy = z^2 \in P^2$ which is not primary, since $x \notin P^2$ and $y \notin P$.

Proposition 6.4. *1. If $r(I)$ is maximal then I is primary*

2. If M is maximal then M^n is M-primary for all $n \geq 1$

Proof. 1. Let $M = r(I)$. Then M/I is the nilradical of R/I, and M/I is prime so R/I has a unique prime ideal, namely M/I. So every non-nilpotent element of R/I is a unit, so it is not a zero-divisor.

2. $r(M^n) = M$ (since $r(M^n) \supseteq M$ and M is maximal)

□

Lemma 6.5. *Any finite intersection of P-primary ideals is again P-primary.*

Proof. Let Q_i be P-primary for $i = 1, \ldots, n$. Set $Q = \cap_{i=1}^n Q_i$. Then $r(Q) = r(\cap_{i=1}^n Q_i) = \cap_{i=1}^n r(Q_i) = \cap_{i=1}^n P = P$. If $xy \in Q$ and $x \notin Q$ then $\exists i$ such that $xy \in Q_i$ but $x \notin Q_i$. Hence $y \in r(Q_i) = P \Rightarrow y \in r(Q)$ □

Lemma 6.6. *Let Q be P-primary and let $x \in R$. Then:*

1. $x \in Q \Rightarrow (Q : x) = R$

2. $x \notin Q \Rightarrow (Q : x)$ is P-primary

3. $x \notin P \Rightarrow (Q : x) = Q$

To make sense of the three cases remember that $Q \subseteq P \subseteq R$.
Recall: $(Q : x) = \{y \in R : xy \in Q\} \supseteq Q$

Proof. 1. If $x \in Q$ then $xy \in Q \, \forall y \in R$.

2. We have $Q \subseteq (Q : x) \subseteq P$, where the second containment holds because $xy \in Q, x \notin Q \Rightarrow y \in P$. So $r(Q) = P \subseteq r(Q : x) \subseteq r(P) = P \Rightarrow r(Q : x) = P$. Now suppose $yz \in (Q : x)$ with $y \notin P \Rightarrow yxz \in Q \Rightarrow y(xz) \in Q \Rightarrow xz \in Q \Rightarrow z \in (Q : x)$. So $(Q : x)$ is indeed P-primary.

3. If $xy \in Q$ but $x \notin P \Rightarrow y \in Q$.

□

Definition 6.7. A *primary decomposition* of an ideal $I \lhd R$ is an expression $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ with each Q_i primary.

Remark. Such a decomposition may or may not exist. It does always exists when R is Noetherian.

Let $P_i = r(Q_i)$ - the primes associated with the decomposition.

Minimality Condition 1 If some $Q_j \supseteq \cap_{i \neq j} Q_i$ then Q_j may be omitted.

Minimality Condition 2 If more than one Q_i has the same radical we may combine them (using Lemma 6.5)

We call the decomposition *minimal* if:

1. No $Q_j \supseteq \cap_{j \neq i} Q_i$.

2. The P_i are distinct.

It will turn out that the primes P_i are uniquely determined by I, but the Q_i need not be.

Example. Let $I = (x^2, xy) \lhd k[x, y]$ where k is any field. Then $I = P_1 \cap P_2^2$ where $P_1 = (x)$ and $P_2 = (x, y)$ (note P_1 is prime hence primary, and P_2 is maximal hence P_2^2 is primary). This is a minimal primary decomposition. Note that $P_1 \subset P_2$ (this means $V(P_2) \subset V(P_1)$, we say P_2 is an embedded prime). Also $I = P_1 \cap Q_2$ where $Q_2 = (x^2, y)$ with $r(Q_2) = P_2$ again.

Theorem 6.8. *Let $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ be a minimal primary decomposition. Let $P_i = r(Q_i)$. Then $P_i, \ldots, P_n$ are all the prime ideals in the set $\{r(I : x) | x \in R\}$. Hence the set of P_i is uniquely determined by I, independent of the decomposition.*

Proof. Consider $(I : x) = (\cap_{i=1}^n Q_i : x) = \cap_{i=1}^n (Q_i : x)$ by the Fact on page 6. This means $r(I : x) = r(\cap_{i=1}^n (Q_i : x)) = \cap_{i=1}^n r(Q_i : x)$. But $r(Q_i : x) = \begin{cases} R & x \in Q_i \\ P_i & x \notin Q_i \end{cases}$ by Lemma 6.6. Hence $r(I : x) = \cap_{i : x \notin Q_i} P_i$.

If $r(I : x)$ is prime, P say, then $P = \cap_{x \notin Q_i} P_i \Rightarrow P = P_i$ by Proposition 1.15.

Conversely for each i choose $x \in Q_j$ $(\forall j \neq i)$, $x \notin Q_i$ (this is possible by minimality condition 1) then $r(I : x) = P_i$. □

Notation 6.9. To each I with a primary decomposition we have a set of primes P_i called the *associated primes* of I. Any minimal elements of this set is called an *isolated* or *minimal* prime of I. Any other primes associated to I are called *embedded* primes.

We'll prove later that P_i isolated $\Rightarrow Q_i$ is uniquely determined.

Corollary 6.10. *Suppose that* 0 *is decomposable. Then $D :=$ {zero-divisors in R} =union of all primes associated to* 0.

