Lecture Notes in Abstract Algebra

Lectures by Dr. Sheng-Chi Liu

Throughout these notes, □ signifies end proof, and ▲ signifies end of example.

Table of Contents

Notes by Jakob Streipel. Last updated August 15, 2020.

Lecture 1 Review of Groups, Rings, and Fields

1.1 Groups

Definition 1.1.1 (Group)**.** The set G equipped with a binary operation $\cdot$, together denoted $(G, \cdot)$, is a ***group*** if

(*i*) the operation is associative, i.e. $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ for all $g_1, g_2, g_2 \in G$;

(*ii*) there exists an identity element $e \in G$ such that $e \cdot g = g \cdot e = g$ for all g; and

(*iii*) for every $g \in G$ there exists an inverse denoted g^{-1} such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Note that these are the properties we require if we wish to be able to solve linear equations of the form $ax = b$. Note also that $\cdot$ being a binary operation very importantly implies that G is closed under $\cdot$, i.e., $g_1 \cdot g_2 \in G$ for all $g_1, g_2 \in G$.

Definition 1.1.2 (Abelian group)**.** A group $(G, \cdot)$ is called ***abelian*** if $g_1 \cdot g_2 = g_2 \cdot g_1$ for all $g_1, g_2 \in G$.

When a group is abelian we typically use $+$ to denote the group operation and 0 to denote the identity element. Moreover we write $-g$ instead of g^{-1}.

Remark 1.1.3. The groups we consider in this course will all be abelian (the hint's in the name—*commutative* algebra).

Examples 1.1.4. Some examples of groups are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ with the usual addition, the symmetric group of order n, $(S_n, \circ)$, polynomial rings, e.g. $(\mathbb{Z}[x], +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, etc. ▲

1.2 Rings

Definition 1.2.1 (Ring)**.** The set R equipped with two binary operations $+$ and $\cdot$, denoted $(R, +, \cdot)$, is a ***ring*** if

(*i*) $(R, +)$ is an abelian group;

(*ii*) it is closed under $\cdot$, i.e. $r_1 \cdot r_2 \in R$ for all $r_1, r_2 \in R$;

(*iii*) multiplication is associative, meaning that $(r_1 \cdot r_2) \cdot r_3 = r_1 \cdot (r_2 \cdot r_3)$ for all $r_1, r_2, r_3 \in R$; and

(*iv*) multiplication is distributive over addition, i.e. $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$ and $(r_2 + r_3) \cdot r_1 = r_2 \cdot r_1 + r_3 \cdot r_1$ for all $r_1, r_2, r_3 \in R$.

Remark 1.2.2. We again only consider commutative rings in this course. Moreover all rings we consider will be rings with identity, meaning that multiplication has a neutral element. Therefore we have the additional properties:

(*v*) $r_1 \cdot r_2 = r_2 \cdot r_1$ for all $r_1, r_2 \in R$; and

(*vi*) there exists $1 \in R$ such that $1 \cdot r = r \cdot 1 = r$ for all $r \in R$.

Date: August 22, 2017.

Remark 1.2.3. As already indicated in the note, $+$ is usually called addition and $\cdot$ is usually called multiplication, as per usual. In addition we often write $r_1 \cdot r_2$ as $r_1 r_2$ for convenience.

Remark 1.2.4. Finally note that when we use the term ***ring*** in this course we will always mean a commutative ring with identity.

Examples 1.2.5. Some examples of rings are $(\mathbb{Z}, +, \cdot)$ (as well as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, etc.) and $(\mathbb{Z}[x], +, \cdot)$. ▲

1.3 Fields

Definition 1.3.1 (Field)**.** A ***field*** F is a commutative ***division ring***, i.e. F is a commutative ring with identity and for each $a \neq 0$, $a \in F$ there exists an element $a^{-1} \in F$ such that $aa^{-1} = 1$.

Example 1.3.2. Note that the ring $(\mathbb{Z}, +, \cdot)$ referred to previously is *not* a field since it does not include inverses for all elements but -1 and 1. On the other hand $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ with the same operations are fields. ▲

Example 1.3.3. Let k be a field and let M be a maximal ideal of $k[x]$. Then $k[x]/M$ is a field.

This gives us an easy means of generating fields of prime power number of elements, since $k = \mathbb{Z}/p\mathbb{Z}$, p prime is of prime order. Now if we let $M = (f)$ where f is an irreducible polynomial in $k[x]$ of degree n, then $|k[x]/M| = p^n$. ▲

1.4 Motivation

Commutative algebra is the study of the structures of commutative rings and of modules, with their applications in algebraic geometry and algebraic number theory.

Example 1.4.1 (Algebraic number theory)**.** The structure of the ring of integers. First note that $\mathbb{Z} \subset \mathbb{Q}$ has the property that for $n \in \mathbb{Z}$ we have $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, with p_i being primes. In particular this factorisation is unique. This means that $\mathbb{Z}$ is a unique factorisation domain. Moreover all ideals in $\mathbb{Z}$, which are of the form $n\mathbb{Z}$, are principal. This means that $\mathbb{Z}$ is a principal ideal domain.

On the other hand consider $\mathbb{Z}[\sqrt{-5}]$, a group of algebraic integers. In this field we don't have unique factorisation, since for example $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, all factors of which are irreducible. Furthermore not all ideals are principal, consider e.g. $I = (2, 1 + \sqrt{-5})$. ▲

Example 1.4.2 (Algebraic geometry)**.** The structure of the set of solutions to

$$\begin{cases} x + 2y + 3z = 0 \\ 5x + y + 2z = 0 \end{cases}$$

in $\mathbb{R}^3$.

Let $V \subset \mathbb{R}^3$ be the set of solution. This has certain structure:

(*i*) $v_1 + v_2 \in V$ for all $v_1, v_2 \in V$;

(*ii*) $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$ for all $v_1, v_2, v_3 \in V$;

(*iii*) $0 \in V$ since the planes go through the origin;

(*iv*) if $v \in V$, then $-v \in V$;

(*v*) for $r \in R$ we have $r \cdot v \in V$ for all $v \in V$;

(*vi*) $(r_1 + r_2) \cdot v = r_1 \cdot v + r_2 \cdot v$ for all $r_1, r_2 \in R$ and $v \in V$;

(*vii*) $r \cdot (v_1 + v_2) = r \cdot v_1 + r \cdot v_2$ for all $r \in R$ and $v_1, v_2 \in V$;

(*viii*) $1 \cdot v = v$ for all $v \in V$.

Now this seems familiar: observations (*i*) through (*iv*) are the axioms of a group, meaning that solutions to these equations form a group, and observations (*v*) through (*viii*) are the axioms of a vector field! ▲

Remark 1.4.3. Of course for an abstract definition of vector space we do not need V to specifically be a subset of $\mathbb{R}^3$.

Remark 1.4.4. We only use the addition and multiplication; we did *not* use the division in the definition. Therefore we may replace the field R with a ring A. If we do this we get the definition of a ***module*** instead of a vector space.

Example 1.4.5. Replace the linear equations with polynomial equations of higher degree. Let k be a field and let $A \coloneqq k[x_1, x_2, \ldots, x_n]$. Further let $f(x_1, x_2, \ldots, x_n) \in A$.

Now calling $V(f) \coloneqq \{\, (a_1, a_2, \ldots, a_n) \in k^n \mid f(a_1, a_2, \ldots, a_n) = 0 \,\}$ is the solution set to $f(x_1, x_2, \ldots, x_n) = 0$.

The structure of $V(f)$ can be recovered by the quotient ring A/I where $I = (f) \subset A$. ▲

Example 1.4.6. Consider $f(x, y) = x \in \mathbb{R}[x, y]$. Then $V(f) = \{\, (0, y) \mid y \in \mathbb{R} \,\}$.

On the other hand if $g(x, y) = x^2$ we have $V(g) = \{\, (0, y) \mid y \in \mathbb{R} \,\}$. These look the same!

However the structure is subtly different, since for one of them we have a double root. Indeed $\mathbb{R}[x, y]/(x)$ has no nontrivial idempotent elements, whereas $\mathbb{R}[x, y]/(x^2)$ has some, for instance $\bar{x}$. ▲

Exercise 1.4.7. Let $p = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$. Let us now define the map $\phi\colon \mathbb{R}[x_1, x_2, \ldots, x_n] \to \mathbb{R}$ by $\phi(f) = f(p)$. Then

(*i*) ϕ is a ring homomorphism, and

(*ii*) $\ker \phi$ is the maximal ideal $M_p = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$.

This gives a correspondence between maximal ideals in $A = \mathbb{R}[x_1, x_2, \ldots, x_n]$ and the points of $\mathbb{R}^n$. In fact this correspondence is one-to-one by the Nullstellensatz.

Solution. First recall that for two rings R and S, a mapping $\phi\colon R \to S$ is a ring homomorphism if it preserves the ring structure, i.e.

(*i*) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$,

(*ii*) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$, and

(iii) $\phi(1_R) = 1_S$.

To see the first property, recall that the polynomial ring $\mathbb{R}[x_1, x_2, \ldots, x_n]$ is abelian, so by distributivity and commutativity we have for any two polynomials f and g that

$$\phi(f+g) = (f+g)(P) = f(P) + g(P) = \phi(f) + \phi(g)$$

and

$$\phi(fg) = (fg)(P) = f(P)g(P) = \phi(f)\phi(g).$$

For the final property simply note that $\phi(1) = 1$ since 1 does not depend on x and so evaluates to itself regardless of P.

To show that $\ker\phi$ is the ideal $M_P = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ we consider two steps: it is clear that $M_P \subset \ker\phi$ since M_P consists only of polynomials that can be written on the form

$$(x_1 - a_1)f_1 + (x_2 - a_2)f_2 + \ldots + (x_n - a_n)f_n \tag{1.4.1}$$

for polynomials $f_1, f_2, \ldots, f_n \in A$, and these of course all evaluate to 0 in $P = (a_1, a_2, \ldots, a_n)$.

That the other inclusion is also true requires a little more work. Since all of $x_i - a_i$ are monic, it means that we have a division algorithm for them. This means that we can write any $f \in A$ as

$$f(x_1, x_2, \ldots, x_n) = p_1(x_1, x_2, \ldots, x_n)(x_1 - a_1) + r_1(x_2, x_3, \ldots, x_n),$$

and in turn

$$r_1(x_2, x_3, \ldots, x_n) = p_2(x_2, x_3, \ldots, x_n)(x_2 - a_2) + r_2(x_3, x_4, \ldots, x_n),$$

and so on until

$$r_{n-1}(x_n) = p_n(x_n)(x_n - a_n) + r_n,$$

where finally r_n is a constant.

This means that we may write

$$f(x_1, x_2, \ldots, x_n) = p_1(x_1, x_2, \ldots, x_n)(x_1 - a_1) + p_2(x_2, x_3, \ldots, x_n)(x_2 - a_2) + \\ + \ldots + p_n(x_n)(x_n - a_n) + r_n,$$

and if $f \in \ker\phi$ then the left-hand side must be 0, which forces the constant r_n in the right-hand side to be 0 as well, and so if $f \in \ker\phi$ we can write it on the form (1.4.1), and therefore $\ker\phi \subset M_P$. Thus $\ker\phi = M_P$.

To see that this ideal is indeed maximal, note that since ϕ is surjective (it evaluates constants to themselves, so certainly it is), by the first isomorphism theorem we have

$$A/\ker\phi \cong \mathbb{R}.$$

But for any commutative ring with identity A, an ideal I of A is maximal if and only if A/I is a field.

Thus since $A/\ker\phi \cong \mathbb{R}$ is indeed a field, $\ker\phi = M_P$ is a maximal ideal. ♦

Lecture 2 More on Rings and Ideals

2.1 Ring Fundamentals

Definition 2.1.1 (Ring homomorphism)**.** Let A and B be two commutative rings with identity. A ***ring homomorphism*** is a map $\phi\colon A \to B$ such that the ring structure is preserved, i.e.

(*i*) $\phi(x+y) = \phi(x) + \phi(y)$ for all $x, y \in A$,

(*ii*) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in A$,

(*iii*) $\phi(1_A) = 1_B$.

Definition 2.1.2 (Ideal)**.** An ***ideal*** of a ring A is a subset $I \subset A$ such that

(*i*) I is an additive subgroup,

(*ii*) $aI \subset I$ for all $a \in A$.

The reason we might want to construct such a thing is to guarantee that A/I is a ring. Cf. quotients of groups, where we wish for the thing we divide by to be normal.

Remark 2.1.3. Let $I \subset A$ be an ideal of A. Then A/I inherits a ring structure from A, and we call A/I a ***quotient ring***. Secondly if $1 \in I$, then $I = (1) = A$, and the other way around.

In fact if I contains any unit, then I is the whole ring.

Definition 2.1.4 (Principal ideal)**.** An ideal I generated by one element x is called a ***principal ideal***, denoted $I = (x)$.

Proposition 2.1.5. *Let $\phi\colon A \to B$ be a ring homomorphism. Then*

(*i*) $\ker\phi$ *is an ideal of* A*;*

(*ii*) *if $I \subset A$ is an ideal, then the map $\phi\colon A \to A/I$ defined by $\phi(a) = a + I$ is a surjective homomorphism, with* $\ker\phi = I$*;*

(*iii*) *the map $\varphi\colon \{$ ideals in $A/I \} \to \{$ ideals in A containing $I \}$ defined by $\varphi(J) \coloneqq \phi^{-1}(J)$ is a one-to-one correspondence.*

Proof. For (*i*), take two elements x and y in the kernel of ϕ, meaning that $\phi(x) = \phi(y) = 0$. Then $x+y$ is also in the kernel, since $\phi(x+y) = \phi(x)+\phi(y) = 0 + 0 = 0$. In addition $\phi(ax) = \phi(a)\phi(x) = \phi(a)0 = 0$ for all $a \in A$. Ergo $\ker\phi$ is an ideal of A.

Next for (*ii*) we need to verify both that this ϕ is a homomorphism and that it is surjective, and finally that its kernel is I.

Firstly taking $x, y \in A$ we have $\phi(x+y) = (x+y)+I = (x+I)+(y+I) = \phi(x) + \phi(y)$, and likewise for $\phi(xy)$. Moreover $\phi(1_A) = 1_A + I = 1_{A/I}$.

To see that this is surjective, note that all elements of A/I can be written on the form $a + I$ for some $a \in A$, and it is clear.

The kernel is clearly I itself since the 0 element in A/I is I itself, and therefore the coset representative can be anything from I and nothing else.

Finally for (*iii*): Later. □

Date: August 24, 2017.

Definition 2.1.6 (Zero-divisor)**.** An element $x \neq 0$ in a ring A is called a ***zero-divisor*** if there exists some $A \ni y \neq 0$ such that $xy = 0$.

Example 2.1.7. Consider the ring $\mathbb{Z}/6\mathbb{Z}$. In this ring we have $2 \cdot 3 = 0$, despite $2 \neq 0$, $3 \neq 0$. ▲

Definition 2.1.8 (Integral domain)**.** A ring with no zero-divisors is called an ***integral domain***.

From this, the key property of integral domains is that we get cancellation laws. That is, if $ax = ay$ with $a \neq 0$, then this implies that $x = y$ since $a(x - y) = 0$, and since there are no zero divisors we must have $x - y = 0$.

Definition 2.1.9 (Nilpotency)**.** An element x in a ring A is called ***nilpotent*** if $x^n = 0$ for some $n > 0$.

Hence a nilpotent element is a special kind of zero-divisor, since $x^n = x \cdot x^{n-1} = 0$, but of course not all zero divisors are nilpotent.

Example 2.1.10. Consider the ring $\mathbb{Z}/n^2\mathbb{Z}$. Then $n^2 = 0$ despite $n \neq 0$.

Note moreover, in view of the previous claim, that the 2 in $\mathbb{Z}/6\mathbb{Z}$ from the previous example will never be 0 even if we take greater and greater powers of it. ▲

Definition 2.1.11 (Unit)**.** An element x in a ring A is called a ***unit*** if there exists some $y \in A$ such that $xy = 1$. We write $y = x^{-1}$.

Definition 2.1.12 (Field)**.** A ***field*** is a ring in which all nonzero elements are units.

Proposition 2.1.13. *Let A be a ring. The following are equivalent:*

(*i*) *A is a field.*

(*ii*) *The only ideals in A are $\{0\}$ and A.*

(*iii*) *Every homomorphism from A onto (meaning it's surjective) a nonzero ring B is one-to-one.*

Proof. For (*i*) implying (*ii*), clearly $\{0\}$ is an ideal regardless, and any ideal different from the trivial ideal would have to contain a nonzero element, and all nonzero elements of a field are units, so the ideal is the whole field.

For (*ii*) implying (*iii*), consider something...

Finally for (*iii*) implying (*i*), let $x \in A$ be any element. Define $\varphi\colon A \to A/(x)$ by $a \mapsto a + (x)$. This is surjective, as we've seen before, and so by (*iii*) φ is injective.

Therefore $\ker \varphi = (0)$ since only one element can map to 0 and that must then be 0, and therefore $(x) = (0)$ and thus $x = 0$. □

Definition 2.1.14 (Prime ideal)**.** An ideal $P \subset A$ is a ***prime ideal*** if $p \neq (1)$ and if $xy \in P$ then $x \in P$ or $y \in P$.

Cf. how if $p \mid xy$, with p a prime, then $p \mid x$ or $p \mid y$.

Definition 2.1.15 (Multiplicative set)**.** A subset S of a ring A is called a ***multiplicative set*** if $1 \in S$ and for all $x, y \in S$ we have $xy \in S$.

Exercise 2.1.16. An ideal P is prime if and only if $S = A \setminus P$ is a multiplicative set.

Solution. First let P be a prime ideal. We then need to show that $1 \in S$, which is clear by definition: since a prime ideal can't be (1) it mustn't contain 1, and so 1 is in the complement.

Moreover let $x, y \in S$. Now suppose $xy \notin S$. This means that $xy \in P$ instead, and since P is a prime ideal, this implies that $x \in P$ or $y \in P$. But if this is the case one of x or y (or maybe both) belong to *both* P and $A \setminus P$, which is clearly impossible, since they are disjoint.

Therefore we have a contradiction and so $xy \in S$, and therefore S is a multiplicative set.

For the converse, let $S = A \setminus P$ be a multiplicative set. Suppose $xy \in P$, meaning that $xy \notin S$. Now if both x and y are in S, then $xy \in S = A \setminus P$ since S is multiplicative, so that cannot be. Consequently at least one of x and y is in P, and so P is prime by definition. (We also know $P \neq (1)$ since by definition $1 \in S$.) ♦

Definition 2.1.17 (Maximal ideal)**.** An ideal $M \subset A$ is a ***maximal ideal*** if $M \neq A$ and there exists no ideal I such that $M \subsetneq I \subsetneq A$.

Proposition 2.1.18. (*i*) *P is a prime ideal if and only if A/P is an integral domain.*

(*ii*) *M is a maximal ideal if and only if A/M is a field.*

Remark 2.1.19. Since all fields are integral domains, but not the converse, we see from this that all maximal ideals are prime ideals, but not the other way around.

Proof. For (*i*), suppose P is a prime ideal, and consider the quotient ring A/P, consisting of $a + P$ for $a \in A$. Now suppose $(a + P)(b + P) = ab + P = 0 + P$, meaning that $ab \in P$. We need to show that either $a+P = 0+P$ or $b+P = 0+P$ so that there are no zero-divisors, or in other words $a \in P$ or $b \in P$.

But this is true directly by the definition of P being a prime ideal!

For the opposite directions we suppose that A/P is an integral domain, meaning that if $(a + P)(b + P) = ab + P = 0 + P$ (meaning that $ab \in P$), then either $a \in P$ or $b \in P$.