$N =$ *{nilpotent in R}* $= N(R) =$ *intersection of all minimal primes associated to* 0

Proof. Note that D is not an ideal (in general), but we can still define $r(D) = \{x \in R : x^n \in D$ for some $n \geq 1\} = D$ (exercise: if x^n is a zero-divisor, so is x). Note that $D = \cup_{x \neq 0} (0 : x)$ so if we take radicals $D = r(D) = \cup_{x \neq 0} r(0 : x)$. Let $0 = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ be minimal primary decomposition. Let $x \neq 0$, $r(0 : x) = \cap_{x \notin Q_j} P_j \subseteq P_{j_0}$ where $x \notin Q_{j_0}$. Note that j_0 exists since $x \neq 0$. Hence $D = \cup_{x \neq 0} r(x : 0) \subseteq \cup_{j=1}^n P_j$. But each $P_j = r(0 : x)$ for some $x \neq 0$ so each $P_j \subseteq D$

$N(R) = r(0) = \cap r(Q_i) = \cap P_i$. □

Corollary 6.11. *Let $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ be a minimal primary decomposition and $P_i = r(Q_i)$. Then $\cup_{i=1}^n P_i = \{x \in R : (I : x) \neq I\}$ $(*)$*

Proof. Apply the previous corollary to R/I: Note that $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n \Rightarrow 0 = \overline{Q_1} \cap \overline{Q_2} \cap \cdots \cap \overline{Q_n}$ where as usual $\overline{Q_i} \lhd R/I$. Each $\overline{Q_i}$ is primary in R/I since $(R/I)/\overline{Q_i} \cong R/Q_i$. So the zero-divisors in R/I are the union of all $r(\overline{Q_i}) = \overline{r(Q_i)} = \overline{P_i}$ and $\overline{y}$ is a zero-divisors in $R/I \iff \exists x \notin I : yx \in I \iff y$ in RHS of $(*)$. While $\overline{y} \in \cup \overline{P_i} \iff y \in \cup P_i$ □

6.1 Primary Decomposition and Localization

Proposition 6.12. *Let Q be P-primary and S a multiplicatively closed set in R*

1. *$S \cap P \neq \emptyset \Rightarrow S \cap Q \neq \emptyset$ and $S^{-1}Q = S^{-1}R$*
2. *$S \cap P = \emptyset \Rightarrow S^{-1}Q$ is $S^{-1}P$-primary and $(S^{-1}Q)^c = Q$*

Proof. 1. $S \cap P \neq \emptyset$, then there exists $s \in S \cap P \Rightarrow s^m \in S \cap Q$ for some m. We can now use Proposition 3.10 (part 2.) to show $S^{-1}Q = S^{-1}R$.

2. $Q^{ec} = \cup_{s \in S}(Q : s)$ by Proposition 3.10 (part 2.) but $x \in (Q : s) \Rightarrow x \cdot s \in Q, s \neq P \supset Q \Rightarrow S^n \notin Q \forall n \Rightarrow x \in Q \Rightarrow Q^{ec} = Q$. To show that $S^{-1}Q$ is $S^{-1}P$-primary, note $r(Q^e) = r(S^{-1}Q) = S^{-1}r(Q) = S^{-1}P$, also if $\frac{x}{s} \cdot \frac{y}{t} \in S^{-1}Q$ (so there exist $u \in S$ such that $uxy \in Q$) and $\frac{x}{s} \notin S^{-1}Q \Rightarrow x \notin Q$ but Q is still primary, hence $uy \in P, u \in S$ and $S \cap P = \emptyset \Rightarrow y \in P \Rightarrow \frac{y}{t} = \frac{uy}{ut} \in S^{-1}P \Rightarrow S^{-1}Q$ is $S^{-1}P$-primary.

□

Notation. We denote $S(I) = (S^{-1}I)^c = \cup_{s \in S}(I : s)$

Proposition 6.13. *Let S be a multiplicatively closed set in R and $I = Q_1 \cap \cdots \cap Q_n$ be a minimal primary decomposition of I numbered so that $\begin{cases} S \cap P_i = \emptyset & 1 \leq i \leq m \\ S \cap P_i \neq \emptyset & m+1 \leq i \leq n \end{cases}$. Then $S^{-1}I = \cap_{i=1}^m S^{-1}Q_i$ and $S(I) = \cap_{i=1}^m Q_i$. Both of these decomposition are minimal primary decompositions.*

Proof. For $i \in \{1, \ldots, m\}$ we have $S^{-1}Q_i$ is $S^{-1}P_i$-primary by the previous proposition, furthermore $S^{-1}P_i$ are distinct primes of $S^{-1}R$ (by Proposition 3.10 part 4.) therefore $S^{-1}I = S^{-1}(\cap_{i=1}^n Q_i) = \cap_{i=1}^n S^{-1}Q_i \underset{i>m \Rightarrow S^{-1}Q_i = S^{-1}R}{=} \cap_{i=1}^m S^{-1}Q_i$ is a minimal primary decomposition. From this it is clear that $S(I) = \cap_{i=1}^m Q_i$. □

Recall: A prime P is minimal (or isolated) for an ideal I if it is minimal under inclusion in the set of associated primes of I. More generally we define:

Definition 6.14. A set $\mathscr{P}$ of primes associated to I to be *isolated* if $P \in \mathscr{P}$, $P' \subset P$ and P' is associated to I then we have $P' \in \mathscr{P}$.