This is the definition of P being prime again, with the caveat that we haven't showed that $P \neq (1)$. But if $P = (1)$, then A/P is (isomorphic to) the zero ring, and the zero ring isn't an integral domain.

Next for (*ii*), we know that there exists a bijection between ideals of A/M and ideals of A containing M. But reading that last part carefully, if M is maximal there is no ideal of A containing M apart from A and M themselves, meaning that there are exactly two ideals of A/M. Now since a ring is always its own ideal and all rings also have the trivial ideal, if A/M has exactly two ideals it can only be A/M and $\{0\}$, and therefore it is a field.

The same argument works in reverse: if A/M is a field, then it has only $\{0\}$ and A/M as ideals, and so by the correspondence there is no ideal strictly between M and A, and so M is maximal. □

Definition 2.1.20 (Spectra)**.** (*i*) The ***prime spectrum*** or Spec of a ring A is the set of all prime ideals of A.

(*ii*) The ***maximal spectrum*** of m-spec of a ring A is the set of all maximal ideals of A.

Example 2.1.21. Let k be a field. Then $\mathrm{Spec}(k) = \{ 0 \} = \text{m-spec}(k)$. ▲

Example 2.1.22. We have $\mathrm{Spec}(\mathbb{Z}) = \{ 0 \} \cup \{ (p) \mid p \text{ prime} \}$. ▲

Example 2.1.23. Let k be a field and let $A = k[x]$. Then $\mathrm{Spec}(A) = \{ 0 \} \cup \{ (f) \mid f \text{ irreducble polynomial in } A \}$, since k is a field meaning that $A = k[x]$ is a Euclidean domain. ▲

2.2 Review of Zorn's Lemma

Let Σ be a ***partially ordered set*** and let $S \subset \Sigma$ be a ***totally ordered*** subset.

An ***upper bound*** of S is an element $u \in \Sigma$ such that $s < u$ for all $s \in S$.

A ***maximal element*** of Σ is an element $m \in \Sigma$ such that $m < s$ does not hold for any $s \in \Sigma$.

Example 2.2.1. Let $\Sigma = \{ A \mid A \subset \mathbb{R} \}$, ordered by inclusion. Then $S = \{ (-m, m) \mid m \in \mathbb{Z}^+ \}$ is a totally ordered subset. ▲

Lemma 2.2.2 (Zorn's lemma)**.** *Let $\Sigma \neq \varnothing$ be a partially ordered set. Suppose any totally ordered subset $S \subset \Sigma$ has an upper bound in Σ. Then Σ has a maximal element.*

Remark 2.2.3. Zorn's lemma, the axiom of choice, and the well-ordering principle are all equivalent.

Theorem 2.2.4 (Existence of maximal ideal)**.** *Let A be a ring and $I \subsetneq A$ be an ideal. Then there exists a maximal ideal M in A containing I.*

Proof. Let Σ be the set of ideals $J \subsetneq A$ containing I, ordered by inclusion. Then $\Sigma \neq \varnothing$ since at least $I \in \Sigma$.

For any totally ordered subset $S = \{ J_\lambda \mid \lambda \in \Lambda \} \subset \Sigma$ define $J^* = \bigcup_{\lambda \in \Lambda} J_\lambda$. Two points of order: $J^* \neq A$ since none of J_λ contain 1 (otherwise they'd be all of A, which is not true by assumption) and secondly J^* is an ideal since J_λ are totally ordered, ergo the union is one of the elements itself!

Now J^* is clearly an upper bound of S since it contains all of S.

Therefore by Zorn's lemma, Σ has a maximal element M, and thus M is a maximal ideal containing I. □

Corollary 2.2.5. *Every non-unit element of A is contained in a maximal ideal.*

Proof. If a is the non-unit element, consider the maximal ideal containing the ideal (a). By the previous theorem this maximal ideal exists. □

Corollary 2.2.6. *Let A be a ring and let $A^\times$ be the set of units in A. Then $A = A^\times \sqcup \bigcup_\lambda M_\lambda$, where M_λ are the maximal ideals and $\sqcup$ denotes a disjoint union.*

Lecture 3 Ideals and Radicals

3.1 More on Prime Ideals

Theorem 3.1.1. *Let A be a ring and S a multiplicative subset of A. Let I be an ideal of A with $I \cap S = \varnothing$ (i.e. they are disjoint). Then there exists a prime ideal P of A containing I, and $P \cap S = \varnothing$.*

Remark 3.1.2. So with $I = (0)$, any multiplicative set yields a prime ideal.

Proof. Let $\Sigma = \{ J \text{ ideal of A} \mid J \supset I, J \supset S = \varnothing \}$, which is partially ordered by inclusion. Since each totally ordered subset is a chain, they have a maximal element which is also an ideal, and so we may apply Zorn's lemma, which tells us that Σ has a maximal element P.

We now claim that P is prime. To see this, take $a, b \notin P$, in which case we need to show that $ab \notin P$.

Consider the ideals $J_1 = P + (a)$ and $J_2 = P + (b)$, where $J_1, J_2 \subsetneq P$ since $a, b \notin P$. This implies that $J_i \cap S \neq \varnothing$ for $i = 1, 2$. Now suppose $p + ac_1 \in S$ and $q + bc_2 \in S$ for $p, q \in P$ and $c_1, c_2 \in A$. Then

$$S \ni (p + ac_1)(q + bc_2) = \underbrace{pq + pbc_2 + ac_1 q}_{\in P} + abc_1c_2.$$

Thus if $ab \in P$ this product is in $P \cap S$, but this is a contradiction since $P \cap S = \varnothing$. Therefore $ab \notin P$ and so P is prime. □

3.2 Local Rings

Recall that we can decompose any ring A as $A = A^\times \sqcup (\bigcup_\lambda m_\lambda)$ where m_λ are all the maximal ideals of A. We are interested in the case when $A = A^\times \sqcup M$, i.e. A has exactly one maximal ideal.

Definition 3.2.1 (Local ring)**.** A ring A with exactly one maximal ideal M is called a ***local ring***.

The field $k = A/M$ is called the ***residue field*** of A.

Proposition 3.2.2. *The following are equivalent:*

(*i*) *A is a local ring (i.e. has exactly one maximal ideal).*

(*ii*) *The set of all non-units of A form an ideal.*

(*iii*) *A has a maximal ideal M such that $1 + M \subset A^\times$, i.e. $1 + x \in A^\times$ for all $x \in M$.*

Proof. For (*i*) implying (*ii*), we remark that the set of all non-units is M since we know by assumption that $A \setminus A^\times = M$, which is a maximal ideal, so it is certainly an ideal.

For (*ii*) implying (*iii*), note that $1 + x \notin A^\times$ implies that $1 + x \in M$, where we let M be the set of all non-units, and $x \in M$ implies that $1 \in M$, which is

Date: August 29, 2017.

a unit so $1 + x \in A^\times$. This M is an ideal by assumption, and it is maximal by the decomposition.

Finally for (iii) implying (i), we need to show that for any $x \in A \setminus M$, x is a unit. Since M is maximal, the ideal generated by M and x is A (since the only ideal containing M and being bigger than M must be A, by the maximality of M). This implies that $1 = xy + t$ for some $y \in A$ and $y \in M$, which rearranged gives $xy = 1 - t \in 1 + M \subset A^\times$, whereby x is a unit. □

Definition 3.2.3 (Semi-local ring)**.** A ring with only a *finite* number of maximal ideals is called ***semi-local***.

Example 3.2.4. Consider

$$\mathbb{Z}_{(2)} = \{\, q \in \mathbb{Q} \mid q = a/b, a, b \in \mathbb{Z}, \gcd(a, b) = 1, 2 \nmid b \,\}.$$

In there $q = a/b$ is a unit if and only if $2 \nmid a$, meaning that $q^{-1} = b/a \in \mathbb{Z}_{(2)}$. Hence the set of all non-units of $\mathbb{Z}_{(2)}$ is the set $\{\, a/b \in \mathbb{Z}_{(2)} \mid 2 \mid a \,\}$, and

$$1 + \frac{a}{b} = \frac{b + a}{b}$$

so $2 \nmid b + a$ implies that $1 + a/b$ is a unit. Therefore $\mathbb{Z}_{(2)}$ is a local ring with maximal ideal $2\mathbb{Z}_{(2)}$, so

$$\frac{\mathbb{Z}_{(2)}}{2\mathbb{Z}_{(2)}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} = \mathbb{F}_2.$$

▲

The above is a special case of what is called localisation.

3.3 Radicals

Definition 3.3.1 (Nilradical)**.** Let A be a ring. The set of all nilpotent elements of A is called the ***nilradical***, denoted $\mathcal{R}$ or $\operatorname{nilrad}(A)$.

We will show in a moment that, interesting, this is the intersection of all prime ideals of A.

Proposition 3.3.2. *Let A be a ring. Then* $\operatorname{nilrad}(A)$ *is an ideal and the quotient* $A/\operatorname{nilrad}(A)$ *has no nonzero nilpotent elements.*

Proof. If $x, y \in \operatorname{nilrad}(A)$, meaning that $x^n = 0$ and $y^m = 0$ for some $n, m > 0$, then $(x + y)^{n+m} = 0$, whereby $x + y \in \operatorname{nilrad}(A)$. Similarly if $a \in A$ and $x \in \operatorname{nilrad}(A)$, then $(ax)^n = a^n x^n = a^n \cdot 0 = 0$, so $ax \in \operatorname{nilrad}(A)$. Hence $\operatorname{nilrad}(A)$ is an ideal of A.

Now let $\bar{x} \in A/\operatorname{nilrad}(A)$, and suppose $\bar{x}^n$, implying that $\overline{x^n} = 0$. This means that $x^n \in \operatorname{nilrad}(A)$, whence $(x^n)^m = 0$, or $x^{nm} = 0$, so $x \in \operatorname{nilrad}(A)$, meaning that $\bar{x} = \bar{0} \in A/\operatorname{nilrad}(A)$. □

Proposition 3.3.3. *Let A be a ring. Then*

$$\operatorname{nilrad}(A) = \bigcap_{P \in \operatorname{Spec}(A)} P.$$

Proof. Let $I = \bigcap_{P \in \mathrm{Spec}(A)} P$. We claim that $\mathrm{nilrad}(A) \subset I$. If $x \in \mathrm{nilrad}(A)$, then $x^n = 0 \in P$ for every $P \in \mathrm{Spec}(A)$, by P being prime. Therefore $x \in P$ for all $P \in \mathrm{Spec}(A)$, and so $\mathrm{nilrad}(A) \subset I$.

For the other inclusion, note that $x \in I$ implying $x \in \mathrm{nilrad}(A)$ is equivalent with $x \notin \mathrm{nilrad}(A)$ implying $x \notin I$. Therefore it suffices to show that for $x \in \mathrm{nilrad}(A)$, there exists a prime ideal P such that $x \notin P$.

Consider $\{ x^n \mid n \geq 0 \}$, a multiplicative set. By the first theorem of the lecture, since $(0) \cap S = \varnothing$ there exists a prime ideal P such that $P \cap S = \varnothing$. Now $0 \notin S$ since x assumed not nilpotent, and therefore $x \notin P$, since $x \in S$. □

Example 3.3.4. By this intersection, $\mathrm{nilrad}(\mathbb{Z}) = \{ 0 \}$. ▲

Definition 3.3.5 (Jacobson radical)**.** Let A be a ring. Then

$$J(A) = \bigcap_{m \in \text{m-spec}(A)} m$$

is called the ***Jacobson radical*** of A.

We can classify the Jacobson radical quite interestingly:

Proposition 3.3.6. *Let A be a ring. Then $x \in J(A)$ if and only if $1 - xy \in A^\times$ for every $y \in A$.*

Proof. For the left implication, suppose $1 - xy$ is not a unit. Then $1 - xy \in M$ for some maximal ideal M, by partition. Since $x \in J(A) \subset M$, this implies that $1 \in M$, which is impossible for a maximal ideal.

For the right implication, suppose $x \notin M$ for some maximal ideal M. Note that the ideal generated by M and x is A since M is maximal. Therefore $xy + u = 1$ for some $y \in A$ and $u \in M$, which rearranged yields $u = 1 - xy \in A^\times$ by assumption. Therefore $M = A$, which is impossible! □

Remark 3.3.7. In a local ring, $J(A)$ is not very useful, since $J(A) = M$. Note also that $1 - xy \in A^\times$ in general rings, versus $1 + x \in A^\times$ in local rings.

Lecture 4 Ideals

4.1 Operations on Ideals

Let I, J be two ideals in a ring A. We define

$$I + J \coloneqq \{ x + y \mid x \in I, y \in J \}$$

to be the smallest ideal containing I and J.

Similarly we define IJ to be the ideal generated by xy for all $x \in I$ and $y \in J$.

Example 4.1.1. Let $A = \mathbb{Z}$. Since this is a principal ideal domain, we have $I = (m)$ and $J = (n)$ for some $m, n \in \mathbb{Z}$. Then $I + J = (k)$ where $k = \gcd(m, n)$, $IJ = (mn)$, and $I \cap J = (h)$, where $h = \mathrm{lcm}(m, n)$. ▲

Date: August 31, 2017.

Note that in the above example, $I \cap J = IJ$ if and only if m and n are relatively prime. This gives us a general definition of the notion of coprime ideals:

Definition 4.1.2 (Coprime)**.** Two ideals I and J of a ring A are said to be ***coprime*** if $I + J = A$, in which case $I \cap J = IJ$.

Let A be a ring and $I_1, I_2, \ldots, I_n$ be ideals of A. Define the map

$$\phi\colon A \to \prod_{i=1}^{n} \frac{A}{I_i}$$

by $\phi(x) = (x + I_1, x + I_2, \ldots, x + I_n)$.

This is a ring homomorphism, and clearly it's injective precisely if $\ker \phi = \bigcap_{i=1}^{n} I_i = (0)$.

This gives us another generalisation of a familiar concept from elementary number theory:

Proposition 4.1.3 (Chinese remainder theorem)**.** *Let A be a ring and I_i and ϕ be defined as above. Then*

(*i*) *ϕ is surjective if and only if I_i and I_j are coprime for all $i \neq j$,*

(*ii*) *ϕ is injective if and only if $\bigcap_{i=1}^{n} I_i = (0)$.*

Proof. For the forward direction of (*i*) we need to show that I_1 and I_2 are coprime, given that ϕ is surjective. Now surjectivity implies that there exists some $x \in A$ such that $\phi(x) = (1, 0, 0, \ldots, 0)$, which means that $x \equiv 1 \pmod{I_1}$ and $x \equiv 0 \pmod{I_2}$, so

$$1 = \underbrace{(1 - x)}_{\in I_1} + \underbrace{x}_{\in I_2} \in I_1 + I_2,$$

hence $I_1 + I_2 = A$ since it contains a unit (1 in particular), and therefore I_1 and I_2 are coprime. Clearly the same general argument holds for any pair I_i, I_j, for $i \neq j$.

For the converse it suffices to show that there exists some $x \in A$ such that $\phi(x) = (1, 0, \ldots, 0)$. Since $I_1 + I_i = (1) = A$ for each $i = 2, 3, \ldots, n$, there exists some $u_i + v_i = 1$ with $u_i \in I_1$ and $v_i \in I_i$.

Now take

$$x = \prod_{i=1}^{n} (1 - u_i) = \prod_{i=2}^{n} v_i$$

where the latter is in I_k for all $k = 2, 3, \ldots, n$. Therefore $x \equiv 1 \pmod{I_1}$ and $x \equiv 0 \pmod{I_k}$, for $k \geq 2$, whereby $\phi(x) = (1, 0, \ldots, 0)$.

Since the same thing can be constructed for a 1 in any position, and since they generate the whole space, we have surjectivity.

For (*ii*) simply note that $\ker \phi = \bigcap_{i=1}^{k} I_i$, and by a previous proposition ϕ is injective if and only if $\ker \phi = (0)$. □

Proposition 4.1.4. (*i*) *Let $P_1, P_2, \ldots, P_n$ be prime ideals. Let $I \subset \bigcup_{i=1}^{n} P_i$ be an ideal. Then $I \subset P_i$ for some i.*

(*ii*) *Let $I_1, I_2, \ldots, I_n$ be ideals. Suppose there exists a $P \supset \bigcap_{i=1}^{n} I_i$ be a prime ideal. Then $P \supset I_i$ for some i. Hence if $P = \bigcap_{i=1}^{n} I_i$, then $P = I_i$ for some i.*

Proof. Next time! □

Lecture 5 Radicals and Modules

First we present the proof of the proposition stated last lecture.

Remark 5.0.1. Note first of all that if $I \subset (J_1 \cup J_2)$, all being ideals, then $I \subset J_1$ or $I \subset J_2$, even if J_1 and J_2 aren't prime.

Proof. (*i*) is equivalent to saying that if $I \not\subset P_i$ for every i, then $I \not\subset \bigcup_{i=1}^{n} P_i$.

We prove this by induction on n. The case of $n = 1$ is trivially true, and so assume the statement true for $n - 1$.

For n, consider choose an element x_1 that isn't in the union of $P_2 \cup P_2 \cup \ldots \cup P_n$, with $x_1 \in I$. Similarly choose an element x_2 in the union of all P_i except P_2, with $x_2 \in I$, and so on, until x_n in the union of all P_i but the last one, with $x_n \in I$ as well.

Now if $x_i \notin P_i$ for some i, then $x_i \notin P_1 \cup P_2 \cup \ldots \cup P_n$. Hence assume that $x_i \in P_i$ for all $i = 1, 2, \ldots, n$.

Consider

$$y = \sum_{i=1}^{n} x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n.$$

Then $y \in I$ since by construction all $x_i \in I$. Now consider y modulo P_i,

$$y \equiv x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n \not\equiv 0 \pmod{P_i}$$

since that is the only summand not containing x_i, and all factors in that summand don't belong to P_i by construction. Moreover P_i is a prime ideal, so if a product is in it, one factor must be, but none of the factors are so the product can't be.

Ergo, $y \notin P_i$ for every $i = 1, 2, \ldots, n$. This therefore implies that $I \not\subset \bigcup_{i=1}^{n} P_i$.

(*ii*) Assume $P \not\supset I$ for all $i = 1, 2, \ldots, n$. Then there exists some $x_i \in I_i$ with $x_i \notin P$ for every $i = 1, 2, \ldots, n$.

Now consider

$$\prod_{i=1}^{n} x_i \in \bigcap_{i=1}^{n} I_i \subset P$$

since I_i are ideals contained in P, and since P is prime, one of the factors x_i must be in P, which is a contradiction.

Date: September 5, 2017.

Finally, if

$$P = \bigcap_{i=1}^{n} I_i,$$

then

$$I_i \subset P = \bigcap_{i=1}^{n} I_i \subset I_i$$

for some i, meaning that $P = I_i$. □

5.1 Ideal Quotients

Definition 5.1.1 (Ideal quotient)**.** Let I and J be ideals in a ring A. Their ***ideal quotient*** is

$$(I : J) = \{\, x \in A \mid xJ \subset I \,\}.$$

Proposition 5.1.2. *The ideal quotient $(I : J)$ is an ideal of A.*

Proof. Take an element $x \in (I : J)$, meaning that $xJ \subset I$. Then xJ are all elements of an ideal, and ideals are closed under multiplication from any element $a \in A$, so $axJ \subset I$ as well.

Moreover let $y \in (I : J)$. Then $x + y \in (I : J)$ since $(x + y)J \subset I$ since xJ and yJ are. □

Definition 5.1.3 (Annihilator)**.** Given an ideal I in a ring A, the ***annihilator*** of I is

$$\operatorname{Ann}(I) = (0 : I) = \{\, x \in A \mid xI = 0 \,\}.$$

Note for the record that if $J = (x)$ is a principal ideal, then we will write $(I : J) = (I : x)$.