Theorem 6.15. *Let I be an ideal of the ring R. Let $\mathscr{P} = \{P_1, \ldots, P_n\}$ be an isolated set of primes associated to I. Then $Q_1 \cap \cdots \cap Q_m$ is independent of the minimal primary decomposition of I.*

Proof. Let $S = R \setminus \cup_{i=1}^m P_i$ then S is a multiplicatively closed set and $P_j \cap S = \emptyset \iff P_j \in \mathscr{P}$. Indeed $P_j \in \mathscr{P}$ means $P_j \cap S = \emptyset$ and conversely $P_j \notin \mathscr{P} \Rightarrow P_j \nsubseteq P_i \forall P_i \in \mathscr{P} \Rightarrow P_j \nsubseteq \cup_{i=1}^m P_i \Rightarrow P_j \cap S \neq \emptyset$. Therefore $S(I) = Q_1 \cap Q_2 \cap \cdots \cap Q_m$. This ideal only depends on the primes in $\mathscr{P}$. □

Corollary 6.16. *The isolated primary component of I are uniquely determined.*

Proof. Choose $\mathscr{P} = \{P\}$ where P is a minimal prime, let $S = R \setminus P$, then $S(I) = Q$ with Q is the unique P-primary factor of I. □

6.2 Primary Decomposition in a Noetherian Ring

The main aim of this sub-section is to prove the existence of primary decomposition in a Noetherian ring.

Definition 6.17. An ideal I is *irreducible* if $I = J_1 \cap J_2$ then $I = J_1$ or $I = J_2$.

Lemma 6.18. *In a Noetherian ring R, every ideal is a finite intersection of irreducible ideals.*

Proof. Let S be the set of ideals which are not finite intersections of irreducible ideals. If $S \neq \emptyset$ then S has a maximal element, I (since R is Noetherian). Then I is not irreducible, therefore $I = J_1 \cap J_2$ with $J_1, J_2 \supsetneq I$. So $J_1, J_2 \notin S$, hence they are finite intersection of irreducible ideals. Since the intersection of two finite intersection of irreducible ideals, I is the intersection of irreducible ideals, i.e., $I \notin S$. This is a contradiction. Hence $S = \emptyset$ □

Lemma 6.19. *In a Noetherian ring R, all irreducible ideals are primary.*

Proof. Let I be irreducible. Let $x, y \in R$ with $xy \in I$. We must show that either $x \in I$ or $y^n \in I$ for some $n \geq 1$.

Define $I_n = (I : y^m)$ for $m = 1, 2, \ldots$. Then $I \subseteq I_1 \subseteq I_2 \subseteq \ldots$, since R is Noetherian there exists N such that $I_n = I_{n+1}$

Claim: $I = (I + (x)) \cap (I + (y^n))$

It is clear that $I \subseteq (I + (x)) \cap (I + (y^n))$. Let $z \in (I + (x)) \cap (I + (y^n))$, so $z = i_1 + r_1 x = i_2 + r_2 y^n$ for some $i_1, i_2 \in I$ and $r_1, r_2 \in R$. Then $yz = i_1 y + r_1 xy \in I$ (since $i_1, xy \in I$). So $r_2 y^{n+1} = yz - i_2 y \in I \Rightarrow r_2 \in (I : y^{n+1}) = I_{n+1} = I_n \Rightarrow r_2 y^n \in I$, hence $z \in I$. So $(I + (x)) \cap (I + (y^n)) \subseteq I$

Since I is irreducible, either:

- $I + (x) = I$, in which case $x \in I$
- or $I + (y^n) = I$, in which case $y^n \in I$

□

Theorem 6.20. *In a Noetherian ring R, every ideal I has a primary decomposition.*

Proof. This follows directly from the previous two lemma. □

Proposition 6.21. *Let R be a Noetherian ring, every ideal I contains a power of its radical. In particular, the nilradical is nilpotent.*

Proof. Let $x_1, \ldots, x_k$ generate $r(I)$ (R is Noetherian). For large enough n we have $x_i^n \in I \, \forall i$. Now $r(I)^{kn} \subseteq I$ since $r(I)^{kn}$ is generated by elements of the form $x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}$ where $\sum m_i = nk$, so at least of one of the $m_i \geq n \Rightarrow$ the generators of $r(I)^{kn}$ is in I, hence $r(I)^{kn} \subseteq I$.

For the in particular part, just apply the proposition to $I = 0$. □

Corollary 6.22. *Let R be a Noetherian ring, M a maximal ideal and Q an ideal. Then the following are equivalent:*

1. *Q is M-primary*
2. *$r(Q) = M$*
3. *$M^n \subseteq Q \subseteq M$ for some $n \geq 1$.*

Proof. 1. $\iff$ 2. (by Definition 6.3)

2. $\Rightarrow$ 3.: By the previous Proposition

3. $\Rightarrow$ 2.: Take the radicals $M = r(M^n) \subseteq r(Q) \subseteq r(M) = M \Rightarrow r(Q) = M$ □

Krull's Theorem. *Let I be an ideal in a Noetherian ring R. Then $\cap_{n=1}^{\infty} I^n = 0$ if and only if $1 + I$ contains no zero-divisors.*

Proof. "$\Rightarrow$": If $1+I$ contains a zero-divisor $1-x$, with $x \in I$, such that $(1-x)y = 0$ for some $y \neq 0$, then $y = xy = x^2y = x^3y = \cdots = x^n y \in I^n$. So $y \in \cap_{n=1}^{\infty} I^n$, hence $\cap_{n=1}^{\infty} I^n \neq 0$

"$\Leftarrow$": Let $J = \cap_{n=1}^{\infty} I^n$

Claim: $IJ = J$.