Remark 5.1.4. The set of all zero divisors in A is

$$F = \bigcup_{x \neq 0} \operatorname{Ann}(x).$$

Example 5.1.5. Let $A = \mathbb{Z}$, and take, say, $I = (144)$ and $J = (12)$. Then $(I : J) = (144 : 12) = (12) = 12\mathbb{Z}$.

In general, if $I = (m)$ and $J = (n)$, then $(I : J) = (k)$ with $k = m/\gcd(m, n)$. ▲

5.2 Radical of an Ideal

Definition 5.2.1 (Radical)**.** Let I be an ideal of A. The ***radical*** of I is

$$\operatorname{rad}(I) = \{\, x \in A \mid x^n \in I \text{ for some } n > 0 \,\}.$$

Some authors prefer the notation $\mathrm{r}(I)$ of $\sqrt{I}$.

Example 5.2.2. We have $\operatorname{nilrad}(A) = \operatorname{rad}(0)$.

Moreover by the natural homomorphism $\phi\colon A \to A/I$. Then since this is surjective,

$$\operatorname{rad}(I) = \phi^{-1}(\operatorname{nilrad}(A/I))$$

is well-defined, and we are taking pre-images of elements that are all nilradical in the quotient, they are in I for the same power that made them 0 in the quotient. By a proposition of homomorphisms from the beginning of this course, this is an ideal. ▲

Definition 5.2.3 (Radical ideal)**.** An ideal I of a ring A is called a ***radical ideal*** if $I = \operatorname{rad}(I)$.

Proposition 5.2.4. *Given a ring A with an ideal I, we have*

$$\operatorname{rad}(I) = \bigcap_{\substack{P \in \operatorname{Spec}(A) \\ P \supset I}} P.$$

Proof. Let $\phi\colon A \to A/I$ be the natural homomorphism. Note that the prime ideals of A containing I are exactly the ideals $\phi^{-1}(Q)$ with Q prime ideal in A/I (this since ideals are one-to-one, and the homomorphism preserves multiplication, and so preserved primality of ideals).

Therefore

$$\operatorname{nilrad}(A/I) = \bigcap_{Q \in \operatorname{Spec}(A/I)} Q,$$

and by the above argument taking pre-images yields

$$\operatorname{rad}(I) = \phi^{-1}(\operatorname{nilrad}(A/I)) = \bigcap_{\substack{P \in \operatorname{Spec}(A) \\ P \supset I}} P. \qquad \square$$

5.3 Modules

Definition 5.3.1 (Module)**.** Let A be a ring. An ***A-module*** is an abelian group M with a multiplication map

$$\begin{aligned} \cdot \ : A \times M &\to M \\ (a \cdot x) &\mapsto ax \end{aligned}$$

satisfying

(*i*) $a(x+y) = ax + ay$ for all $a \in A$ and $x, y \in M$,

(*ii*) $(a+b)x = ax + bx$ for all $a, b \in A$ and $x \in M$,

(*iii*) $(ab)x = a(bx)$ for all $a, b \in A$ and $x \in M$,

(*iv*) $1_A x = x$ for $1_A \in A$ and all $x \in M$.

Remark 5.3.2. If $A = k$ is a field, then a module M over A is a vector space over k.

Remark 5.3.3. In a module, we might not have a basis. We do, however, have a basis if the module is over a principal ideal domain.

Example 5.3.4. An ideal I of a ring A is an A-module. ▲

Example 5.3.5. Any module over $\mathbb{Z}$ is an abelian group. ▲

Definition 5.3.6 (Homomorphism of module)**.** Let M, N be A-modules. A mapping $f\colon M \to N$ is an ***A-module homomorphism*** or an ***A-linear map*** if

(*i*) $f(x+y) = f(x) + f(y)$ for every $x, y \in M$,

(*ii*) $f(ax) = af(x)$ for every $a \in A$ and $x \in M$.

Remark 5.3.7. If $A = k$ is a field, then an A-module homomorphism is a linear transformation of vector spaces.

Proposition 5.3.8. *Let M, N be A-modules, and $f\colon M \to N$ be a homomorphism between them. Then*

(*i*) $\ker f \subset M$ *is a submodule of* M *and* $\operatorname{im} f \subset N$ *is a submodule of* N*,*

(*ii*) $M/\ker f \cong \operatorname{im} f$*.*

The proofs of these are exactly the same as the proofs for linear maps in vector spaces.

Definition 5.3.9 (Quotient module)**.** Let M be an A-module and let $N \subset M$ be a submodule. Then M/N is an A-submodule defined by

$$a(x+N) = (ax) + N$$

for $a \in A$ and $x \in M$.

Theorem 5.3.10 (Isomorphism theorems)**.** *Let A be a ring.*

(*i*) *If $L \subset M \subset N$ are all A-modules, then*

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

(*ii*) *If $M, N \subset L$ are submodules, then*

$$\frac{M+N}{N} \cong \frac{M}{M \cap N}.$$

Remark 5.3.11. If $N \not\subset M$, then M/N makes no sense. There are two natural ways to resolve this: either enlarge M to contain N (giving $M + N$ as the smallest alternative), or shrink N until it is contained in M (yielding $M \cap N$). (*ii*) above says that these are equivalent.

Proof. (*i*) Define $\varphi\colon L/N \to L/M$ by $\varphi(x+N) = x + M$. This is well-defined (i.e. doesn't depend on the choice of coset representative) since if $x+N = y+N$ we have $x - y \in N \subset M$ and therefore

$$\varphi(x+N) = x + M = y + M = \varphi(y+N).$$

By definition of coset operations, φ is A-linear and surjective.

If we can now show that $\ker \varphi = M/N$, then we are done by the Isomorphism theorem. To see this, consider $x+N \in \ker \varphi$, if and only if $\varphi(x+N) = x+M = M$ if and only if $x \in M$.

(*ii*) The strategy is to construct a homomorphism from M to $(M+N)/N$ that is surjective and has $M \cap N$ as its kernel.

Consider

$$\psi \colon M \hookrightarrow M+N \to \frac{M+N}{N}.$$

Now $\ker \psi = M \cap N$ since the elements in the kernel must be elements of N, and since everything is from M only the intersection suffices. Moreover it is surjective since elements in $(M+N)/N$ are of the form $m+n+N = m+N$ since $n \in N$, and so by the Isomorphism theorem we're done. □

Lecture 6 Generating Sets

6.1 Faithful Modules and Generators

Recall that if V and W are vector spaces over a field k, then the set of all linear transformations $f \colon V \to W$ is itself a k-vector space. The same thing is true for modules:

Proposition 6.1.1. *Let M, N be A-modules. Let*

$$\operatorname{Hom}(M,N) \coloneqq \{\, f \colon M \to N \mid f \text{ is an } A\text{-modle homomorphism} \,\}.$$

Then $\operatorname{Hom}(M,N)$ *is also an A-module with*

$$(f+g)(x) \coloneqq f(x) + g(x)$$

and

$$(af)(x) \coloneqq af(x)$$

for all $x \in M$ and $a \in A$.

The proof of this is straightforward computation.

Exercise 6.1.2. Show that $\operatorname{Hom}(A, M) \cong M$.

We have several objects in modules that are completely analogous to that of rings.

Definition 6.1.3 (Module quotient)**.** Let N, P be submodules of a module M over a ring A. We call

$$(N : P) \coloneqq \{\, a \in A \mid aP \subset N \,\}$$

a ***module quotient***, which is an ideal of A.

Definition 6.1.4 (Annihilator)**.** The ***annihilator*** of a module M over a ring A is

$$\operatorname{Ann}(M) \coloneqq (0 : M) = \{\, a \in A \mid aM = 0 \,\}.$$

Note that if $I \subset \operatorname{Ann}(M)$ with I an ideal, then M is an A/I-module: if $\bar{a} \in A/I$, then $\bar{a}x \coloneqq ax$ for $x \in M$. This is well-defined because $(a+I)M = aM + IM = aM$, since I is inside the annihilator of M.

Definition 6.1.5 (Faithful module)**.** Let A be a ring. An A-module M is called ***faithful*** is $\operatorname{Ann}(M) = 0$.

Exercise 6.1.6. If $\operatorname{Ann}(M) = I$, then M is a faithful A/I-module.

Date: September 7, 2017.

6.2 Generators of a Module

Given an A-module M and $x_1, x_2, \ldots, x_k \in M$, consider

$$(x_1, x_2, \ldots, x_k) \coloneqq \sum_{i=1}^{k} Ax_i = \left\{ \sum_{i=1}^{k} a_i x_i \;\middle|\; a_i \in A \right\}$$

is a submodule of M.

This becomes harder to think about if we're indexing over a set I that isn't finite, or even countable.

If

$$M = \sum_{i \in I} Ax_i = \left\{ \sum_{i \in I} a_i x_i \;\middle|\; a_i \in A, a_i \neq 0 \text{ only for finitely many } i \right\}$$

then we call $\{ x_i \}_{i \in I}$ a ***set of generators*** of M.

A module M is called a ***finitely generated*** A-module if it has a finite set of generators.

Definition 6.2.1 (Direct sum, Direct product)**.** Let M, N be A-modules. The ***direct sum***

$$M \oplus N \coloneqq \{ (x, y) \mid x \in M, y \in N \}$$

is an A-module with addition and scalar multiplication defined by

$$(x_1, y_1) + (x_2, y_2) \coloneqq (x_1 + x_2, y_1 + y_2)$$

and

$$a(x, y) \coloneqq (ax, ay).$$

If $(M_i)_{i \in I}$ is a family of A-modules, their ***direct sum***

$$\bigoplus_{i \in I} M_i = \{ (x_i)_{i \in I} \mid x_i \in M_i, x_i \neq 0 \text{ only for finitely many } i \}.$$

The ***direct product*** is

$$\prod_{i \in I} M_i = \{ (x_i)_{i \in I} \mid x_i \in M_i \}.$$

Note that if $|I| < \infty$, then these coincide.

Let I be an index set. Then we write

$$A^{|I|} \coloneqq \{ (a_i)_{i \in I} \mid a_i \in A, a_i \neq 0 \text{ only for finitely many } i \}.$$

Consider $(x_i)_{i \in I} \subset M$. Define $\varphi \colon A^{|I|} \to M$ by

$$(a_i)_{i \in I} \mapsto \sum_{i \in I} a_i x_i$$

(cf. how $(a_1, a_2, \ldots, a_n)$ corresponds to $a_1 v_1 + a_2 v_2 + \ldots a_n v_n$ in vector spaces).

Note that if φ is surjective, then $\{ x_i \}_{i \in I}$ is a set of generators of M.

Definition 6.2.2 (Free module, Basis)**.** An A-module M is said to be ***free*** is φ is an isomorphism and $\{ x_i \}_{i \in I}$ is called a ***basis*** of M. In this case $M \cong A^{|I|}$.

In particular, a finitely generated free A-module is isomorphic to A^n.

Example 6.2.3. Let A be a ring. Take $I \neq (0) \subset A$, an ideal. Then A/I is an A-module, finitely generated by $\bar{1} = 1 + I$. However $A/I \ncong A$ and so A/I is not free. ▲

Example 6.2.4. Let $A = k[x, y]$, with k a field. Let $M = (x, y)$, which is a maximal ideal of A. This maximal ideal M is an A-module, but M is not free (x and y are linearly independent, but they do not produce a basis: consider for example $xy \in M$). The map $\varphi \colon A^2 \to M$ by $(a, b) \mapsto ax + by$ has the kernel $\ker \varphi = \{ (cy, -cx) \mid c \in A \} \neq 0$, and by the first isomorphism theorem $A^2 / \ker \varphi \cong M$. ▲

Astonishingly, this is the only type of isomorphisms we have:

Proposition 6.2.5. *Let A be a ring. M being a finitely generated A-module is equivalent with M being isomorphic to a quotient of A^n for some $n > 0$.*

Proof. Let $\{ x_1, x_2, \ldots, x_n \}$ be generators of M. The map $\phi \colon A^n \to M$ defined by

$$\phi(a_1, a_2, \ldots, a_n) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$$

is surjective since $\{ x_1, x_2, \ldots, x_n \}$ is a generating set. Hence $A^n / \ker \phi \cong M$.

For the converse, if $M \cong A^n / I$, consider $\phi \colon A^n \to A^n / I \cong M$. Then $\{ \phi(e_i) \}_{i=1}^n$, with $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the ith position is a set of generators of M. □

Recall the Cayley-Hamilton theorem from linear algebra. It says that the characteristic polynomial of a matrix evaluates to 0 in that matrix itself.

We have something similar for modules.

Proposition 6.2.6. *Let M be a finitely generated A-module (generated by n elements). Let $I \subset A$ be an ideal, and let $\phi \colon M \to M$ be an A-module homomorphism such that $\phi(M) \subset IM$. Then ϕ satisfies an equation of the form*

$$\phi^n + a_1 \phi^{n-1} + \ldots + a_n = 0$$

where $a_i \in I^i$ for $i = 1, 2, \ldots, n$.

Lecture 7 Finding Generators

7.1 Generalising Cayley-Hamilton's Theorem

We start by proving the proposition stated at the end of the last lecture.

Proof. Let $x_1, x_2, \ldots, x_n$ be a set of generators of M. Then $\phi(x_i) \in IM$ and so

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j$$

Date: September 12, 2017.

with $a_{ij} \in I$ since $x_1, x_2, \ldots, x_n$ generate M. Rearranging we therefore have

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})x_j = 0$$

which we can write in matrix form[1] as

$$\begin{pmatrix} \phi - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \phi - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & a_{n2} & \cdots & \phi - a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{7.1.1}$$

We treat the matrix on the left-hand side as a matrix Δ with elements from $\mathrm{End}(M)$, the set of ***endomorphisms*** of M, i.e. homomorphisms from M to itself.

Recall how in linear algebra, i.e. in a vector space, we have that $A^{-1} = 1/\det(A)A^*$, where A^* is the adjoint of A. Rearranging this we have $A^*A = \det(A)I_n$, where notably we only require multiplication, addition, and subtraction to compute the adjoint, meaning that this latter statement is true in a ring as well.

Therefore let Δ^* denote the adjoint matrix of Δ. Then $\Delta^*\Delta = \det(\Delta)I_n$.

Now multiply both sides of (7.1.1) by Δ^*, yielding

$$\det(\Delta)I_n \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

which in turn means that $\det(\Delta)x = 0$ for all $x \in M$ since $x_1, x_2, \ldots, x_n$ generate M.

Expanding the determinant of Δ we get the polynomial required in the proposition, and noting that the coefficient in front of ϕ^{n-k} has k elements from I, we clearly have $a_i \in I^i$ as requested. □

Using this we can in fact prove a generalisation of Cayley-Hamilton's theorem on modules.

Theorem 7.1.1 (Cayley-Hamilton)**.** *Let A be a commutative ring with unity. Let $N = (a_{ij})$ be an $n \times n$ matrix with entries $a_{ij} \in A$. Moreover let $P_N(x) = \det(xI_n - N)$ be the characteristic polynomial of N.*

Then $P_N(N) = 0$.

Proof. Let $M = A^n$, an A-module. Define $\phi\colon M \to M$ by $\phi(x) = Nx$. Then $\phi(M) \subset AM$, and so by the proposition $P_N(N) = \det \Delta = 0$. □

Corollary 7.1.2. *Let M be a finitely generated A-module. Let $I \subset A$ be an ideal such that $IM = M$. Then there exists some $x \equiv 1 \pmod{I}$ such that $xM = 0$.*

[1] Note that matrix form isn't unique in a module, but still something we can work with.

Proof. Take $\phi = \mathrm{Id}_M$, the identity function on M, i.e. $\phi(m) = m$ for all $m \in M$. By the proposition above

$$\phi^n + a_1\phi^{n-1} + \ldots + a_n = 0$$

and so if we apply m we get

$$m + a_1 m + \ldots + a_n m = 0$$

and therefore

$$(1 + a_1 + a_2 + \ldots + a_n)m = 0.$$

Taking the element in the parentheses to be x we clearly have $xM = 0$, and also $x \equiv 1 \pmod{I}$. □

Corollary 7.1.3 (Nakayama's lemma)**.** *Let M be a finitely generated A-module. Let $I \subset A$ be an ideal such that $I \subset J(A)$. Suppose $IM = M$. Then $M = 0$.*

Proof. By the last corollary there exists an x such that $x \equiv 1 \pmod{I}$ and $xM = 0$. This then implies that $1 - x \in I \subset J(A)$, and since $1 - x$ is in the Jacobson radical, $1 - (1 - x) = x$ is a unit, so x^{-1} exists. Therefore $x^{-1}xM = 0$ meaning that $M = 0$. □

Corollary 7.1.4. *Let M be a finitely generated A-module and $N \subset M$ a submodule. Let $I \subset J(A)$ be an ideal. Suppose $M = IM + N$. Then $M = N$.*

Proof. Consider the quotient module M/N. Then

$$I\frac{M}{N} = \frac{IM}{N} = \frac{IM + N}{N} = \frac{M}{N}$$

and therefore this satisfies the assumptions of Nakayama's lemma since $I \subset J(A)$, and therefore $M/N = 0$ and so $M = N$. □

7.2 Finding Generators

We begin with a special case. Let A be a local ring (i.e. a ring with exactly one maximal ideal m). Let $k = A/m$ be the residue field.

Now let M be a finitely generated A-module. Then $mM \subset M$ is a submodule. Consider $M/(mM)$. It is an A-module, and

$$m \subset \mathrm{Ann}\left(\frac{M}{mM}\right)$$

meaning that $M/(mM)$ is an A/m-module, and since A/m is a field, it is in fact a vector space. This lets us lift a basis from the vector space to a generating set in the module.

Proposition 7.2.1. *Let $x_1, x_2, \ldots, x_n \in M$ be a set whose image in $M/(mM)$ forms a basis in the k-vector space. Then $\{ x_1, x_2, \ldots, x_n \}$ generates M.*

Proof. Let $N = (x_1, x_2, \ldots, x_n) \subset M$ be a submodule. Consider the map

$$\phi\colon N \hookrightarrow M \to \frac{M}{mM}.$$

This is surjective since $\{ x_1, x_2, \ldots, x_n \}$ is a basis in $M/(mM)$. Therefore $N + mM = M$, and since A is a local ring $J(A) = m$ and therefore $N = M$ by the previous result. □

If A isn't local, then we would have to first localise, but more on that in the future.

7.3 Exact Sequences

Definition 7.3.1 (Exact sequence)**.** Suppose L, M, and N are A-modules and that

$$L \xrightarrow{f} M \xrightarrow{g} N$$

is a sequence of homomorphisms. The sequence is called ***exact*** at M if $\operatorname{im} f = \ker g$.

A longer sequence

$$\cdots \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow \cdots$$

is called ***exact*** if it is exact at each M_i.

Example 7.3.2. The sequence $0 \to L \xrightarrow{f} M$ is exact if and only if f is injective, since the kernel of f must be trivial.

Similarly $L \xrightarrow{f} M \to 0$ is exact if and only if f is surjective, since everything in M is mapped to 0, making the kernel all of M, and this must then be the image of f. ▲

Example 7.3.3. If

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

is a ***short exact sequence*** (meaning three modules between the zeros), then the ***cokernel*** is

$$\operatorname{coker}(f) \coloneqq \frac{M}{\operatorname{im} f} = \frac{M}{\ker g} = N$$

where the first equality is by exactness and the second is from the first isomorphism theorem. ▲

This means that if we know that $L \subset M$ and we understand M/L, then we can learn something about M. The best case scenario is $M = L \oplus M/L$, since then we know everything.

One wonders, then, when this happens.