Certainly $IJ \subseteq J$. Let $IJ = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ be a minimal primary decomposition of IJ with $r(Q_i) = P_i$, so we must show that $J \subseteq Q_i \, \forall i$. We have $IJ \subseteq Q_i$.

Case 1. If $I \subseteq P_i$ then $Q_i \supseteq P_i^m$ (by Proposition 6.21) $\supseteq I^m \supseteq J \Rightarrow J \subseteq Q_i$

Case 2. If $I \nsubseteq P_i$ then $J \subseteq Q_i$ since if $x \in I, x \notin P_i$ then $xJ \subseteq IJ \subseteq Q_i$ so for all $y \in J, xy \in Q_i$ but $x \notin r(Q_i) = P_i \Rightarrow y \in Q_i$.

Hence $J \subseteq \cap Q_i = IJ$ so $J = IJ$.

By Nakayama's Lemma since J is finitely generated, $xJ = 0$ for some $x \in 1+I$. If $1+I$ has no zero-divisors then x is not a zero-divisor, so $xJ = 0 \Rightarrow J = 0$. □

Corollary 6.23. *In a Noetherian domain R, if $I \neq R$ then $\cap_{n=1}^{\infty} I^n = 0$*

Proof. Obvious □

Corollary 6.24. *If $I \subset J(R)$ then $\cap_{n=1}^{\infty} I^n = 0$*

Proof. Obvious from Proposition 1.12 □

Corollary 6.25. *In a Noetherian local ring with maximal idea M, $\cap_{n=1}^{\infty} M^n = 0$*

Proof. Obvious since $M = J(R)$.

□

7 Rings of small dimension

Proposition 7.1. *In the ring R, suppose $0 = M_1 M_2 \dots M_n$ with M_i maximal ideals. Then R is Noetherian if and only if R is Artinian.*

Proof. $R \supset M_1 \supseteq M_1M_2 \supseteq M_1M_2M_3 \supseteq \cdots \supseteq M_1M_2\dots M_n = 0$. Let $V_i := M_1M_2\dots M_{i-1}/M_1M_2\dots M_i$, notice that each V_i is a module over the field R/M_i, i.e, is a vector space. So each V_i is Noetherian $\iff$ Artinian $\iff$ finite dimensional. We then use Proposition 5.4, over and over again on the following set of short exact sequences.

$$\begin{array}{lcl}
0 \to M_1 \to R \to V_1 \to 0 \quad R \text{ Noetherian} & \iff & M_1, V_1 \text{ are both Noetherian} \\
0 \to M_1M_2 \to M_1 \to V_2 \to 0 & \iff & M_1M_2, V_1, V_2 \text{ are all Neotherian} \\
0 \to M_1M_2M_3 \to M_1M_2 \to V_3 \to 0 & \iff & M_1M_2M_3, V_1, V_2, V_3 \text{ are all Noetherian} \\
\vdots & \dots & \dots \\
0 \to \overset{M_1M_2\dots M_n}{=0} \to M_1M_2\dots M_{n-1} \to V_n \to 0 & \iff & V_1, V_2, \dots V_n \text{ are all Noetherian} \\
0 \to \overset{M_1M_2\dots M_n}{=0} \to M_1M_2\dots M_{n-1} \to V_n \to 0 & \iff & V_1, V_2, \dots, V_n \text{ are all Artinian} \\
\vdots & \dots & \dots \\
0 \to M_1 \to R \to V_1 \to 0 & \iff & R \text{ is Artinian}
\end{array}$$

□

Proposition 7.2. *Let R be a Noetherian local ring with maximal ideal M. Then either $M^n \neq M^{n+1}$ for all $n \geq 1$. Or $M^n = 0$ for some n in which case R is Artinian and M is its only prime ideal.*

Proof. Suppose $M^n = M^{n+1}$ for some n. Then $M^n = M^{n+1} = M^{n+1} = \dots$. So $\cap_{k=1}^{\infty} M^k = M^n$, but by Corollary 6.25 we have $\cap_{k=1}^{\infty} M^k = 0$, hence $M^n = 0$. By previous proposition, R is Artinian.

Let P be a prime of R. Then $P \supseteq 0 = M^n$, taking radicals $P = r(P) \supseteq r(M^n) = M$, so $P = M$ □

Definition 7.3. A ring in which every prime is maximal is said to have *dimension* 0.

Example. Any field
$\mathbb{Z}/n\mathbb{Z}$ (since primes are $p\mathbb{Z}/n\mathbb{Z}$, $p \nmid n$)
Any finite ring (since every finite integral domain is a field)

Proposition 7.4. *Artinian rings have dimension 0.*

Proof. Let $P \lhd R$ be a prime. Let $\overline{R} = R/P$, a domain. Let $\overline{x} \in \overline{R}$, $\overline{x} \neq 0$ (so $x \in R \setminus P$). Now in $\overline{R}$ we have $(\overline{x}) \supseteq (\overline{x}^2) \supseteq (\overline{x}^3) \supseteq \dots$. By Descending Chain Condition in $\overline{R}$ (which is also Artinian) there exists n such that $(\overline{x}^n) = (\overline{x}^{n+1})$, so $\overline{x}^n = \overline{x}^{n+1}\overline{y}$ for some $\overline{y} \in \overline{R}$. Since $\overline{x} \neq 0$ and $\overline{R}$ is a domain, cancel $\overline{x}$ from both sides n times to get $1 = \overline{xy}$. Hence $\overline{R}$ is a field and P is maximal. □

Proposition 7.5. *An Artinian ring R has only finitely many maximal ideals.*

Proof. Consider the set of all finite intersections of maximal ideals $M_1 \cap M_2 \cap \cdots \cap M_n, n \geq 1$. Since R Artinian, this set has a minimal element $M_1 \cap M_2 \cap \cdots \cap M_n = I$. Let M be any maximal ideal in R. Then $M \cap I \subseteq I$, so by minimality of I we have $M \cap I = I \Rightarrow M \supseteq I = M_1 \cap \cdots \cap M_n \Rightarrow M \supseteq M_i$ for some i by Proposition 1.15, hence $M = M_i$ for some i. □

Proposition 7.6. *Let R be an Artinian ring, then $N(R) = J(R)$ is nilpotent, i.e., $(N(R))^k = 0$ for some $k \geq 1$.*

Proof. Let $N := N(R)$, and consider $N \supseteq N^2 \supseteq N^3 \supseteq \dots$ so by the Descending Chain Condition there exists k such that $N^k = N^{k+1} = N^{k+2} = \dots =: I$. We want to show that $I = 0$. Suppose $I \neq 0$. Let $S = \{\text{ideals } J \lhd R \text{ such that } IJ \neq 0\}$. Notice $S \neq \emptyset$ since $R \in S$ as $I \neq 0$. So let $J \in S$ be minimal (which exists since R is Artinian). Then $\exists x \in J$ such that $xI \neq 0$, so $(x) \subseteq (J)$ and $(x)I \neq 0$ so $(x) \in S$ and by minimality $J = (x)$. Now $((x)I)I = (x)I^2 = (x)I \neq 0$ since $I^2 = I$, so $(x)I \in S$ and $(x)I \subseteq (x) = J$ so by minimality of J we have $(x)I = (x)$. So there exist $y \in I$ such that $xy = x \Rightarrow xy = xy^2 = xy^3 = \dots = xy^n = \dots$, but $y \in I \subseteq N$ so y is nilpotent, so $y^n = 0$ for some $n \Rightarrow x = 0$. This contradicts the fact $I \neq 0 = (x)$ □

Proposition 7.7. *Every Artinian ring R is Noetherian*

Proof. Let $M_1, M_2, \dots, M_n$ be the complete set of all maximal ideals of R (by Proposition 7.5). So $N = N(R) = J(R) = \cap_{i=1}^n M_i$. Also $N^k = 0$ for some $k \geq 1$. Consider $M_1^k M_2^k \dots M_n^k = (M_1 M_2 \dots M_n)^k \subseteq (M_1 \cap M_2 \cap \dots \cap M_n)^k = N^k = 0$. So $M_1^k M_2^k \dots M_n^k = 0$ so by Proposition 7.1 we have that R Artinian $\Rightarrow R$ Noetherian. □

Remark. Every Noetherian ring of dimension 0 is Artinian. (c.f. Atiyah and Macdonald pg.90)

The Structure Theorem for Artinian Rings. *Every Artinian ring is uniquely isomorphic to a finite direct product of Artinian local rings.*

Proof. Existence: Let $M_1, \dots, M_n$ be the maximal ideals of R. Then $\prod_{i=1}^n M_i^k = 0$ for some k. The ideals M_i^k are pairwise comaximal so by the Chinese Remainder Theorem we have

$$\begin{aligned} R &= R/0 \\ &= R/\prod_{i=1}^{n} M_i^k \\ &= R/\bigcap_{i=1}^{n} M_i^k \text{ by comaximality} \\ &\cong \bigoplus_{i=1}^{n} R/M_i^k \text{ by Chinese Remainder Theorem} \end{aligned}$$

Now each R/M_i^k has only one maximal ideal, M_i/M_i^k so is an Artinian local ring.

Uniqueness: c.f. Atiyah and Macdonald pg. 90 □

7.1 Noetherian integral domains of dimension 1

Including Dedekind domain and Discrete Valuation Rings

Definition 7.8. The *dimension* of a ring R is the maximal length (≥ 0) of a chain of prime ideals $P_0 \subsetneqq P_1 \subsetneqq \dots \subsetneqq P_n$ in R.

Dim0: All primes are maximal

Dim1: e.g., $R = \mathbb{Z}$ and any integral domain, not a field in which all non-zero primes are maximal.

Example. $k[x_1, \dots, x_n]$ has dimension n.