Proposition 7.3.4. *Let*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

be a short exact sequence of A-modules. Then the following are equivalent:

(*i*) *There exists an isomorphism $M \cong L \oplus N$ under which $f\colon m \mapsto (m, 0)$ is the natural embedding and $g\colon (m, n) \mapsto n$ is the natural projection.*

(*ii*) *There exists a map $h\colon N \to M$ such that $g \circ h = \mathrm{Id}_N$.*

(*iii*) *There exists a map $k\colon M \to L$ such that $k \circ f = \mathrm{Id}_L$.*

Remark 7.3.5. If these conditions hold, then the sequence is called a ***split exact sequence***.

Lecture 8 Exact Sequences

8.1 More on Exact Sequences

We ended last lecture by stating a result but didn't prove it—we do so now.

Proof. To see that (i) implies (ii) and (iii), just take $h\colon N \to M = L \oplus N$ to be $h(n) = (0, m)$ and $k\colon M \to L$ by $(m, n) \mapsto m$.

For (ii) implying (i), we have

$$0 \longrightarrow L \xrightarrow{f} M \underset{h}{\overset{g}{\rightleftarrows}} N \longrightarrow 0$$

where f is injective by exactness, h is injective since $g \circ h = \mathrm{Id}_L$. We then wish to show that $M = f(L) \oplus h(N) \cong L \oplus N$.

For $m \in M$ we have $m \mapsto g(m) \mapsto h(g(m)) \in h(N)$, whereby

$$m = \underbrace{(m - h(g(m)))}_{\in f(L) = \ker g} + \underbrace{h(g(m))}_{\in h(N)}$$

where the second membership is clear, but the first one needs some work:

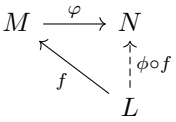
$$g(m - h(g(m))) = g(m) - g \circ h \circ g(m) = g(m) - g(m) = 0$$

since $g \circ h = \mathrm{Id}_L$. Therefore we have the requisite decomposition. For it to be the desired direct sum we also need to verify that the two parts have a trivial intersection. Let $m \in f(L) \cap h(N)$, meaning that $m = h(n)$ for some $n \in N$. We also have $m \in f(L) = \ker g$ and so $g(m) = 0$, meaning in turn that $g(h(n)) = n$, so $n = 0$ and $m = 0$.

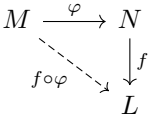
(iii) implying (i) is quite similar. □

Let $\varphi\colon M \to N$ be an A-module homomorphism. Let L be an A-module. Then φ induces two homomorphisms:

(i) First $\bar{\varphi}\colon \mathrm{Hom}(L, M) \to \mathrm{Hom}(L, N)$ by $f \mapsto \varphi \circ f$, i.e. $\bar{\varphi}(f) = \varphi \circ f$. To see this we draw the commutative diagram corresponding to $f\colon L \to M$ and $\varphi\colon L \to M$, and follow the arrows:



(ii) Similarly $\bar{\varphi}\colon \mathrm{Hom}(N, L) \to \mathrm{Hom}(M, L)$ defined by $\bar{\varphi}(f) = f \circ \varphi$, again by just filling in the diagram:



Date: September 19, 2017.

Proposition 8.1.1. (*i*) *The sequence*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N$$

is exact if and only if the sequence

$$0 \longrightarrow \mathrm{Hom}(P, L) \longrightarrow \mathrm{Hom}(P, M) \longrightarrow \mathrm{Hom}(P, N)$$

is exact for every A-module P.

(*ii*) *The sequence*

$$L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is exact if and only if the sequence

$$0 \longrightarrow \mathrm{Hom}(N, P) \longrightarrow \mathrm{Hom}(M, P) \longrightarrow \mathrm{Hom}(L, P)$$

is exact for every A-module P.

Remark 8.1.2. This says that Hom is ***left exact***, i.e. it only preserved the injectivity, but not the surjectivity.

We can preserve surjectivity with an additional requirement:

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is split exact if and only if

$$0 \longrightarrow \mathrm{Hom}(P, L) \longrightarrow \mathrm{Hom}(P, M) \longrightarrow \mathrm{Hom}(P, N) \longrightarrow 0$$

is split exact for every A-module P.

Proof. For the forward direction of (*i*), we have

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N$$

and

$$0 \longrightarrow \mathrm{Hom}(P, L) \xrightarrow{\bar{f}} \mathrm{Hom}(P, M) \xrightarrow{\bar{g}} \mathrm{Hom}(P, N)$$

Now the first step is to show that $\ker \bar{f} = 0$. Suppose $h \in \ker \bar{f}$. Then

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M \\ & & {\scriptstyle h}\uparrow & \nearrow_{f\circ h} & \\ & & P & & \end{array}$$

and $\bar{f}(h) = 0$ since h is in the kernel, and so since f is injective $h(x) = 0$ for all $x \in P$.

Secondly let us show that $\mathrm{im}\, \bar{f} = \ker \bar{g}$ by considering the two inclusions. So first $\mathrm{im}\, \bar{f} \subset \ker \bar{g}$, for which we have the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N \\ & & & {\scriptstyle k}\nwarrow & \uparrow{\scriptstyle h} & \nearrow_{\bar{g}(h)=g\circ h} & \\ & & & & P & & \end{array}$$

where $h \in \operatorname{im} \bar{f}$, and by following the diagram we have $\bar{g}(h) = g \circ h = g \circ f \circ k = 0$ since $g \circ f = 0$ since $\operatorname{im} f = \ker g$. Therefore $h \in \ker \bar{g}$.

Secondly for $\ker \bar{g} \subset \operatorname{im} \bar{f}$ consider the same diagram, with $h \in \ker \bar{g}$. Let $x \in P$, so that $x \mapsto h(x) \mapsto g(h(x)) = 0$ since $g \circ h = 0$. Moreover there exists some $y \in L$ such that $k(x) = y$ since $\ker g = \operatorname{im} f$ by exactness. Therefore $\bar{f}(k) = h$, so $h \in \operatorname{im} \bar{f}$.

For the opposite direction, first verify that $\ker f = 0$. We take $P = \ker f \subset L$, with

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M \\ & & \uparrow{\scriptstyle \text{inclusion}} & \nearrow_{f\circ\ell=0} & \\ & & P = \ker f & & \end{array} \qquad (\ell \text{ from } P \text{ to } L)$$

But $\bar{f}$ is injective, meaning that $\ell = 0$, whereby $\ker f = 0$.

Secondly we verify exactness. First check $\operatorname{im} f \subset \ker g$ by taking $P = L$.

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N \\ & & \nwarrow{\scriptstyle \text{inclusion}} \swarrow_{\ell} & & \uparrow{\scriptstyle f} & \nearrow_{g\circ f=0} & \\ & & & & P = L & & \end{array}$$

with $f = \bar{f}(\ell) \in \operatorname{im} \bar{f}$. Since $\operatorname{im} \bar{f} = \ker \bar{g}$, we have $g \circ f = 0$, and so $g \circ f(\ell) = g(f(\ell)) = 0$ implying that $\operatorname{im} f \subset \ker g$.

For the opposite inclusion, take $P = \ker g$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N \\ & & \nwarrow_{h} & & \uparrow{\scriptstyle \text{inclusion}} & \nearrow_{g\circ\ell=0} & \\ & & & & P = \ker g & & \end{array} \qquad (\ell \text{ from } P \text{ to } M)$$

Following the diagram along we have $\ell \in \ker \bar{g} = \operatorname{im} \bar{f}$, and so $x \in \operatorname{im} f$ if $x \in \ker g$.

(ii) is similar. □

Proposition 8.1.3 (Snake lemma)**.** *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & L' & \xrightarrow[f']{} & M' & \xrightarrow[g']{} & N' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of A-modules with rows being exact. Then there exists an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker \alpha & \xrightarrow{f} & \ker \beta & \xrightarrow{g} & \ker \gamma & & \\ & & & & & \xrightarrow{\delta} & & & \\ & & \operatorname{coker} \alpha & \xrightarrow{f'} & \operatorname{coker} \beta & \xrightarrow{g'} & \operatorname{coker} \gamma & \longrightarrow & 0 \end{array}$$

with δ being the **connecting homomorphism** *and* $\operatorname{coker} \alpha = L'/\operatorname{im} \alpha$*, and similarly for the other cokernels.*

The connecting homomorphism stems from the fact that g is surjective, meaning that there exists a y such that $g(y) = x \in \ker \gamma$, and we map that y over to M' using β and use surjectivity to fetch $\bar{w} \in \operatorname{coker} \alpha = L'/\operatorname{im} \alpha$.

8.2 Tensor Product of Modules

Definition 8.2.1 (Tensor product of modules)**.** Let M and N be A-modules. Let

$$C = \left\{ \sum_{i=1}^{k} a_i(x_i, y_i) \;\middle|\; x_i \in M, y_i \in N \right\}$$

be a free A-module in $M \times N$. Moreover let D be the submodule of C generated by all elements of the following times: $(x + x_1, y) - (x, y) - (x_1, y)$, $(x, y + y_1) - (x, y) - (x, y_1)$, (ax, y), and (x, ay) for $a \in A$, $x, x_1 \in M$, and $y, y_1 \in N$.

We define $M \otimes N = C/D$, called the ***tensor product*** of M and N.

Then $M \otimes N$ is generated by $x \otimes y$ for $x \in M$ and $y \in N$, and we have linearity in both coordinates.

Remark 8.2.2. Note that the linearity in the coordinates follows directly from construction, since we quotient away the expressions we want to be 0 for that to hold.

Remark 8.2.3. Roughly why one wants to do these sort of things is because tensor products are, in some sense, more well behaved than direct products. Take for instance the continuous functions on X and the continuous functions on Y, $C(X)$ and $C(Y)$ respectively. Then the continuous functions on $X \times Y$, $C(X \times Y)$ are not $C(X) \times C(Y)$, but—at least with some good assumptions—are $C(X) \otimes C(Y)$.

Lecture 9 Tensor Products

9.1 More on Tensor Products

Recall from last time that for two A-modules M and N, $M \otimes N$ is generated by $x \otimes y$ for $x \in M$ and $y \in N$, with bilinearity, i.e. linearity in both variables, meaning that $(x + x_1) \otimes y = x \otimes y + x_1 \otimes y$, $x \otimes (y + y_1) = x \otimes y + x \otimes y_1$, and finally $a(x \otimes y) = (ax) \otimes y = x \otimes (ay)$ for all $a \in A$.

This is equivalent with the following universal property: Let $\ell \colon M \times N \to M \otimes N$ defined by $\ell(x, y) = x \otimes y$. Then for any bilinear map $f \colon M \times N \to P$ there exists a *unique* homomorphism $\bar{f} \colon M \otimes N \to P$ called the ***tensor*** such that $f = \bar{f} \circ \ell$. This comes from the following commutative diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{\ell} & M \otimes N \\ \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \bar{f}} & \\ P & & \end{array}$$

Proposition 9.1.1. *Let M, N, and P be A-modules. Then*

(*i*) $M \otimes N \cong N \otimes M$,

Date: September 21, 2017.

(*ii*) $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$,

(*iii*) $(M \oplus N) \otimes P = (M \otimes N) \oplus (N \otimes P)$, *and*

(*iv*) $A \otimes M \cong M$.

All of these follow by the natural isomorphisms.

Definition 9.1.2 (Extension of Scalars)**.** Let M be an A-module. Suppose $B \supset A$ is a ring (meaning that we can view B as an A-module). Then $M_B \coloneqq B \otimes M$ is an A-module. Moreover it is also a B-module—we take

$$b(b_1 \otimes x) = (bb_1) \otimes x$$

for all $b, b_1 \in B$ and $x \in M$. In other words we extend scalars in A to scalars in B.

Proposition 9.1.3. *If M is a finitely generated A-module, then M_B is a finitely generated B-module.*

Proof. Let $x_1, x_2, \ldots, x_n$ generate M over A. Then $1 \otimes x_1, 1 \otimes x_2, \ldots, 1 \otimes x_n$ generate M_B over B since $M \ni b \otimes x = b(1 \otimes x)$ where x is a linear sum of $x_1, x_2, \ldots, x_n$. □

Theorem 9.1.4 (Adjoint associativity)**.** *Let M, N, and P be A-modules. Then*

$$\operatorname{Hom}(M \otimes N, P) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, P))$$

by the isomorphism ϕ, defined in the following way. Let $f\colon M \otimes N \to P$, i.e. $f \in \operatorname{Hom}(M \otimes N, P)$. Then for $x \in M$ and $y \in N$ we have

$$\big(\phi(f)(x)\big)(y) \coloneqq f(x \otimes y).$$

Sketch of proof. Let S be the set of bilinear maps $M \times N \to P$. We have an injective correspondence between S and $\operatorname{Hom}(M \otimes N, P)$ by the universal property. Therefore we

$$\begin{array}{ccc} M \times N & \xrightarrow{\ g\ } & P \\ \big\downarrow & \nearrow_{f} & \\ M \otimes N & & \end{array}$$

Fixing $x \in M$ we have $g(x, \cdot)\colon N \to P$ where $g(x, \cdot) \in \operatorname{Hom}(N, P)$ by linearity. Given $\psi\colon M \to \operatorname{Hom}(N, P)$, ψ lifts to the bilinear map $\bar{\psi}\colon M \times N \to P$ by $\bar{\psi}(x, y) = \big(\psi(x)\big)(y)$.

We then have that $\operatorname{Hom}(M, \operatorname{Hom}(N, P)) \leftrightarrow S$, and combining this with the universal property yields our bijection. □

Remark 9.1.5. Note that the important takeaway from this theorem is this: tensor product $\otimes$ is the adjoint functor to Hom.

9.2 Exactness

Proposition 9.2.1. *Let*

$$L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

be exact. Then

$$L \otimes P \xrightarrow{f\otimes 1} M \otimes P \xrightarrow{g\otimes 1} N \otimes P \longrightarrow 0$$

is exact for any A-module P.

Remark 9.2.2. This says that the tensor product is ***right-exact***.

Proof. We use the left-exactness of Hom, i.e. Proposition 8.1.1 from last lecture. In other words

$$L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is exact if and only if

$$0 \longrightarrow \mathrm{Hom}(N, R) \longrightarrow \mathrm{Hom}(M, R) \longrightarrow \mathrm{Hom}(L, R)$$

is exact for any R-module, which again is true if and only if

$$0 \longrightarrow \mathrm{Hom}(P, \mathrm{Hom}(N, R)) \longrightarrow \mathrm{Hom}(P, \mathrm{Hom}(M, R)) \longrightarrow \mathrm{Hom}(P, \mathrm{Hom}(L, R))$$

is exact for every A-module P. Finally by the adjoint associativity we have that this is true if and only if

$$P \otimes L \longrightarrow P \otimes M \longrightarrow P \otimes N \longrightarrow 0$$

is exact for any A-module P. □

Remark 9.2.3. It is *not* true in general that

$$L \longrightarrow M \longrightarrow N$$

being exact implies that

$$L \otimes P \longrightarrow M \otimes P \longrightarrow N \otimes P$$

is exact. In other words, the surjectivity of the last map is important.

Example 9.2.4. Consider $A = \mathbb{Z}$. The following sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

with $f(x) = 2x$ is exact, but

$$0 \longrightarrow \mathbb{Z} \otimes \tfrac{\mathbb{Z}}{2\mathbb{Z}} \xrightarrow{f\otimes 1} \tfrac{\mathbb{Z}}{2\mathbb{Z}}$$

is *not* exact since $f \otimes 1$ is not injective. To see this, consider

$$(f \otimes 1)(x \otimes y) = (2x) \otimes y = x \otimes (2y),$$

but then $2y \in \mathbb{Z}/(2\mathbb{Z})$, meaning that it is 0, and so the above is $x \otimes 0 = 0$, meaning that $f \otimes 1$ is identically 0 and certainly not injective. ▲

Definition 9.2.5 (Flat module)**.** An A-module P is called ***flat*** if for any exact sequence

$$L \longrightarrow M \longrightarrow N$$

the sequence

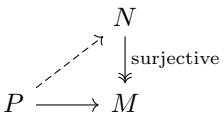
$$L \otimes P \longrightarrow M \otimes P \longrightarrow N \otimes P$$

is also exact.

Example 9.2.6. (i) Vector spaces are flat.

(ii) Free modules are flat. Note however that this is very restrictive; there aren't all that many free modules that aren't also vector spaces.

(iii) ***Projective modules*** are flat. We won't discuss projective modules much (if at all) in this course, for reference a module is ***projective*** if we have the situation



where we can lift to N.

▲

Proposition 9.2.7. *The following are equivalent:*

(i) *P is flat.*

(ii) *If*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is exact then

$$0 \longrightarrow L \otimes P \longrightarrow M \otimes P \longrightarrow N \otimes P \longrightarrow 0$$

is exact.

(iii) *If $f\colon M \to N$ is injective, then $(f \otimes 1)\colon M \otimes P \to \mathbb{N} \otimes P$ is injective.*

(iv) *If $f\colon M \to N$ is injective and M and N are* finitely generated*, then $(f \otimes 1)\colon M \otimes P \to N \otimes P$ is injective.*

Proof. (i) being equivalent to (ii) is immediate by definition since we specifically ask for injectivity in $0 \to L \otimes P$. Likewise (ii) is equivalent to (iii) again. Moreover (iii) implies (iv) trivially. That leaves (iv) implying (iii), which is the interesting result.

We claim that $\ker f = 0$. We have

$$\ker f \ni u = \sum_{i=1}^{n} x_i \otimes p_i$$

since we can view $u \in M \otimes P$, and M is finitely generated by assumption.

Now take $M_0 \otimes P \subset M \otimes P$ to be the subset generated by $x_i \otimes p_i$. Then

$$(f \otimes 1)(u) = \sum_{i=1}^{n} f(x_i) \otimes p_i$$

and we take $N_0 \subset N$ to be generated by $f(x_i)$.

Therefore

$$f \otimes 1\Big|_{M_0 \otimes P} : M_0 \otimes P \to N_0 \otimes P$$

being $f \otimes 1$ restricted to $M_0 \otimes P$ is a map between two finitely generated A-modules, which by assumption make them injective. Therefore $u \in M_0 \otimes P$ implies that $u = 0$. □

9.3 Localisation of a Ring

The goal of this part is to generalise the idea of fractions—in other words we wish to generalise the construction of quotient fields to not require an integral domain.

That is to say, let A be an integral domain. Then as we know A has a ***field of fractions*** or ***quotient field***, made up of elements a/b, with $a, b \in A$ and $b \neq 0$. But the representation for elements here is not unique: just like how in $\mathbb{Q}$ we have, say, $1/2 = 2/4$, we have

$$\frac{a}{b} = \frac{au}{bu}$$

for $u \in A$, $u \neq 0$. The way we reconcile this is to say that

$$\frac{a}{b} = \frac{s}{t} \quad \iff \quad \frac{at - bs}{bt} = 0.$$

In other words we write them with common denominator and check whether the numerator is 0. We say that

$$k = \{\, (a, b) = \frac{a}{b} \mid a \in A, b \in A, b \neq 0 \,\}$$

under the equivalence relation $(a, b) \sim (s, t)$ if and only if $at - bs = 0$. When proving transitivity of this relation we require the absence of zero divisors in the integral domain. Meaning that $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$ implies $(a, s) \sim (c, u)$ we have that $at - bs = 0$ and $bu - tc = 0$, and if we multiply the first one by u and the second one by s and add the two we have

$$0 = atu - bsu + bus - tcs = atu - tcs = t(au - cs)$$

which, since we have no zero-divisors, means that $t = 0$ (which can't be since it's the denominator of a fraction) or $au - cs = 0$, i.e. $(a, s) \sim (c, u)$.

Our goal, therefore, is to generalise this in such a way that we have a meaningful equivalence relation of this variety despite potentially having zero-divisors.