Proposition 7.9. *Let R be a Noetherian domain of dimension 1. Then every non-zero ideal I of R has a unique expression as a product of primary ideals with distinct radicals.*

Proof. Let $I = Q_1 \cap \dots \cap Q_n$ with each Q_i primary and each $P_i = r(Q_i)$ maximal. ($P_i \supseteq Q_i \supseteq I \neq 0$). No $P_i \subseteq P_j$ ($i \neq j$) so no embedding primes, hence the Q_i are unique. The P_i are pairwise comaximal ($P_i + P_j = R$ for all $i \neq j$) hence so are the Q_i. To see this $r(Q_i + Q_j) = r(P_i + P_j) = r(1) = (1) \Rightarrow Q_i + Q_j = (1)$. Hence $Q_1 \cap \dots \cap Q_n = Q_1 \dots Q_n$.

Conversely if $I = Q_1' Q_2' \dots Q_m'$ where Q_i' are primary with distinct radicals $r(Q_i')$. As before the Q_i' are comaximal, so $I = \prod Q_i' = \cap Q_i'$. By uniqueness of primary decomposition, $m = n$ and $Q_i = Q_i'$ after permuting. □

Recall: A DVR (Discrete Valuation Ring) is the valuation ring R of a ($\mathbb{Z}$-valued) discrete valuation $\nu : R \to \mathbb{Z} \cup \{\infty\}$. Such an R has the properties:

- R is local with maximal ideal $M = \{x : \nu(x) \geq 1\}$
- M is principal: $M = (\pi)$ with $\nu(\pi) = 1$
- All non-zero ideals of R are $M^n = (\pi^n)$, $n \geq 0$.
- Hence R is Noetherian (it's a PID) and a domain
- R has dimension 1 since the only primes are 0 and M

Lemma 7.10. *Let R be a Noetherian integral domain of dimension 1 which is local, with maximal ideal M and residue field $k = R/M$. Then*

1. *Every ideal $I \neq (0), (1)$ is M-primary, so $I \supseteq M^n$ for some n.*
2. $M^n \neq M^{n+1}\, \forall n \geq 0$

Proof. R has two prime ideal, (0) and M. Let $I \lhd R$ with $I \neq (0), (1)$, then $r(I) =$ intersections of the primes containing I. So $r(I) = M$, and M is maximal, hence I is M-primary. Now $I \supseteq M^n$ for some $n \geq 1$ since R is Noetherian.

If $M^n = M^{n+1}$ then $M^n = 0$ which implies R has dimension 0. □

Proposition 7.11. *Let R be a Noetherian integral domain of dimension 1 which is local, with maximal ideal M and residue field $k = R/M$. Then the following are equivalent:*

1. *R is a DVR,*
2. *R is integrally closed,*
3. *M is principal,*
4. $\dim_k(M/M^2) = 1$,
5. *every non-zero ideal of R is a power of M,*
6. *there exists $\pi \in R$ such that every non-zero ideal is principal, of the form (π^n), $n \geq 0$.*

Proof. **1 ⇒ 2:** Every valuation ring is integrally closed (See Proposition 4.14)

2 ⇒ 3: Let $a \in M$, $a \neq 0$. If $(a) = M$ we are done. Otherwise $(a) \subsetneqq M$. Choose $n \geq 0$ such that $M^n \subseteq (a), M^{n-1} \nsubseteq (a)$. Such an n exists since (by the previous lemma) $r((a))$ is a power of M and $(a) \supseteq M^n$ for some n. Choose $b \in M^{n-1} \setminus (a)$ so $\frac{b}{a} \notin R$. Let $x = \frac{a}{b} \in K$, the field of fractions of R.

Claim $M = (x)$.

Since $b \notin (a)$, $x^{-1} \notin R$. Since R is integrally closed, x^{-1} is not integral over R. This means that $x^{-1}M \nsubseteq M$. To see this suppose $x^{-1}M \subseteq M$, then M is a module over the ring $R[x^{-1}]$ which is a finitely generated R-module, since R is Noetherian, and faithful as an $R[x^{-1}]$-module (since K has no zero-divisors so if $y \in R[x^{-1}]$ satisfies $yM = 0$ then $y = 0$); and these would imply that x^{-1} is integral over R. But $x^{-1}M \subseteq R$, since $bM \subseteq M^{n-1}M = M^n \subseteq (a)$. So $x^{-1}M$ is an ideal of R not contained in its unique maximal ideal. Hence $x^{-1}M = R$, and hence $M = (x)$ proving the claim.

3 ⇒ 4: Let $M = (x)$, i.e., x generates M (as R-module), so $\overline{x}$ generates M/M^2 (as $k = R/M$-module), i.e., $\dim_k M/M^2 \leq 1$. But $M \neq M^2 \Rightarrow M/M^2 \neq 0$ hence $\dim_k M/M^2 \geq 1$.