Definition 9.3.1. Let A be a ring and let $S \subset A$ be a multiplicative set (recall that this means $1 \in S$ and $ab \in S$ if $a, b \in S$). Define $\sim$ on $A \times S$ by

$$(a, s) \sim (b, t) \quad \iff \quad (at - bs)u = 0$$

for some $u \in S$.

The relation $\sim$ so defined is an equivalence relation. It is clearly ***reflexive***, since $(a, s) \sim (a, s)$ since by commutativity $as - sa = 0$. Similarly it is trivially ***symmetric*** since $(a, s) \sim (b, t)$ implies $(b, t) \sim (a, s)$ also by commutativity.

The interesting one—and the one where previously we required the absence of zero-divisors—is ***transitivity***. Suppose $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Show that $(a, s) \sim (c, u)$.

The proof of this is similar to the previous one, we just need to keep track of a few extra terms, namely the elements of the multiplicative set. So $(at-bs)v = 0$ for some $v \in S$, and $(bu - tc)w = 0$ for some $w \in S$. Then multiplying the first one by uw and the second one by sv we have

$$0 = atvuw - bsvuw + buwsv - tcwsv = tvw(au - cs)$$

where tvw is in S since $t, v, w \in S$. Therefore $(a, t) \sim (c, s)$.

This, therefore, is how we define our generalisation of the quotient ring:

Definition 9.3.2. Given a ring A and a multiplicative set $S \subset A$, then $S^{-1}A$ is the commutative ring of fractions a/s with $a \in A$ and $s \in S$, with the usual arithmetic operations:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \text{and} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Remark 9.3.3. If A is an integral domain and $S = A \setminus \{ 0 \}$, then $S^{-1}A = k$ is exactly the quotient field of A.

Example 9.3.4. Let A be a ring and $P \subset P$ be a prime ideal. Then, as proven before, $S = A \setminus P$ is a multiplicative set, so we can use it to define the above. We then get that $S^{-1}A$ is a local ring—it has exactly one maximal ideal. ▲

Remark 9.3.5. Define $f \colon A \to S^{-1}A$ by $a \mapsto a/1$. Then f is a ring homomorphism, but f is *not* injective in general, since if $(a - b)u = 0$ and $a - b$ is a zero-divisor, then $a/1 = b/1$, so two distinct $a, b \in B$ can map to the same element in $S^{-1}A$.

Lecture 10 Localisation

Recall that A is a ring, $S \subset A$ is a multiplicative subset, and that

$$S^{-1}A = \left\{ \frac{a}{s} \;\middle|\; a \in A, s \in S \right\}$$

is a ring of fractions in which

$$\frac{a}{s} = \frac{b}{t} \quad \iff \quad \frac{(at - bs)u}{stu} = 0$$

for some $u \in S$ if and only if $(at - bs)u = 0$ for some $u \in S$.

There is a natural map f from A to $S^{-1}A$, namely $a \mapsto a/1$. Then

$$\ker f = \{ a \in A \mid as = 0 \text{ for some } s \in S \}.$$

Date: September 26, 2017.

Moreover if $s \in S$, then $f(s) = s/1$ is a unit in $S^{-1}A$.

Consider $A = k[x, y]/(xy)$, with k a field, so that $xy = 0$ in A. Let $S = \{ 1, x, x^2, \dots \}$. Then

$$S^{-1}A \cong k[x, x^{-1}].$$

Also $\operatorname{Im} f = f(A) = k[x]$, since $f(y) = y/1 = yx/x = 0$.

10.1 Extension and Contraction

Definition 10.1.1 (Extension and Contraction)**.** Let $f\colon A \to B$ be a ring homomorphism. If I is an ideal in A, then $f(I)$ is not necessarily an ideal in B, but we can make it one by extending to $f(I)B$. In other words there is a correspondence

$$e\colon \{ \text{ideals in } A \} \to \{ \text{ideals in } B \}$$

defined by $e(I) = f(I)B$ which we call ***extension***. It is also sometimes written I^e.

Similarly we can contract an ideal in B to an ideal in A,

$$c\colon \{ \text{ideals in } B \} \to \{ \text{ideals in } A \}$$

by $c(J) = f^{-1}(J)$ called the ***contraction*** or ***restriction***. This is sometimes written J^c.

Proposition 10.1.2. *Let $f\colon A \to S^{-1}A$ be defined by $f\colon a \mapsto a/1$.*

(*i*) *For any ideal J in $S^{-1}A$, we have $e(c(J)) = J$.*

(*ii*) *For any ideal I in A, we have*

$$c(e(I)) = \{ a \in A \mid sa \in I \text{ for some } s \in S \}.$$

(*iii*) *If P is a prime ideal in A, and $P \cap S = \varnothing$, then $e(P)$ is a prime ideal in $S^{-1}A$.*

For an ideal $I \subset A$, we will denote $e(I)$ by $S^{-1}I$.

Proof. (*i*) That $e(c(J)) \subset J$ is trivial. For the other direction, suppose $a/s \in J$. Then $s/1 \cdot a/s = a/1 \in J$, and so $a \in f^{-1}(J) = c(J)$, meaning that $a/1 \in e(c(J))$.

(*ii*) Call $\{ a \in A \mid sa \in I \text{ for some } s \in S \} = B$. First let us show that $c(e(I)) \subset B$. If $a \in c(e(I))$, then $f(a) \in e(I)$, and in turn $f(a) = a/1 = b/s$ for some $b \in I$ and $s \in S$ since $f(a) \in S^{-1}I$. This means that $(as - b)u = 0$ for some $u \in S$, and so $asu = bu \in I$. Since $b \in I$ and $s, u \in I$, we have that $a \in B$.

For the opposite direction, take $a \in B$, meaning that $as \in I$ for some $s \in S$. Then

$$f(a) = \frac{a}{1} = \frac{as}{s} \in e(I)$$

since $as \in I$, and so $a \in c(e(I))$.

(*iii*) Suppose $x/s \cdot y/t \in e(P)$, where $x, y \in A$ and $s, t \in S$. Then

$$\frac{xy}{st} = \frac{p}{u}$$

with $p \in P$ and $u \in S$, so $(xyu - stp)v = 0$ for some $v \in S$, and so

$$(xy)(uv) = stpv \in P$$

since $p \in P$, and since $u, v \in S$ we must have $xy \in P$ since $P \cap S = \varnothing$, and because P is prime, $x \in P$ or $y \in P$. Therefore $x/s \in e(P)$ or $y/t \in e(P)$. □

Corollary 10.1.3. *Localisation commutes with nilradical, i.e.* $\operatorname{nilrad}(S^{-1}A) = S^{-1}(\operatorname{nilrad}(A))$.

Proof. We write the nilradical as the intersection of prime radicals:

$$\operatorname{nilrad}(A) = \bigcap_{P \in \operatorname{Spec}(A)} P.$$

Therefore

$$S^{-1}(\operatorname{nilrad}(A)) = S^{-1}\Big(\bigcap_{P \in \operatorname{Spec}(A)} P \Big).$$

Now if $P \cap S \neq \varnothing$, then $S^{-1}P = S^{-1}A$ since the former will contain some $s/1$, which is a unit. Therefore for the intersection it suffices to consider prime ideals P with $P \cap S = \varnothing$. Then

$$\begin{aligned} S^{-1}(\operatorname{nilrad}(A)) = S^{-1}\Big(\bigcap_{P \in \operatorname{Spec}(A)} P \Big) &= \bigcap_{P \in \operatorname{Spec}(A)} S^{-1}P \\ = \bigcap_{P \cap S = \varnothing} S^{-1}P = \bigcap_{Q \in \operatorname{Spec}(S^{-1}A)} Q &= \operatorname{nilrad}(S^{-1}A). \end{aligned}$$

Note that we have not yet proved that intersection and localisation commute. We'll do this next time. □

Speaking of prime ideals, they allow us to construct a special kind of localisation. Let P be a prime ideal of A. Then $S = A \setminus P$ is a multiplicative set, and therefore we can localise using it. We let $A_P = S^{-1}A$, called the ***localisation at P localisation***.

Proposition 10.1.4. *An element $a/s \in A_P$ is a unit if and only if $a \notin P$. Hence A_P is a local ring with maximal ideal $e(P) = S^{-1}P = PA_P$.*

Proof. Start by assuming $a \notin P$. By construction this means that $a \in S$, whereby $s/a \in A_P$ since it's a valid denominator, and so $a/s \cdot s/a = 1$, and a/s is a unit.

In the other direction, let a/s be a unit, meaning that $a/s \cdot b/t = 1$ for some $a \in A$ and $t \in S$. This means that $(ab - st)u = 0$ for some $u \in S$, and so $abu = stu$, which is in S since $s, t, u \in S$ and S is multiplicative. Therefore $abu \notin P$ and so we must have $a \notin P$ for otherwise $abu \in P$ since P is an ideal.

In other words $A_P = A^\times \sqcup S^{-1}P$, so it is a local ring. □

Corollary 10.1.5. *Let P be a prime ideal in A. The prime ideals of A_P are in one-to-one correspondence with the prime ideals of A contained in P.*

Example 10.1.6. Let $A = \mathbb{Z}$ and $P = (p)$, p a prime. Then

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b,\ a, b \in \mathbb{Z} \right\}$$

is a local ring with maximal ideal

$$M = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \;\middle|\; p \mid a \right\} = P\mathbb{Z}_{(p)}.$$ ▲

10.2 Modules of Fractions

Definition 10.2.1 (Module of fractions)**.** Let M be an A-module. Let $S \subset A$ be a multiplicative set. Define $S^{-1}M$ to be the $S^{-1}A$-module as follows:

The equivalence relation $\sim$ on $M \times S$ is defined by $(m, s) \sim (n, t)$ if and only if $(tm - sn)u = 0$ for some $u \in S$. Then $S^{-1}M = (M \times S)/\sim$. As before we have

$$\frac{m}{s} \pm \frac{n}{t} = \frac{mt \pm sn}{st}$$

and

$$\frac{a}{t} \cdot ms = \frac{am}{ts}$$

with $a \in A$, $s, t \in S$, and $m \in M$.

As before, if $S = A \setminus P$ with P being a prime ideal of A, then we write $S^{-1}M = M_P$. In fact, it turns out that $M_P = S^{-1}A \otimes_A M$.

Let $f\colon M \times N$ be an A-module homomorphism. This homomorphism induces an $S^{-1}A$-module homomorphism

$$S^{-1}f\colon S^{-1}M \to S^{-1}N$$

by

$$S^{-1}f\Big(\frac{m}{s}\Big) = \frac{f(m)}{s},$$

i.e. it preserves the denominator. Clearly $S^{-1}(f \circ g) = S^{-1}f \circ S^{-1}g$.

Lecture 11 Exactness of Localisation

11.1 Exactness of Localisation

Proposition 11.1.1. *Let L, M, and N be A-modules. If*

$$L \xrightarrow{f} M \xrightarrow{g} N$$

is an exact sequence, then

$$S^{-1}L \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}N$$

is an exact sequence.

Proof. We want to show that $\operatorname{Im} S^{-1}f = \ker S^{-1}g$, so start by assuming the former is a subset of the latter. Now $S^{-1}f \circ S^{-1}g = S^{-1}(f \circ g)$, but since the first sequence is exact, $\operatorname{Im} f = \ker g$, so $f \circ g = 0$, and therefore $S^{-1}(f \circ g) = 0$.

Next we show that $\ker S^{-1}g \subset \operatorname{Im} S^{-1}f$. Let $m/s \in \ker S^{-1}g$, meaning that

$$S^{-1}g\Big(\frac{m}{s}\Big) = \frac{g(m)}{s} = 0.$$

Date: September 28, 2017.

This means that there exists some $t \in S \subset A$ such that $tg(m) = 0$. But g is A-linear, being an A-module homomorphism, so $tg(m) = g(tm) = 0$, meaning that $tm \in \ker g = \operatorname{Im} f$. Therefore $tm = f(x)$ for some $x \in L$, so

$$\frac{m}{s} = \frac{tm}{ts} = \frac{f(x)}{ts} = S^{-1}f\Big(\frac{x}{ts}\Big) \in \operatorname{Im} S^{-1}f,$$

and we are done. □

Corollary 11.1.2. *Let N_i, N, and L be submodules of M. Then*

(*i*) $S^{-1}(N + L) = S^{-1}N + S^{-1}L$;

(*ii*) $S^{-1}\Big(\bigcap_i N_i\Big) = \bigcap_i S^{-1}N_i$; *and*

(*iii*) *As $S^{-1}A$-modules,*

$$S^{-1}\Big(\frac{M}{N}\Big) \cong \frac{S^{-1}M}{S^{-1}N}.$$

Proof. (*i*) is trivial by the very definition of fractions: just split a given fraction into two parts.

For (*ii*), let $m/s \in S^{-1}(\bigcap_i N_i)$. This means that $m \in bigcap_i N_i$, and in turn $m \in N_i$ for all i. Therefore $m/s \in S^{-1}N_i$ for all i, and so $m/s \in \bigcap_i S^{-1}N_i$.

For the opposite direction, if $m/s \in \bigcap_i S^{-1}N_i$, then $m/s \in S^{-1}N_i$ for all i. Now this does not immediately imply that $m \in N_i$ for all i, since we are working with equivalence classes, but it does mean that $m/s = n_i/s_i$ for some $n_i \in N_i$, and $(s_i m - s n_i)u_i = 0$ for some $u_i \in S$. Therefore $s_i u_i m = s u_i n_i \in N_i$ since $n_i \in N_i$ and N_i is a module. Therefore

$$\frac{m}{s} = \frac{s_i u_i m}{s_i u_i s} \in S^{-1}N_i$$

for all i.

(*iii*) Consider

$$0 \longrightarrow N \longrightarrow M \longrightarrow \tfrac{M}{N} \longrightarrow 0.$$

This is exact since $N \subset M$, and so by the previous proposition

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}\Big(\tfrac{M}{N}\Big) \longrightarrow 0$$

is exact. The first isomorphism theorem now tells us that

$$\frac{S^{-1}M}{S^{-1}N} \cong S^{-1}\Big(\frac{M}{N}\Big).$$ □

Proposition 11.1.3. *Let M be an A-module. Then $S^{-1}M \cong S^{-1}A \otimes_A M$ as an $S^{-1}A$-module.*

The isomorphism is given by $f\colon S^{-1}A \otimes M \to S^{-1}M$,

$$f\Big(\frac{a}{s} \otimes m\Big) = \frac{am}{s}$$

with $a \in A$, $s \in S$, and $m \in M$.

Proof. That f is a homomorphism is obvious, since we just distribute and simplify fractions. Moreover that it is surjective is clear too, since taking $a = 1$ suffices to yield all of $S^{-1}M$.

That it is injective is less obvious. Consider an element $a/s \otimes m = 1/s \otimes (am)$. Then all elements in $S^{-1}A \otimes M$ can be written as $1/a \otimes m$. Now let such an element be in the kernel of f, i.e.

$$f\Big(\frac{1}{s} \otimes m\Big) = \frac{m}{s} = 0.$$

This implies that $tm = 0$ for some $t \in S$, and therefore

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes (tm) = 0$$

since $tm = 0$. □

Corollary 11.1.4. *The A-module $S^{-1}A$ is flat.*

Recall that this means that tensor products preserve exactness.

Proof. Suppose

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is exact. Then we'd like to show that

$$0 \longrightarrow S^{-1}A \otimes L \longrightarrow S^{-1}A \otimes M \longrightarrow S^{-1}A \otimes N \longrightarrow 0$$

is exact. But we just showed that $S^{-1}A \otimes L \cong S^{-1}L$, and so on for M and N, and we know from before that localisation is an exact functor, so the result follows. □

Proposition 11.1.5. *If M and N are A-modules, then $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N)$ as $S^{-1}A$-modules.*

The isomorphism is given by $f\colon S^{-1}M \otimes S^{-1}N \to S^{-1}(M \otimes N)$,

$$f\Big(\frac{m}{s} \otimes \frac{n}{t}\Big) = \frac{m \otimes n}{st}.$$

In particular, for any prime ideal $P \subset A$, $M_P \otimes_{A_P} N_P = (M \otimes_A N)_P$.

Proof. That f is a homomorphism is obvious. Surjectivity is clear by definition, and so is injectivity. □

11.2 Local Property

A property K of a ring A (or an A-module M) is called a ***local property*** if A (or M) has K if and only if A_P (or M_P) has K for all prime ideals $P \subset A$.

Example 11.2.1. A homomorphism $f\colon M \to N$ is injective (or surjective) if and only if $f\colon M_P \to N_P$ is injective (or surjective) for every prime ideal P of A. This means that injectivity and surjectivity, and thereby bijectivity, is a local property. We'll prove this later. ▲

Lecture 12 Primary Decomposition

An aside: We spent a significant amount of time toying with commutative diagrams and so on and so forth. In the opening scene of the movie *It's My Turn* from 1980, a mathematics professor by the name of Kate Gunzinger (portrayed by Jill Clayburgh) is proving the Snake lemma on the board, to which Daniel Stern's character Cooperman responds by saying that 'This stuff is just garbage,' asking when they'll move on to interesting stuff.

So here we are, moving on to interesting stuff!

12.1 Local Properties

As established last time, a property K of a ring A or A-module M is called local if the ring or module has the property if and only if A_P (or M_P) has the same property for all prime ideals $P \subset A$.

Proposition 12.1.1. *Let M be an A-module. Then the following are equivalent:*

(*i*) $M = 0$.

(*ii*) $M_P = 0$ *for all prime ideals P of A.*

(*iii*) $M_m = 0$ *for all prime ideals m of A.*

Proof. It is clear that (*i*) implies (*ii*) implies (*iii*), in the second case since maximal ideals are prime. It remains to show that (*iii*) implies (*i*), therefore.

Suppose $x \neq 0$ is some element in M. Let $I = \operatorname{Ann}(x) = \{\, a \in A \,|\, ax = 0 \,\} \subset A$, which is an ideal. Then $I \neq A = (1)$, since otherwise $1x = 0$ which means that $x = 0$. Hence $I \subset m \subset A$, and m is maximal. So we localise! Thus

$$\frac{x}{1} \in M_m = 0,$$

by assumption, and so $sx = 0$ for some $s \in S = A \setminus m$, implying that $s \in \operatorname{Ann}(x) = I \subset m$. In other words $s \in m$ and $s \notin m$, which is impossible, and so M contains no nonzero elements. □

In other words, the 0-module is a local property. This might not seem terribly interesting or useful, but it is:

Proposition 12.1.2. *Let $\phi\colon M \to N$ be an A-module homomorphism. Then the following are equivalent:*

(*i*) ϕ *is injective.*

(*ii*) $\phi_P\colon M_P \to N_P$ *is injective for all prime ideals P of A.*

(*iii*) $\phi_m\colon M_m \to N_m$ *is injective for all maximal ideals m of A.*

The same is true if we replace injectivity by surjectivity.

Date: October 3, 2017.

Proof. For (i) implying (ii), we have that

$$0 \longrightarrow M \xrightarrow{\phi} N$$

being exact (i.e. ϕ is injective) implies that

$$0 \longrightarrow M_P \xrightarrow{\phi_P} N_P$$

is exact since we've proved previously that localisation is an exact functor.

Next (ii) implying (iii) is trivial since maximal ideals are prime ideals.

Finally assume (iii) and consider $L = \ker \phi$. Then

$$0 \longrightarrow L \longrightarrow M \xrightarrow{\phi} N$$

is exact by embedding L in M. But then

$$0 \longrightarrow L_m \longrightarrow M_m \xrightarrow{\phi_m} N_m$$

is exact since localisation is an exact functor, and $L_m = \ker \phi_m = 0$ since ϕ_m is injective by assumption. But this means that $L = 0$ by last proposition, since 0-module is a local property, and so ϕ itself is injective.

For surjectivity, we do almost exact the same thing, but consider the diagram

$$M \xrightarrow{\phi} N \longrightarrow 0$$

instead. □

12.2 Primary Decomposition

In $\mathbb{Z}$, prime ideals are (0) and $P = (p)$, for p primes. These then model the idea that if $p \mid xy$, then either $p \mid x$ or $p \mid y$.

Suppose instead that $p^n \mid xy$. Then possibly $p^n \mid x$, but that doesn't have to be the case—some factors of p could be in x and some in y—and we could instead have $p^n \nmid x$, in which case we must have $p \mid y$. That does not account for all n factors of p, however, so we have $p^n \mid y^n$.

Generalising this to ideals in the same way we did with primes to prime ideals we get the ***primary ideals***, which in $\mathbb{Z}$ are $P^n = (p)^n = (p^n)$.

Definition 12.2.1 (Primary ideal)**.** An ideal Q of A is ***primary*** if $Q \neq A$ and for $x, y \in A$, if $xy \in Q$, then $x \in Q$ or $y^n \in Q$ for some $n > 0$. Note that $y^n \in Q$ for some positive power simply means that $y \in \operatorname{rad}(Q)$.

Another way to look at it therefore is that Q is primary if and only if all zero-divisors of A/Q, which is nonzero since $Q \neq A$, are nilpotent. This is because if we consider a product $xy \in Q$, this in A/Q will be $\bar{x}\bar{y} = 0$. Then either $x \in Q$, meaning $\bar{x} = 0$, or $y^n \in Q$, or $\bar{y}^n = 0$, so y is nilpotent.

Example 12.2.2. Every prime ideal is primary. A quick way to see this: if P is a prime ideal of A, then A/P is an integral domain, which contain no zero divisors, and so all zero-divisors are nilpotent is vacuously true. ▲

Example 12.2.3. The contraction of a primary ideal is primary, i.e. if $f\colon A \to B$ and $Q \subset B$ is primary, then $f^{-1}(Q) \subset A$ is primary. To see why, consider

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \longrightarrow & B/Q \\ & \searrow & & \nearrow & \\ & & \phi & & \end{array}$$

where ϕ is the composite map. Then $A/f^{-1}(Q) \cong \operatorname{Im}\phi \subset B/Q$ by the first isomorphism theorem, and since every zero-divisor is nilpotent in B/Q since Q is primary in B, then by isomorphism the same is true in $A/f^{-1}(Q)$, so $f^{-1}(Q)$ is primary in A. ▲

Proposition 12.2.4. *Let Q be a primary ideal of A. THen $P = \operatorname{rad}(Q)$ is the smallest prime ideal contained in Q.*

Proof. It suffices to show $\operatorname{rad}(Q)$ is prime, since

$$\operatorname{rad}(S) = \bigcap_{P \subset S \text{ prime}} P$$

and so it is automatically the smallest. Now let $xy \in \operatorname{rad}(Q)$. Then $(xy)^n = x^n y^n \in Q$ for some $n > 0$. Since Q is primary, either $x^n \in Q$ or $y^{nm} \in Q$ for some positive power m. Therefore $x \in \operatorname{rad}(Q)$ or $y \in \operatorname{rad}(Q)$, so $\operatorname{rad}(Q)$ is a prime ideal. □

Definition 12.2.5 (P-primary ideal)**.** An ideal Q of a ring A is called ***P-primary*** if Q is primary and $\operatorname{rad}(Q) = P$.

Example 12.2.6. The primary ideals in $\mathbb{Z}$ are (0) or (p^n) for $n > 0$ and p prime. Now consider ideals generated by composites instead. That is, let $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Then

$$(n) = (p_1^{n_1}) \cap (p_2^{n_2}) \cap \ldots \cap (p_k^{n_k}).$$ ▲

There are two natural questions that follow. Firstly, in what rings can we decompose ideals as intersections of primary ideals (this being the titular ***primary decomposition***)? Secondly, given a primary ideal Q in a ring A, what sort of ring must A be in order for $Q = P^n$ for some prime ideal P and power n?

The answers—and we'll explore at least the first one more later on in this course—is that in ***Notherian rings*** we have primary decomposition, and in ***Dedekind domains*** we can write all primary ideals as powers of prime ideals.

Example 12.2.7. Let $A = k[x, y]$, with k a field. Let $Q = (x, y^2)$, and consider $A/Q = k[y]/(y^2)$, since x is killed. Here every zero-divisor is nilpotent since it must contain y, and $y^2 = 0$ in the quotient. Therefore Q is primary in A.

We also have $\operatorname{rad}(Q) = (x, y) = P$, which is prime, but clearly $P \supsetneq Q \supsetneq P^2$ since the first one contains a lone y, which the middle one does not, and the middle one contains a lone x, which the last one does not, since $P^2 = (x^2, xy, y^2)$. Therefore Q is not a prime power. ▲

Next, let us demonstrate that a prime power isn't necessarily primary.

Example 12.2.8. Let $A = k[x, y, z]/(xy - z^2)$, with k a field. Let $\bar{x}$, $\bar{y}$, and $\bar{z}$ denote images of x, y, and z in A, and let $P = (\bar{x}, \bar{z}) \subset A$.

We have $A/P = k[y]$, which since k is a field is an integral domain, and so P is a prime ideal. Now consider $P^2 = (\bar{x}^2, \bar{x}\bar{z}, \bar{z}^2)$, and let us work in A/P^2.

In here $\bar{x}\bar{y} = \bar{z}^2 \in P^2$, since $xy - z^2 = 0$ in A itself. Therefore $\bar{x}\bar{y} = 0$ in A/P^2, which makes $\bar{x}$ and $\bar{y}$ zero-divisors. They are not both nilpotent, however: $\bar{x}$ is, since $\bar{x}^2 = 0$ in here, but $\bar{y}$ is not zero for any power in A/P^2, and so P^2 is not primary.

We still have $\mathrm{rad}(P^2) = P$, however, which is why we specifically require Q to be primary in the definition of P-primary ideals above. ▲

Proposition 12.2.9. *Suppose Q is P-primary and that P is finitely generated. THen $P \supset Q \supset P^n$ for some $n > 0$.*

Proof. Let $P = (x_1, x_2, \ldots, x_k) = \mathrm{rad}(Q)$. Then for every $i = 1, 2, \ldots, k$ we hjave $x_i^{n_i} \in Q$ for some $n_i > 0$. Taking $n = n_1 + n_2 + \ldots + n_k$, we have therefore that $P^n \subset Q$. □

Note, by the way, that this is not true for every ideal I.

However, if instead we're considering a maximal ideal m, all of these good properties hold:

Proposition 12.2.10. *If $m = \mathrm{rad}(Q)$ is maximal, then Q is m-primary. In particular the powers of a maximal ideal m are m-primary.*

Proof. Consider $A \to A/Q$. Then m is mapped to $\bar{m}$, which is still maximal, and $m = \mathrm{rad}(Q)$ corresponds to $\mathrm{nilrad}(A/Q) = \bar{m}$. But then we have

$$\frac{A}{Q} = \left(\frac{A}{Q}\right)^{\times} \sqcup \bar{m}$$

and so any zero-divisor in here must belong to the maximal ideal $\bar{m}$, since it can't be a unit. Therefore Q is primary.

The second part, about m^k being primary, is trivial given the above since $\mathrm{rad}(m^k) = m$. □

Lecture 13 More on Primary Decomposition

13.1 First Uniqueness Theorem

Lemma 13.1.1. *If Q_1 and Q_2 are P-primary ideals, then $Q = Q_1 \cap Q_2$ is P-primary as well.*

Proof. First establish that Q has the correct radical:

$$\mathrm{rad}(Q) = \mathrm{rad}(Q_1 \cap Q_2) = \mathrm{rad}(Q_1) \cap \mathrm{rad}(Q_2) = P \cap P = P.$$

Next we show that Q is primary. Let $xy \in Q = Q_1 \cap Q_2$. Then $xy \in Q_1$ and $xy \in Q_2$. If $x \in Q$, then we're done, so assume it isn't. Then x doesn't belong to one Q_1 or Q_2, let's say $x \notin Q_1$. But this, by Q_1 being primary, implies that $y \in \mathrm{rad}(Q_1) = P = \mathrm{rad}(Q)$, so Q is primary. □

Date: October 5, 2017.

Remark 13.1.2. We can of course iterate on this, so that if $Q_1, Q_2, \ldots, Q_k$ are P-primary, then $Q_1 \cap Q_2 \cap \ldots \cap Q_k$ is P-primary.

Definition 13.1.3 (Primary decomposition)**.** Let A be a ring and $I \subset A$ an ideal. A ***primary decomposition*** of I is

$$I = Q_1 \cap Q_2 \cap \ldots \cap Q_k$$

with each $Q_1, Q_2, \ldots, Q_k$ being primary. This primary decomposition is called ***minimal*** (or ***shortest***, ***irredundant***, ***reduced***, ***normal***, et cetera) if

(*i*) $\operatorname{rad}(Q_i)$ are all distinct for $i = 1, 2, \ldots, k$, and

(*ii*) $Q_i \not\subset \bigcap_{j \neq i} Q_j$, i.e. each Q_i is necessary.

Note that if two primary ideals Q_i and Q_j have the same radical P, then we can combine them as per the previous lemma. Therefore a minimal decomposition always exists if a decomposition exists.

Definition 13.1.4 (Decomposable ideal)**.** An ideal $I \subset A$ is said to be ***decomposable*** if it has a primary decomposition.

These primary decompositions are not quite unique, but the radicals of the primary ideals are.

Theorem 13.1.5 (First uniqueness theorem)**.** *Let I be a decomposable ideal of A. Let $I = Q_1 \cap Q_2 \cap \ldots \cap Q_k$ be a minimal primary decomposition. Let $P_i = \operatorname{rad}(Q_i)$ for $i = 1, 2, \ldots, k$. Then*

$$\{ P_1, P_2, \ldots, P_k \} = \{ \operatorname{rad}(I : x) \text{ prime} \mid x \in A \}$$

is determined only by the ideal I, whereby the P_i are uniquely determined by the ideal I and do not depend on the decomposition.

Proof. Recall $(I : x) = \{ y \in A \mid xy \in I \}$. Since fractional ideal commutes with intersection, we have for $x \in A$ that

$$(I : x) = \Big(\bigcap_i Q_i : x \Big) = \bigcap_i (Q_i : x).$$

Therefore if $x \in Q_i$, then $Q_i : x) = A$ since Q_i is an ideal. For this reason it suffices to take the intersection over Q_i not containing x, i.e.

$$(I : x) = \bigcap_{x \notin Q_i} (Q_i : x).$$

We now wish to take radicals of both sides, but for that we first note that if $x \notin Q_i$, then $\operatorname{rad}(Q_i : x) = P_i$. To see this, note that

$$Q_i \subset (Q_i : x) \subset P_i.$$

The first inclusion is always true. For the second one, note that if $y \in (Q_i : x)$, then $xy \in Q_i \subset P_i$, and since $x \notin Q_i$, it implies that $y \in \operatorname{rad}(Q_i) = P_i$.

Taking radicals of all three we squeeze $\operatorname{rad}(Q_i : x)$ between P_i and P_i.

All this to say:

$$\operatorname{rad}(I : x) = \bigcap_{x \notin Q_i} \operatorname{rad}(Q_i : x) = \bigcap_{x \notin Q_i} P_i.$$

Now suppose $\operatorname{rad}(I : x) = P$ is prime. Then

$$P = \bigcap_{x \notin Q_i} P_i$$

which by a theorem long in the past implies that $P = P_j$ for some j. Ergo

$$\{ \operatorname{rad}(I : x) \text{ prime} \} \subset \{ P_1, P_2, \ldots, P_k \}.$$

For the opposite inclusion, note that by minimality of the decomposition there exists some $x_i \notin Q_i$, yet

$$x_i \in \bigcap_{j \neq i} Q_j.$$

Then $\operatorname{rad}(I : x_i) = P_i$ since all other P_j contain x_i by the above intersection. □

Remark 13.1.6. (*i*) For each I, there exists some $x_i \in A$ such that $(I : x_i)$ is P_i primary.

(*ii*) Consider the A-moduile A/I. The prime ideals P_i are precisely the prime ideals that occur as radicals of annihilators of elements of A/I since $(I : x)$ corresponds to $(0 : x) = \operatorname{Ann}(x)$.

Definition 13.1.7 (Associated prime)**.** The prime ideals P_i in the above theorem are said to ***belong to*** I or ***associated with*** I.

Remark 13.1.8. The ideal I is primary if and only if it has only one associated prime ideal.

Example 13.1.9. Let $A = k[x, y]$, with k a field. The ideal $I = (x^2, xy)$ is not primary since $\bar{y}$ is a zero divisor but not nilpotent. We can decompose it as $I = P_1 \cap P_2^2$ with $P_1 = (x)$ and $P_2 = (x, y)$. The first one is a prime ideal, and the second one is maximal, making P_2^2 primary. Therefore P_1 and P_2 are unique, but the decomposition itself is not:

$$(x^2, xy) = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, y)$$

are two valid primary decompositions, but the radicals are of course the same. ▲

There is another aspect of the decomposition which is unique: the component corresponding to the smallest prime.

Definition 13.1.10 (Minimal prime, isolated prime)**.** The minimum elements of $\{ P_1, P_2, \ldots, P_k \}$ is called the ***minimal*** or ***isolated*** prime ideals belonging to I.

The other prime ideals associated with I are called ***embedded*** prime ideals.

Proposition 13.1.11. *Let I be a decomposable ideal in A. Then any prime ideal $P \supset I$ contains a minimal prime ideal associated with I.*

Hence the minimal prime ideals associated with I are precisely the minimal elements in the set $\{ P \text{ prime} \mid P \supset I \}$.

Proof. We have $P \supset I = \bigcap_i Q_i$. Taking radicals, $P \supset \bigcap_i \operatorname{rad}(Q_i) = \bigcap_i P_i$, whereby $P \supset P_j$ for some j. □

Proposition 13.1.12. *Let I be a decomposable ideal and*

$$I = \bigcap_{i=1}^{n} Q_i$$

be a minimal primary decomposition with $\operatorname{rad}(Q_i) = P_i$. *Then*

$$\bigcup_{i=1}^{n} P_i = \{\, x \in A \mid (I : x) \supsetneq I \,\}.$$

In particular, if (0) *is decomposable, then the set D of zero-divisors is the union of prime ideals associated with* (0).

Proof. Consider $A \to A/I$. If I is decomposable, then (0) is decomposable in A/I. Indeed

$$I = \bigcap_{i=1}^{n} Q_i$$

is minimal if and only if

$$(0) = \bigcap_{i=1}^{n} \bar{Q}_i$$

is minimal. Therefore it suffices to consider $I = (0)$, which means we're considering $D = \{\, x \in A \mid (0 : x) \supsetneq (0) \,\}$, the set of all zero-divisors, which is the same as

$$\bigcup_{x \neq 0} \operatorname{rad}(0 : x).$$

So let us check if this is equal to the union of prime ideals:

$$\operatorname{rad}(0 : x) = \operatorname{rad}\Big(\bigcap_{P \in \operatorname{Spec} A} P : x) = \bigcap_{x \notin P_i} P_i \subset P_j$$

and $P_i = \operatorname{rad}(0 : x)$ for some x by the previous theorem. □

Proposition 13.1.13. *Let S be a multiplicative set, and let Q be a P-primary ideal. Then*

(*i*) *If $S \cap P \neq \varnothing$, then $S^{-1}Q = S^{-1}A$;*

(*ii*) *If $S \cap P = \varnothing$, then $S^{-1}Q$ is $S^{-1}P$-primary and its contraction in A is Q.*

That is to say, localisation preserves the structure of primary ideals.

Proof. For (*i*), if the intersection is nonempty, then $s \in S \cap P$, meaning that $s^n \in S \cap Q$ for some n, whereby $S^{-1}Q$ is $S^{-1}A$ since it contains a unit.

For (*ii*), recall that for $A \to S^{-1}A$, we have the correspondence

$$\{\, I \mid a \in I \text{ if } as \in I \text{ for some } s \in S \,\} \longleftrightarrow \{\, S^{-1}I \mid \text{ideals in } S^{-1}A \,\}.$$

If $as \in Q$, $s \in S$, and $Q \supset P$ with $S \cap P = \varnothing$, then $S \cap Q = \varnothing$, and so $a \in Q$, since otherwise if $a \notin Q$ we have $s \in \operatorname{rad}(Q) = P$, a contradiction. Therefore Q is in one-to-one correspondence with $S^{-1}Q$. Moreover $\operatorname{rad}(S^{-1}Q) = S^{-1}(\operatorname{rad}(Q)) = S^{-1}P$. □

Lecture 14 Ring Extensions

14.1 Second Uniqueness Theorem

Recall how when we localise a ring A into $S^{-1}A$, we carry over the ideals I such that $as \in I$ for all $s \in S$ implies $a \in I$, and such ideals are in one-to-one correspondence with the ideals $S^{-1}I$ of $S^{-1}A$.

We move between these ideals by extension and contraction, and naturally the correspondence is true for prime ideals as well and, as we proved at the end of the last lecture, also for primary ideals.

For any ideal I in A, the contraction in A of the ideal $e(I)$ is denoted by $S(I)$, i.e. $S(I) = c(e(I))$.

Proposition 14.1.1. *Let A be a ring and $S \subset A$ a multiplicative subset. Let I be a decomposable ideal and let*

$$I = \bigcap_{n=1}^{n} Q_i$$

be a minimal primary decomposition. Moreover let $P_i = \operatorname{rad}(Q_i)$ for each $i = 1, 2, \ldots, n$.

Assume $P_i \cap S = \varnothing$ for all $i = 1, 2, \ldots, m$ and $P_i \cap S \neq \varnothing$ for the remaining $i = m+1, m+2, \ldots, n$.

Then

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i$$

and

$$S(I) = \bigcap_{i=1}^{m} Q_i.$$

Before we prove this, note that it is always possible to arrange the conditions above: just reorder the primary decomposition so that the ideals whose radicals don't meet S are at the front.

Proof. Both of these are fairly straight forward:

$$S^{-1}I = S^{-1}\Big(\bigcap_{i=1}^{n} Q_i\Big) = \bigcap_{i=1}^{n} S^{-1}Q_i = \bigcap_{i=1}^{m} S^{-1}Q_i$$

since if $Q_i \cap S \neq \varnothing$, then Q_i contains a unit in $S^{-1}A$, so $S^{-1}Q_i = S^{-1}A$, and so doesn't influence the intersection.

The second one is similar. Since we have correspondence between primary ideals,

$$S(I) = c(S^{-1}I) = c\Big(\bigcap_{i=1}^{m} S^{-1}Q_i\Big) = \bigcap_{i=1}^{m} c(S^{-1}Q_i) = \bigcap_{i=1}^{m} Q_i. \qquad \square$$

With this in hand we are able to prove the second uniqueness theorem for primary decompositions:

Date: October 10, 2017.

Theorem 14.1.2 (Second uniqueness theorem)**.** *Let*

$$I = \bigcap_{i=1}^{n} Q_i$$

be a minimal primary decomposition with $P_i = \operatorname{rad}(Q_i)$*. Suppose* P_j *is a minimal element of* $\{ P_1, P_2, \ldots, P_n \}$ *under inclusion. Let* $S = A \setminus P_j$*. Then* $Q_j = S(I) = c(S^{-1}I)$ *is uniquely determined by* I *and* P_j*, i.e. the primary component belonging to a minimal prime is uniquely determined and does not depend on the primary decomposition.*

Proof. First note that since P_j is a minimal element of $\{ P_1, P_2, \ldots, P_n \}$, we have that $P_j \not\supset P_i$ for $i \neq j$, implying that $P_i \cap S \neq \varnothing$ for all $i \neq j$.