4 ⇒ 5: For any $\overline{x}$ which generates M/M^2, the element $x \in R$ generates M. (By Corollary 2.17). So $M = (x)$, so $M^n = (x^n)$ $(\forall n \geq 0)$. Let I be a proper non-zero ideal of R. So $I \subseteq M$, since $\cap_{k=1}^{\infty} M^k = 0$ there exists $n \geq 1$ such that $I \subseteq M^n$ and $I \nsubseteq M^{n+1}$. Let $y \in I \setminus M^{n+1}$, since $y \in I \subseteq M^n = (x^n)$, we have $y = cx^n$, with $c \notin M = (x)$. So c is a unit of R, so $M^n = (x^n) = (y) \subseteq I \subseteq M^n$. Therefore $I = M^n$

$5 \Rightarrow 6$**:** Let $\pi \in M \setminus M^2$. Then $(\pi) = M$ by 5. so every non-zero ideal $I = M^n = (\pi^n)$.

$6 \Rightarrow 1$**:** Note that $M = (\pi)$ where π is given as in 6. So $M^n = (\pi^n)\ \forall n \geq 0$. Let $a \in R, a \neq 0$, then $(a) = M^n$ for some $n \geq 0$. Define $\nu(a) = n$. Extend to a function $\nu : K^* \to \mathbb{Z}$ by setting $\nu(\frac{a}{b}) = \nu(a) - \nu(b) \in \mathbb{Z}$. Easy check that:

1. ν is well define
2. ν is a group homomorphism. $(\nu(xy) = \nu(y) + \nu(x))$
3. $\nu(\pi) = 1 \Rightarrow \nu$ is surjective
4. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$

So ν is a discrete valuation and $R = \{x \in K : \nu(x) \geq 0\}$

□

7.2 Dedekind Domains

These are Noetherian integral domains R of dimension 1 such that every localization R_p (for all maximal p) is a DVR.

Lemma 7.12 (Definition)**.** *A Dedekind Domain R is a Noetherian integral domain of dimension* 1 *satisfying any of the following equivalent conditions:*

1. *R is integrally closed.*
2. *Every primary ideal of R is a prime power.*
3. *Every localization R_p (at non-zero primes P) is a DVR.*

Proof. $1 \iff 3$**:** Since being integrally closed is a local property, so we use the Proposition 7.11.

$2 \Rightarrow 3$**:** Let P be a non-zero prime and let $M = P_p$ be the extension of P to R_p, so M is the unique maximal ideal in R_p. Every ideal $(\neq (0), (1))$ in R_p is M-primary. Every P-primary ideal of R is a power of P (by condition 2.) so its extension to R_p is M-primary and is a power of M. So all non-zero ideals of R_p are powers of M. So we can use 5. from Proposition 7.11 and hence R_p is a DVR.

$3 \Rightarrow 2$**:** Let Q be P-primary in R (where P is a non-zero prime). Its extension to R_p is M-primary so is a power of M, hence Q is a power of P. Since $Q = (M^n)^c = (M^c)^n = P^n$

□

Corollary 7.13. *In a Dedekind domain, every non-zero ideal has a unique factorization as a product of prime ideals.*

Let I be an ideal of a Dedekind domain R. Then $I = P_1^{n_1} P_2^{n_2} \dots P_k^{n_k}$ with each P_i distinct maximal and $n_i \geq 1$. If P is any non-zero prime the extension of I in R_P is the product of the extensions of the $P_i^{n_i}$in R_p. If $P_i \neq P$, the extension is the whole ring R_p. If $P_i = P$ the extension is the maximal ideal of R_p, P_p. So $I_p = P_p^n$ where n is the exponent of P in the factorization of $I, n \geq 0$.

Define ν_p to be the discrete valuation which has valuation ring R_p, so ν_p is a discrete valuation of the field of fractions K of R. Hence

$$I = \prod_{P \text{ non-zero prime}} P^{\nu_P(I)}.$$

Consequences:

- $$\begin{array}{ccc} I \subseteq J & \Longleftrightarrow & J \mid I \\ \Updownarrow & & \Updownarrow \\ \forall P : I_P \subseteq J_P & \Longleftrightarrow & \nu_p(J) \leq \nu_p(I)\ \forall P \end{array}$$

  Note $I_p = P_p^{\nu_p(I)}, J_p = P_p^{\nu_p(J)}$. Therefore $I \subseteq J \iff J|I$

  "to contain is to divide"

- $\nu_p(I+J) = \min\{\nu_p(I), \nu_p(J)\}$
- $\nu_p(I \cap J) = \max\{\nu_p(I), \nu_p(J)\}$
- $\nu_p(IJ) = \nu_p(I) + \nu_p(J)$

7.3 Examples of Dedekind Domains

1. Every PID is a Dedekind Domain.

   - Noetherian (every ideal has 1 generator)
   - Integrally closed (since a UFD)
   - Dimension 1 (the non-zero primes are (π) with π irreducible - these are maximal)

2. Let K be a number field, i.e, a finite extension (field) of $\mathbb{Q}$, of degree n. $n = [K : \mathbb{Q}] = \dim_{\mathbb{Q}} K$. The ring of integers $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, i.e., $\mathcal{O}_K$ is the set of all algebraic integers in K.

   Claim: $\mathcal{O}_K$ is a Dedekind Domain

   Proposition. *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, i.e., there exists $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$ ("integral basis"). This implies $K = \mathbb{Q}\alpha_1 + \ldots \mathbb{Q}\alpha_n$.*

   Proof. Omitted (See Algebraic Number Theory Course) □

   Corollary 7.14. *$\mathcal{O}_K$ is Noetherian.*

   $\mathcal{O}_K$ is integrally closed, being in the integral closure of $\mathbb{Z}$ in K. We need to check that it has dimension 1. Let P be a non-zero prime of $\mathcal{O}_K$. We want to show that P is maximal.