Therefore by the previous proposition, $S(I) = Q_j$. □

Example 14.1.3. Let $A = k[x, y]$. Then $I = (x^2, y^2) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$, with $\operatorname{rad}(x) = (x) = P_1$ and $\operatorname{rad}(x, y)^2 = (x, y) = \operatorname{rad}(x^2, y) = P_2$. We have $P_1 \subset P_2$, so P_1 is minimal and $Q_1 = (x)$ must therefore be in any primary decomposition of I. ▲

Note that since $\subset$ is a partial order, we can have multiple minimal elements.

14.2 Integral Ring Extensions

The goal of this next part is to try to generalise the idea of algebraic field extensions to the setting of rings. Recall how if we have a field extension F of a field k, then $u \in F$ is called ***algebraic*** over k if there exists a nonzero polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in k[x]$$

with $a_n \neq 0$ such that $f(u) = 0$. Since k is a field, all nonzero elements are units, meaning that they have multiplicative inverses, so we can always multiply by a_n^{-1} and get a monic polynomial. This is the prototype for our generalisation:

Definition 14.2.1 (Integral element)**.** Let $B \supset A$ be a ring extension. An element $b \in B$ is ***integral*** over A if there exists a monic polynomial

$$f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in A[x]$$

such that $f(b) = 0$.

Example 14.2.2. Let $A = \mathbb{Z} \subset B = \mathbb{Q}$. Suppose

$$b = \frac{r}{s} \in Q$$

is integral over $\mathbb{Z}$, with $\gcd(r, s) = 1$. Thus

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \ldots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

with $a_i \in \mathbb{Z}$. If we multiply by s^n, then

$$r^n + a_{n-1} r^{n-1} s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0,$$

which means that if we move all the terms with s over to the other side, we see that $s \mid r^n$. Since s and r are coprime, this means $s = \pm 1$, and so $b \in \mathbb{Z}$. Therefore all rational numbers integral over $\mathbb{Z}$ are $\mathbb{Z}$, motivating the name. ▲

We will eventually study the same structure for ***algebraic number fields***, i.e. finite extensions of $\mathbb{Q}$, so

$$\begin{array}{ccc} \mathbb{Q} & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathcal{O} \end{array}$$

with $\mathcal{O}$ being the ring of integers of the extensions.

Proposition 14.2.3. *Let $B \supset A$ be a ring extension. Let $x \in B$. The following are equivalent:*

(*i*) *$x \in B$ is integral over A.*

(*ii*) *$A[x]$ is a finitely generated A-module.*

(*iii*) *$A[x]$ is contained in a subring $C \subset B$ such that C is a finitely generated A-module.*

(*iv*) *There exists a faithful $A[x]$-module M which is finitely generated as an A-module.*

Proof. That (*i*) implies (*ii*) is seen as follows: Since $x \in B$ is integral over A, we have

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

with $a_i \in A$. Therefore

$$x^n = -(a_{n-1}x^{n-1} + \ldots + a_1 x + a_0),$$

whereby all x^m with $m \geq n$ can be expressed in terms of $1, x, \ldots, x^{n-1}$. Therefore $A[x]$ is finitely generated by these as an A-module.

To see that (*ii*) implies (*iii*), just take $C = A[x]$.

For (*iii*) implying (*iv*), take $M = C$. Suppose $b \in \mathrm{Ann}(M)$, meaning that $bM = 0$. We have $1 \in M = C \subset B$, so $b \cdot 1 = 0$, implying $b = 0$, meaning that $\mathrm{Ann}(M) = 0$, so M is faithful.

Finally (*iv*) implies (*i*): Consider $\phi\colon M \to M$ by $\phi(m) = mx$. This is an A-module homomorphism. By Cayley-Hamilton's theorem, we have

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_1\phi + a_0 = 0$$

with $a_i \in A$. Therefore

$$(x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0)M = 0,$$

so $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathrm{Ann}(M)$ over $A[x]$. But $\mathrm{Ann}(M) = 0$ since M is faithful, whereby

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

so x is integral over A. □

Corollary 14.2.4. *Let $x_1, x_2, \ldots, x_n \in B$ be integral over A.*

Then $A[x_1, x_2, \ldots, x_n]$ is a finitely generated A-module.

Proof. This follows immediately by induction—we add one x_i at a time and use the previous proposition. □

Corollary 14.2.5. *Let $B \supset A$ be a ring extension. Let*

$$C = \{\, x \in B \mid x \text{ integral over } A \,\}.$$

Then X is a subring of B containing A.

Proof. For $x, y \in C$, we wish to show that $x \pm y \in C$ and that $xy \in C$. Now $A[x, y]$ is a finitely generated A-module, and $A[x \pm y] \subset A[x, y]$, so by the previous proposition $x \pm y$ are integral over A, and similarly for xy. □

Note that it is quite cumbersome to prove this directly, i.e. given two polynomials with x and y as roots, constructing the polynomials with $x \pm y$ or xy as roots.

Definition 14.2.6 (Integral closure)**.** The ring C above is called the ***integral closure*** of A in B.
If $C = A$, then A is called ***integrally closed*** in B.
If $C = B$, then C is called ***integral*** over A.

Example 14.2.7. Consider $\mathbb{Q} \supset \mathbb{Z}$ again. We know $\mathbb{Z}[1/3]$ is not integral over $\mathbb{Z}$, so by the above $\mathbb{Z}[1/3]$ is not finitely generated as a $\mathbb{Z}$-module. (Indeed we know this already, from an exercise!) ▲

Example 14.2.8. Let A be an integral domain. Let $f \in A$ be a nonzero nonunit in A. Then $A[1/f]$ is not integral over A since it is not finitely generated as an A-module. ▲

Example 14.2.9. The golden ratio

$$x = \frac{1 + \sqrt{5}}{2}$$

is integral over $\mathbb{Z}$, since it is a root to the polynomial equation $x^2 - x - 1 = 0$. ▲

Example 14.2.10. The element

$$x = \frac{1 + \sqrt{3}}{2}$$

is not integral over $\mathbb{Z}$, since it is a root of $2x^2 - 2x - 1$, which is not monic. ▲

Example 14.2.11. Let k be a field. Then $k[x] \supset k[x^2] = A$ is an integral extension, since x is a root of $f(t) = t^2 - x^2 \in A[t]$, so x is integral over A. ▲

Lecture 15 Ring Extensions continued

15.1 Last Lecture, concluded

Corollary 15.1.1. *Let $A \subset B \subset C$ be ring extensions. Suppose B is integral over A and C is integral over B. Then C is integral A.*

Date: October 12, 2017.

In other words, the property of being integral is transitive.

Proof. Let $x \in C$. Then we have

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 = 0$$

with $b_i \in B$. Now consider $B' = A[b_0, b_1, \ldots, b_{n-1}] \subset B$. Then x is integral over B', and $B'[x]$ is a finitely generated B'-module. Moreover $B'[x] = A[b_0, b_1, \ldots, b_{n-1}, x]$, so B' is a finitely generated A-module by the proposition last lecture.

Therefore $B'[x]$ is a finitely generated A-module, and so $A[x]$ is integral over A. □

Corollary 15.1.2. *Let $A \subset B$ be a ring extension. Let C be the integral closure of A in B. Then C is integrally closed in B.*

Lecture 16 The Going-Up Theorem

16.1 Integral Dependence

Proposition 16.1.1. *Let $A \subset B$ be a ring extension. Assume B is integral over A.*

(*i*) *Let $J \subset B$ be an ideal and let $I = J \cap A$. Then B/J is integral over A/I.*

(*ii*) *Let S be a multiplicative subset of A. Then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof. In the proof of both we will let $x \in B$ which, being integral over A, satisfies an equation

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

with $a_i \in A$.

For (i), we reduce this equation modulo J, whereby $x + J$ is integral over A/I since it satisfies such an equation.

For (ii), let $x/s \in S^{-1}B$, with $x \in B$ as above and $s \in S$. We multiply the integral equation by $1/s^n$, so

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{a_1}{s^{n-1}}\left(\frac{x}{s}\right) + \frac{a_0}{s} = 0.$$

Now $a_i/s^{n-i} \in S^{-1}A$, so x/s is integral over $S^{-1}A$. □

Proposition 16.1.2. *Let $A \subset B$ be integral domains, and assume B is integral over A. Then B is a field if and only if A is a field.*

Proof. First assume B is a field, and let take any nonzero $x \in A \subset B$. Then $x^{-1} = y \in B$ since B is a field. We want to show that $y \in A$ as well. Now y is integral over A since it is in B, so

$$y^n + a_{n-1}y^{n-1} + \ldots + a_1 x + a_0 = 0$$

Date: October 17, 2017.

with $a_i \in A$. We solve for y:

$$\begin{aligned} y &= -y^{-(n-1)}(a_{n-1}y^{n-1} + \ldots + a_1 x + a_0) \\ &= -(a_{n-1} + a_{n-2}y^{-1} + \ldots + a_1 y^{-(n-2)} + a_0 y^{-(n-1)}) \\ &= -(a_{n-1} + a_{n-2}x + \ldots + a_1 x^{n-2} + a_0 x^{n-1}) \end{aligned}$$

which is in A since a_i and x are all in A. Therefore $x^{-1} \in A$, and so A is a field.

For the converse, take $y \neq 0$ in B. Since B is integral over A, we again have

$$y^n + a_{n-1}y^{n-1} + \ldots + a_1 x + a_0 = 0$$

with $a_i \in A$. Assume $a_0 \neq 0$, otherwise factor out and cancel a y—we're in an integral domain, so we have cancellation laws. Thus a_0 is a unit in A, so $a_0^{-1} \in A$. We then multiply by a_0^{-1} rearrange to solve for the resulting constant 1:

$$1 = -y a_0^{-1}(y^{n-1} + a_{n-1}y^{n-2} + \ldots + a_2 y + a_1),$$

and all terms are in B, so $y^{-1} \in B$, and so B is a field. □

Corollary 16.1.3. *Let $A \subset B$ be a ring extension. Assume B is integral over A. Let Q be a prime ideal of B, and let $P = Q \cap A$. Then Q is maximal in B if and only if P is maximal in A.*

Proof. First note that P is prime in A since Q is prime in B, since Q is the preimage of P under the inclusion.

By the first proposition of the lecture, B/Q is integral over A/P, and since Q and P are prime ideals, these quotients are integral domains.

So by the previous result, B/Q is a field if and only if A/P is a field, and so Q is maximal in B if and only if P is maximal in A. □

Example 16.1.4. Consider, as in the past, a number field K with its ring of integers:

$$\begin{array}{ccccc} K & \supset & \mathcal{O} & \supset & \mathcal{P} \neq 0 \text{ prime ideal} \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & (p). \end{array}$$

Now since (p) is a maximal ideal in $\mathbb{Z}$, by the last result $\mathcal{P}$ must also be maximal in $\mathcal{O}$.

In particular, consider $K = \mathbb{Q}(\sqrt{d})$, with d being square free. Then

$$\begin{array}{ccc} K = \mathbb{Q}(\sqrt{d}) & \supset & \mathcal{O} = \mathbb{Z}[\alpha] \\ | & & | \\ \mathbb{Q} & \supset & \mathbb{Z}. \end{array}$$

where α is $(1 + \sqrt{d})/2$ is $d \equiv 1 \pmod 4$ and $\alpha = \sqrt{d}$ is $d \not\equiv 1 \pmod 4$. ▲

Corollary 16.1.5. *Let $A \subset B$ be a ring extension. Assume B is integral over A, and let Q_1 and Q_2 be prime ideals of B such that $Q_1 \subset Q_2$. Moreover suppose $Q_1 \cap A = Q_2 \cap A = P$. Then $Q_1 = Q_2$.*

In other words, if we have two prime ideals above P, with one contained in the other, then the prime ideals coincide. If one is not contained in the other, this need not be the case.

Proof. Localising at P, we have that $S^{-1}P$ is the maximal ideal in the local ring A_P. Hence by the previous result $S^{-1}Q_1$ and $S^{-1}Q_2$ are maximal in B_P, and since one is contained in the other they must coincide, since they are both maximal.

Finally by the one-to-one correspondence of ideals, $Q_1 = Q_2$. □

Theorem 16.1.6. *Let $A \subset B$ be a ring extension. Suppose B is integral over A. Let $P \subset A$ be a prime ideal. Then there exists a prime ideal Q of B such that $Q \cap A = P$.*

Proof. The strategy is to localise both A and B at P, yielding

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & B_P \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_P. \end{array}$$

The reason for this is that if we take any maximal ideal $\mathfrak{m}$ in B_P, its intersection with A_P is a maximal ideal in A_P, but A_P is a local ring and has only the maximal ideal $S^{-1}P$.

But then $\varphi^{-1}(\mathfrak{m}) = Q$, and so it is prime in B, and since the diagram commutes we must also have $Q \cap A = P$. □

16.2 The Going-Up Theorem

Theorem 16.2.1 (Going-up theorem)**.** *Let $A \subset B$ be a ring extension. Assume B is integral over A. Let $P_1 \subset P_2 \subset P_3 \subset \ldots \subset P_n$ be a chain of prime ideals in A, and let $Q_1 \subset Q_2 \subset \ldots \subset Q_m$ be a shorter chain of prime ideals in B, i.e. $m < n$, and moreover $Q_i \cap A = P_i$ for $i = 1, 2, \ldots, m$. Then the chain of Q_i can be extended to $Q_1 \subset Q_2 \subset \ldots \subset Q_n$ such that $Q_i \cap A = P_i$ for $i = 1, 2, \ldots, n$.*

Before proving this we'll demonstrate the objective in a diagram. We want to find Q_2 in the diagram

$$\begin{array}{ccccccc} B & \subset & Q_1 & & & & Q_2 \\ | & & | & & & & \\ A & \subset & P_1 & \subset & P_2 & & \end{array}$$

in such a way that $Q_1 \subset Q_2$. By the previous proposition we already know that we can find *something* above P_2, so the clincher is the inclusion in Q_1.

Proof. It suffices to consider $n = 2$ and $m = 1$, since we could then repeat.

The way to accomplish the inclusion we desire is to work in $\bar{A} = A/P_1$ and $\bar{B} = B/Q_1$, since all ideals that remain after taking quotients are ones that contain the ideal we divided by. Now we know that $\bar{B}$ is integral over $\bar{A}$, and so by the previous proposition there exists a prime ideal $\bar{Q}_2 \subset \bar{B}$ such that $\bar{Q}_2 \cap \bar{A} = \bar{P}_2$.

Let $\varphi\colon B \to B/Q_1$, and like before let $Q_2 = \varphi^{-1}(\bar{Q}_2)$. Then $Q_2 \subset B$ is a prime ideal such that $Q_2 \cap A = P_2$, and we are done. □

Proposition 16.2.2. *Let $A \subset B$ be a ring extension, and let C be the integral closure of A in B. Let $S \subset A$ be a multiplicative subset. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. Suppose $b/s \in S^{-1}B$, which we know is integral over $S^{-1}A$. Then

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_1}{s_1}\left(\frac{b}{s}\right) + \frac{a_0}{s_0} = 0,$$

with $a_i/s_i \in S^{-1}A$, i.e. $a_i \in A$ and $s_i \in S$. Let $t = s_0 s_1 \cdot \ldots \cdot s_{n-1} \in S$, and multiply the integral equation above by $(st)^n$, whereby

$$(bt)^n + d_{n-1}(bt)^{n-1} + \ldots + d_1(bt) + d_0 = 0$$

with $d_i \in A$, meaning that bt is integral over A, and so $bt \in C$ since C is the integral closure of A. Therefore

$$\frac{b}{s} = \frac{bt}{st} \in S^{-1}C$$

hence $S^{-1}C$ is the integral closure of S^{-1} over $S^{-1}B$. □

Definition 16.2.3 (Integrally closed)**.** An integral domain is called ***integrally closed*** or ***normal*** if it is integrally closed in its field of fractions.

Example 16.2.4. We have seen already that $\mathbb{Z}$ is integrally closed over $\mathbb{Q}$, and since $\mathbb{Q}$ is its field of fractions, it is integrally closed.

In fact, any unique factorisation domain is integrally closed—the proof is almost identical to that of $\mathbb{Z}$ over $\mathbb{Q}$, modulo some small details. In particular $k[x_1, x_2, \ldots, x_n]$ with k a field is integrally closed. ▲

Proposition 16.2.5. *Let A be an integral domain. Then the following are equivalent:*

(*i*) *A is integrally closed.*

(*ii*) *A_P is integrally closed for every prime ideal P of A.*

(*iii*) *$A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A.*

Proof. Let k be the field of fractions of A, and let C be the integral closure of A in k. Consider the embedding $f\colon A \hookrightarrow C$, which induces $f_p\colon A_P \hookrightarrow C_P$ and $f_{\mathfrak{m}}\colon A_{\mathfrak{m}} \hookrightarrow C_{\mathfrak{m}}$.

Now A is integrally closed if and only if $A = C$, and likewise $A_P = C_P$ if and only if A_P is integrally closed, and the same for $A_{\mathfrak{m}}$. In other words A is integrally closed if and only if f is surjective, and we know surjectivity is a local property, so this is true if and only if f_P is surjective, if and only if $f_{\mathfrak{m}}$ is surjective, and we are done. □

Lecture 17 The Going-Down Theorem

17.1 The Going-Down Theorem

Lemma 17.1.1. *Let $A \subset B$ be a ring extension. Suppose B is integral over A. Let $I \subset A$ be an ideal and $b \in B$. Then the following are equivalent:*

Date: October 19, 2017.

(*i*) *b is integral over I;*

(*ii*) *b^n is integral over I for some $n \geq 1$;*

(*iii*) *$b^n \in IB$ for some $n \geq 1$ (i.e. $b \in \mathrm{rad}(IB)$).*

In particular, if I is integrally closed in B, then $I = \mathrm{rad}(I)$.

Proof. That (*i*) and (*ii*) are equivalent is trivial: if b is integral certainly b^n is, and if b^n is integral, then its integral equation is an integral equation for b, just with other powers.

Let us then prove that (*ii*) implies (*iii*). If b^n is integral over I, then we have

$$(b^n)^m + a_{m-1}(b^n)^{m-1} + \ldots + a_1(b^n) + a_0 = 0$$

for $a_i \in I$. If we rearrange this to solve for b^{nm} we get

$$b^{nm} = -(a_{m-1}(b^n)^{m-1} + \ldots + a_0),$$

which is in IB since the coefficients are in I and the powers of b are in B. Therefore $b^{nm} \in IB$, and we have (*iii*).

Next for (*iii*) implying (*i*) and (*ii*), we have $b^n \in IB$, meaning that

$$b^n = \sum_{i=1}^{k} a_i b_i$$

for $a_i \in I$ and $b_i \in B$. Let $M = A[b_1, b_2, \ldots, b_k]$, which is a finitely generated A-module since $b_1, b_2, \ldots, b_k$ are integral over A.

If we now define $\phi\colon M \to M$ by $\phi(x) = b^n x$, then $\phi(M) \subset IM$. By the generalised Cayley-Hamilton theorem, we have

$$\phi^m + a_1\phi^{m-1} + \ldots + a_m = 0$$

for $a_i \in I$. Now evaluate this at $1 \in M$, giving us

$$(b^n)^m + a_1(b_n)^{m-1} + \ldots + a_0 = 0,$$

whereby b and b^n are integral over I.