   Method 1: Show $\mathcal{O}_K/P$ is finite. (In fact P is also a free $\mathbb{Z}$-module of rank n). Now every finite integral domain is a field so P is maximal.

   Method 2: Consider $P \cap \mathbb{Z}$, this is a prime ideal of $\mathbb{Z}$. It is non-zero since $\mathcal{O}_K$ is an integral extension of $\mathbb{Z}$ so we cannot have both 0 and P (prime of $\mathcal{O}_K$) contracting to 0, primes of $\mathbb{Z}$. So $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. Now $p\mathbb{Z}$ is maximal so P is maximal.

   All of this proves that $\mathcal{O}_K$ is a Dedekind Domain.

   Two special properties of $\mathcal{O}_K$, not shared by Dedekind Domains in general:

   (a) (Dirichlet) $\mathcal{O}_K^\times$ (the group of units) is finitely generated. If $K = \mathbb{Q}(\alpha)$, where α has minimal polynomial $f(x)\mathbb{Q}[x]$, irreducible of degree n (the degree of the number field). Let m be the number of irreducible factors of f in $\mathbb{R}[x]$. Then there exists units $\epsilon_1, \ldots, \epsilon_{m-1} \in \mathcal{O}_K^\times$ such that every unit is uniquely $\zeta\epsilon_1^{n_1}\epsilon_2^{n_2}\ldots\epsilon_{m-1}^{n_{m-1}}$, where ζ is a root of unity and $n_j \in \mathbb{Z}$.

   (b) Let $I, J \lhd \mathcal{O}_K$ be non-zero ideals. Define an equivalence relation: $I \sim J \iff \alpha I = \beta J$ with $\alpha, \beta \in \mathcal{O}_K$ and non-zero. In particular $I \sim \mathcal{O}_K$ if and only if I is principal.

   Exercise. $I \sim J \iff I \cong J$ as $\mathcal{O}_K$-module

   The equivalence classes form a group (induced by ideal multiplication), i.e., $\forall I$ there exists J such that IJ is principal. This is called the ideal class group (attached to any Dedekind Domain). For rings of integers $\mathcal{O}_K$ it is a finite group.

3. The coordinate ring of a smooth irreducible plane curve C. Let $f \in \mathbb{C}[X, Y]$ be irreducible then $C = \{(a, b) \in \mathbb{C}^2 : f(a, b) = 0\}$. The coordinate ring of C is $R = \mathbb{C}[X, Y]/(f) = \mathbb{C}[x, y]$ with $f(x, y) = 0$. This is an integral domain (since f is irreducible)

   Claim R is a Dedekind Domain:

   - R is Noetherian (By the Hilbert Basis Theorem)
   - Every non-zero prime of R is maximal.

Proof. Let P be a prime of $\mathbb{C}[X,Y]$ with $P \supsetneqq (f)$. Let $g \in P \setminus (f)$, so $\gcd(f,g) = 1$. View $f, g \in \mathbb{C}(X)[Y]$ (as this as Euclidean property), then there exists $a, b \in \mathbb{C}(X)[Y]$ such that $af + bg = 1$. Write $a = \frac{a_1}{d}, b = \frac{b_1}{d}$ where $a_1, b_1 \in \mathbb{C}[X,Y]$ and $d \in \mathbb{C}[X]$, $d \neq 0$. So $a_1 f + b_1 g = d \Rightarrow$ the set of common zero of f, g has only finitely many x-coordinate (roots of d). So f, g have only finitely many common zeroes. In fact there is only <u>one</u> common zero, (x_0, y_0), (after some work) this implies $P = (X - x_0, Y - y_0)$ which is maximal. (Fill in the gaps yourself) □

- We'll show that every localization R_P is a DVR, where P a non-zero prime of R. Without loss of generality, $P = (x,y)$, i.e., P is associated to the point of $(0,0)$. P is smooth: $\frac{\partial f}{\partial X x}, \frac{\partial df}{\partial Y}$ do not vanish at $(0,0)$. So $f = aX + bY +$higher term, a, b not both zero. Without loss of generality, we can assume $a = 0$ and $b = 1$. So $Y = 0$ at the tangent to C at $(0,0)$. Now $f(X,Y) = Y \cdot G(X,Y) + X^2 H(X)$ with $G(0,0) = 1$. Module f we have $0 = y \cdot g + x^2 \cdot h$ where $g = G(x,y), h = h(x) \in R$. The maximal ideal of R_P is generated by x, y. $R_P = \{\frac{r(x,y)}{s(x,y)} | r, s \in R, s(0,0) \neq 0\}$. The maximal ideal PR_P is $\{\frac{r}{s} : r(0,0) = 0, s(0,0) \neq 0\}$, i.e., $r \in P$. But $yg = -x^2 h$ so $y = -x^2 \frac{h}{g}$ where $g(0,0) = 1 \neq 0$, so $-x^2 \frac{h}{g} \in R_P$. So x alone generates $P \cdot R_P$, hence R_P is a DVR.