Finally assume I is integrally closed in B. The inclusion $I \subset \mathrm{rad}(I)$ is trivial, since this is true for all ideals. The opposite inclusion, $\mathrm{rad}(I) \subset I$, we get by noting that if $a \in \mathrm{rad}(I)$, then $a^n \in I \subset IB$. By (*iii*) implying (*i*), we have that a is integral over I, whereby $a \in I$, since I is integrally closed. □

Lemma 17.1.2. *Let $A \subset B$ be a ring extension, and $I \subset A$ an ideal. Let C be the integral closure of A in B, and let $e(I) = CI$, the extension of I in C. Then the integral closure of I in B is* $\mathrm{rad}(e(I)) = \mathrm{rad}(IC)$

Proof. By the above, the integral closure of I in C is $\mathrm{rad}(IC)$. So if $b \in B$ is integral over $I \subset A$, then $b \in C$ as well, so then integral closure of I in B is $\mathrm{rad}(IC)$ as well. □

Definition 17.1.3 (Algebraic element)**.** Let F be a field extension of a field k. An element $a \in F$ is ***algebraic*** over k if a is a root of a nonzero polynomial

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0 \in k[t],$$

with $a_n \neq 0$. Since k is a field we may assume $a_n = 1$, otherwise multiply through by a_n^{-1}. If $f(t)$ is the polynomial in $k[t]$ of smallest degree such that $f(a) = 0$ and f is monic, then we call f the ***minimal polynomial*** of a. This polynomial is unique.

Proposition 17.1.4. *Let $A \subset B$ be integral domains, and assume A is integrally closed. Let $I \subset A$ be an ideal, and suppose $b \in B$ is integral over I. Then b is algebraic over the field of fractions k of A, and its minimal polynomial over k is*

$$f(t) = t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

with $a_i \in \operatorname{rad}(I)$.

Proof. We want to show that $a_i \in \operatorname{rad}(I)$. Let L be the splitting field of $f(t)$ over k, wherein we have, say,

$$f(t) = (t - b_1)(t - b_2) \ldots (t - b_n).$$

Since b is integral over I, there exists some $g(t) \in I[t]$ such that $g(b) = 0$. Therefore $f(t) \mid g(t)$ in $k[t]$ by the division algorithm since f is minimal. Moreover this implies $g(b_i) = 0$ for all $i = 1, 2, \ldots, n$, and therefore b_i are integral over I.

Expanding the polynomial f we have

$$f(t) = (t - b_1)(t - b_2) \ldots (t - b_n) = t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

where a_k are polynomials in b_i. Now since b_i are integral over I, so are the a_k, and so by the previous lemma we have $a_k \in \operatorname{rad}(I)$, since I is its own extension since A is integrally closed. □

Theorem 17.1.5 (Going-down)**.** *Let $A \subset B$ be integral domains. Assume B is integral over A and that A is integrally closed. Let $P_1 \supset P_2$ be prime ideals of A and Q_1 a prime ideal in B such that $Q_1 \cap A = P_1$. Then there exists a prime ideal Q_2 of B such that $Q_1 \supset Q_2$ and $Q_2 \cap A = P_2$.*

To prove this we use the following lemma:

Lemma 17.1.6. *Let $\phi \colon A \to B$ be a ring homomorphism. Let $P \subset A$ be a prime ideal. Then P is the contraction of a prime ideal of B if and only if $c(e(P)) = P$.*

Proof. □

Proof of theorem. By the lemma, it suffices to show that $B_{Q_1} P_2 \cap A = P_2$, so by the lemma there exists a prime $\bar{Q}_2 \subset B_{Q_1}$ such that $\bar{Q}_2 \cap A = P_2$. Take $\bar{Q}_2 \cap B \coloneqq Q_2$.

Suppose $B_{Q_1} P_2 \cap A \neq P_2$. Then there exists $x \in B_{Q_1} P_2 \cap A$ with $x \notin P_2$. Note that since $x \in B_{Q_1} P_2$, we have $x = y/s$ for $y \in BP_2$ and $s = S = B \setminus Q_1$. Then by the earlier lemma, specifically (iii) implying (i), we know that y is

integral over P_2, and so by the proposition the minimal polynomial of y over the quotient field k of A is of the form

$$f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$$

with $a_i \in \mathrm{rad}(P_2) = P_2$ since P_2 is prime. Therefore

$$y^n + a_{n-1}y^{n-1} + \ldots + a_1 y + a_0 = 0,$$

which if we multiply by $1/x^n$ becomes

$$\big(\frac{y}{x}\big)^n + \frac{a_{n-1}}{x}\big(\frac{y}{x}\big)^{n-1} + \ldots + \frac{a_1}{x^{n-1}}\big(\frac{y}{x}\big) + \frac{a_0}{x^n} = 0.$$

Now $y/x = s$, so

$$s^n + \frac{a_{n-1}}{x}s^{n-1} + \ldots + \frac{a_1}{x^{n-1}}s + \frac{a_0}{x^n} = 0$$

and so

$$g(t) = t^n + \frac{a_{n-1}}{x}t^{n-1} + \ldots + \frac{a_1}{x^{n-1}}t + \frac{a_0}{x^n} \in k[t]$$

is the minimal polynomial of s in $k[t]$ (if it isn't minimal, we could reduce the degree by f, but f is minimal, so that can't be the case).

Now $s \in S = B \setminus Q_1$. Since $s \in B$ is integral over A, we have

$$\frac{a_{n-1}}{x^i} \in \mathrm{rad}(A) = A$$

and so

$$\frac{a_{n-i}}{x^i} = d_i \in A.$$

Moreover $a_{n-i} = d_i x^i$, where the left-hand side if in P_2 but x^i is not, so by P_2 being prime we have $d_i \in P_2$. Therefore $g(t) \in P_2[t]$, so s is integral over P_2, implying that $s^n \in P_2 B \subset P_1 B \subset Q_1$, but $s \notin Q_1$, which is a contradiction. Therefore, recalling that our assumption was $B_{Q_1}P_2 \cap A \neq P_2$, we must instead have $B_{Q_1}P_2 \cap A = P_2$. □

Counterexample 17.1.7. To see that this does not work if A isn't integrally closed, consult page 32 of 'Commutative Algebra' by Matsumaia. ▲

Lecture 18 Valuation Rings

18.1 Between Rings and Fields

Theorem 18.1.1. *Let A be a subring of the field K and $h\colon A \to C$ a ring homomorphism where C is an algebraically closed field. If $\alpha \neq 0$ is in $K \setminus A$, then either h can be extended to a ring homomorphism $\bar{h}\colon A[\alpha] \to C$ or to $\bar{h}\colon A[\alpha^{-1}] \to C$.*

Date: October 24, 2017.

Proof. We reduce to the case when A is a local ring and $F = h(A)$ is a subfield of C. Let P be the kernel of h. Then $P \subset A$ is a prime ideal (since 0 is a prime ideal in C, and $\ker h$ is the pullback of it). Extend h to $g\colon A_P \to C$ by $g(a/s) = h(a)/h(s)$ with $s \in A \setminus P$. Therefore $h(s) \neq 0$, so the inverse of $g(a/s)$ exists in C. Moreover $A_P \subset K$ as well, and $\ker g = PA_P$ is the maximal ideal in A_P, so by the First isomorphism theorem

$$g(A_P) = \operatorname{Im} g \cong \frac{A_P}{\ker g} = \frac{A_P}{PA_P},$$

a field. So we replace (h, A) with (g, A_P).

Thus we assume A is local and that $F = h(A)$ a subfield of C. First extend h to a surjective homomorphism of polynomial rings $h\colon A[x] \to F[x]$ in the following way: the elements in $A[x]$ are

$$f(x) = \sum_{i=1}^{n} a_i x^i \in A[x]$$

and so

$$h(f) = \sum_{i=1}^{n} h(a_i) x^i.$$

We can't just replace x by α since it might not make h well-defined (we could add any polynomial which vanishes in α).

Let

$$I = \{\, f \in A[x] \mid f(\alpha) = 0 \,\}.$$

Then $J = h(I)$ is an ideal of $F[x]$ (this is easy to see—if two polynomials vanish in α, so do their sum, and if one polynomial vanishes in α, so does the product of it and anything else). Since F is a field, $F[x]$ is a principle ideal domain by the division algorithm, meaning that $J = (p(x))$ for some $p(x) \in F[x]$.

We have three possibilities. First, $p(x)$ is nonconstant. Then $p(x)$ has a root $\beta \in C$ since C is algebraically closed. Define $\bar{h}\colon A[\alpha] \to C$ by $\bar{h}(\alpha) = \beta$. Then $\bar{h}$ is well-defined, since if $g(\alpha) = g(\alpha) + f(\alpha)$ for $f \in I$, we have

$$\bar{h}(g(\alpha)) = \bar{h}(g(\alpha) + f(\alpha)) = \bar{h}(g(\alpha)) + \bar{h}(f(\alpha)).$$

Since $h(f) \in J = (p(x))$, we have $h(f) = p(x)q(x)$ for some $q(x) \in F[x]$ which means that

$$\bar{h}(f(\alpha)) = p(\beta)q(\beta) = 0,$$

so $\bar{h}$ is well-defined.

Secondly, if $p(x)$ is identically 0, i.e. $J = (0)$, then α is a free variable—everything goes to 0. So defining $\bar{h}(\alpha) = \beta$ with β arbitrary is sufficient.

Third and finally, suppose $p(x) = c \neq 0$. This means that $J = (1)$, the whole space, and so there exists some $f \in I$ such that $h(f) = 1$. If

$$f(x) = a_r x^r + a_{r-1} x^{r-1} + \ldots + a_1 x + a_0 \in A[x]$$

then

$$\sum_{i=0}^{r} a_i \alpha^i = 0 \tag{18.1.1}$$

since $f \in I$. Moreover $h(f) = 1$, so $h(a_0) = 1$ and $h(a_i) = 0$ for $i = 1, 2, \ldots, r$. Let r be the smallest degree amongst such f, and consider α^{-1}.

If α^{-1} is in the first or second case, then we extend $\bar{h}\colon A[\alpha^{-1}] \to C$. Hence we can assume α^{-1} is also in the third case, so we have

$$\sum_{i=0}^{s} b_i(\alpha^{-1})^i = 0 \tag{18.1.2}$$

with $b_i \in A$, $h(b_0) = 1$, and $h(b_i) = 0$ for $i = 1, 2, \ldots, s$, and s is the smallest degree amongst these.

Without loss of generality we assume $r \geq s$. Note that $h(b_0) = 1 = h(1)$, meaning that $1 - b_0 \in \ker h \subset M$, the unique maximal ideal of A. Therefore $1 - (1 - b_0) = b_0$ is a unit in A, so $b_0^{-1} \in A$.

Multiplying (18.1.2) by $b_0^{-1}\alpha^s$ we get

$$\alpha^s + b_0^{-1}b_1\alpha^{s-1} + \ldots + b_0^{-1}b_s = 0 \tag{18.1.3}$$

where the coefficients are in A. Now if $r > s$, then (18.1.1) minus α^{r-s} times (18.1.3) produces a smaller degree r satisfying (18.1.1), which is a contradiction since we assumed minimality.

Next if $r = s$, then (18.1.1) minus a_r times (18.1.3) is 0, so $a_0 = a_r b_0^{-1} b_s$, but

$$h(a_0) = h(a_r b_0^{-1} b_s) = 0$$

where the left-hand side if 1 but the right-hand side is 0 because of b_s, which is a contradiction. □

Definition 18.1.2. A subring B of a field K is called a ***valuation ring*** of K if for every non-zero $\alpha \in K$ either $\alpha \in B$ or $\alpha^{-1} \in B$ (or both).

Example 18.1.3. The field K is a valuation ring of itself. ▲

Example 18.1.4. Take $K = \mathbb{Q}$ and $p \in \mathbb{Z}$ a prime. Then

$$\mathbb{Z}_p = \left\{ \frac{p^r m}{n} \in \mathbb{Q} \;\middle|\; r \geq 0, \gcd(m, p) = \gcd(n, p) = 1 \right\}$$

is a valuation ring of $\mathbb{Q}$. ▲

Let K be a field and C an algebraically closed field. Let

$$\Sigma = \{\, (A, f) \mid A \text{ a subring of } K,\ f\colon A \to C \text{ a ring homomorphism} \,\}.$$

We define a partial order on Σ as follows: $(A, f) \leq (B, g)$ if and only if $A \subset B$ and $g\big|_A = f$. That is to say, (B, g) is an extension of (A, f).

It is easy to verify that Σ satisfies the conditions of Zorn's lemma, meaning that Σ has at least one maximal element.

Theorem 18.1.5. *Let (B, g) be a maximal element of Σ. Then B is a valuation ring of the field K.*

Proof. Let $\alpha \neq 0$, $\alpha \in K$. Then g has an extension to $B[\alpha]$ or $B[\alpha^{-1}]$. By maximality of (B, g) we must therefore have $B[\alpha] = B$ or $B[\alpha^{-1}] = B$, meaning that $\alpha \in B$ or $\alpha^{-1} \in B$. □

Proposition 18.1.6. *Let B be a valuation ring of K. Then*

(*i*) *The fractional field of B is K.*

(*ii*) *If A is a subring such that $B \subset A \subset K$, then A is a valuation ring of K.*

(*iii*) *B is a local ring.*

(*iv*) *B is integrally closed in K.*

Proof. For (i), simply note that $\alpha \in K$ implies $\alpha \in B$ or $\alpha^{-1} \in B$. In the first case we are done, and in the second we note that $1/\alpha^{-1} = \alpha$, and again we are done.

For (ii), if $\alpha \in K$ we have $\alpha \in B$ or $\alpha^{-1} \in B$, but since $A \supset B$, the elements in B are also in A.

Taking on (iii), let M be the set of non-units in B. Hence $x \in M$ if and only if $x = 0$ or $x^{-1} \notin B$. We claim that M is an ideal of B, in which case B is a local ring.

First we check that $BM \subset M$, which is true since $ax \in M$ for nonzero $a \in B$ and $x \in M$, for otherwise $ax \notin M$ implies $(ax)^{-1} \in B$, but then $(ax)^{-1}a = x^{-1} \in B$, a contradiction.

Secondly, if nonzero $x, y \in M$, then we need to show that $x + y \in M$. But we have either $x/y \in B$ or $y/x \in B$ since B is a valuation ring. Without loss of generality assume the former. Then

$$x + y = y\big(\frac{x}{y} + 1\big) \in BM \subset M,$$

hence M is an ideal in B.

Finally for (iv), suppose $x \in K$ is integral over K. Then

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 = 0$$

with $b_i \in B$. If $x \in B$, we are done, and if $x \notin B$ then we must have $x^{-1} \in B$, in which case the above integral equation multiplied by $(x^{-1})^{n-1}$ yields

$$x = -(b_{n-1} + b_{n-2}x^{-1} + \ldots + b_0(x^{-1})^{n-1})$$

where the left-hand side is in B, so $x \in B$, which is a contradiction. □

Lecture 19 Chain Conditions

19.1 Valuation Rings and Integral Closures

Proposition 19.1.1. *Let B be a valuation ring of the field K. For any ideals I and J in B, we have either $I \subset J$ or $J \subset I$. In other words, the ideals of a valuation ring are ordered by inclusion.*

Proof. Suppose $I \not\subset J$, i.e. there exists some $a \in I$ such that $a \notin J$. Since all ideals contain 0, this automatically means $a \neq 0$.

We claim that $J \subset I$.

Date: October 26, 2017.

For any nonzero $b \in J$, we have $a/b \in K$, so either $a/b \in B$ or $b/a \in B$ since B is a valuation ring. In the case of the first one, $b \cdot a/b = a \in J$ since $b \in J$ and J is an ideal, which is a contradiction since $a \notin J$. Therefore we must have $b/a \in B$, meaning that $a \cdot b/a = b \in I$, so $J \subset I$, and we are done. □

The converse is true as well:

Proposition 19.1.2. *Let B be an integral domain and K be its field of fractions. Suppose the ideals of B are totally ordered by inclusion. Then B is a valuation ring.*

Proof. Suppose $\alpha \in K$, $\alpha \neq 0$. Then we can write $\alpha = a/b$ with $a, b \in B$ since K is its quotient field. Let $I = (a)$ and $J = (b)$, which by assumption means that either $I \subset J$ or $J \subset I$.

If $(a) \subset (b)$, then $a = bc$ for some $c \in B$, and therefore $\alpha = a/b = c \in B$.

If on the other hand $(b) \subset (a)$, then $b = ac$ for some $c \in B$, meaning that $\alpha^{-1} = b/a = c \in B$. □

Corollary 19.1.3. *Let B be a valuation ring of the field K. If $P \subset B$ is a prime ideal, then B_P and B/P are valuation rings of their respective quotient fields.*

Proof. This follows directly from the past two propositions: B being a valuation ring means that its ideals are totally ordered by inclusion, and that order remains after localisation or quotient. □

Proposition 19.1.4. *Let A be a subring of a field K. Then the integral closure $\bar{A}$ of A in K is the intersection of all valuation rings B of K such that $B \supset A$, i.e.*

$$\bar{A} = \bigcap_{\substack{B \supset A \\ B \text{ valuation ring}}} B.$$

Proof. We start by showing $\bar{A} \subset \bigcap_{B \supset A} B$. For $a \in \bar{A}$, a is integral over A, meaning that a is integral over B, but B is integrally closed since it is a valuation ring, so $a \in B$.

For $\bigcap_{B \supset A} B \subset \bar{A}$, we note that this is true if and only if $a \notin \bar{A}$ implies $a \notin B$, for some valuation ring $B \supset A$.

Suppose $a \notin \bar{A}$. Then $a \notin A' = A[a^{-1}]$, otherwise

$$a = b_n(a^{-1})^n + b_{n-1}(a^{-1})^{n-1} + \ldots + b_1 a^{-1} + b_0$$

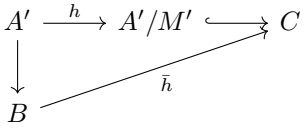
with $b_i \in A$. If we multiply this by a^n we get

$$a^{n+1} = b_n + b_{n-1}a + \ldots + b_1 a^{n-1} + b_0 a^n.$$

Therefore a is integral over A, so $a \in \bar{A}$, which is a contradiction.

Thus a^{-1} is not a unit in A', meaning that $a^{-1} \in M' \subset A'$, with M' being a maximal ideal of A'.

Now let C be an algebraic closure of the field $k' = A'/M'$, and consider $h\colon A' \to A'/M' \hookrightarrow C$. Then by last lecture h has a maximal extension $\bar{h}\colon B \to C$ for some evaluation ring B of K. When $B \supset A' \supset A$, we have



Now since $a^{-1} \in M'$, we have $\bar{h}(a^{-1}) = h(a^{-1}) = 0$. If $a \in B$, then

$$1 = \bar{h}(1) = \bar{h}(a \cdot a^{-1}) = \bar{h}(a)\bar{h}(a^{-1}) = 0,$$

so $1 = 0$, a contradiction, whereby $a \notin B$. □

Corollary 19.1.5. *Let A be an integral domain with fraction field K. Then A is integrally closed if and only if*

$$A = \bigcap_{\substack{B \supset A \\ B \text{ valuation ring}}} B.$$

19.2 Chain Conditions

If we have a k-vector space V with finite dimension, and V has a subspace W, then we know that W automatically has finite dimension as well.

If, however, M is an A-module, then even if M is finitely generated, a submodule N of M might not be. We will concern ourselves in the near future with the special case where the submodules do inherit the finite generation.

First a statement purely about set theory:

Proposition 19.2.1. *Let Σ be a set that is partially ordered by $\leq$. Then the following conditions on Σ are equivalent:*

(*i*) *Σ satisfies the* **ascending chain condition***, meaning that every chain $x_1 \leq x_2 \leq x_3 \leq \ldots$ in Σ is stationary, i.e. there exists some n such that $x_n = x_{n+1} = \ldots$.*

(*ii*) *Every nonempty subset of Σ has a maximal element.*

Proof. To see that (*i*) implies (*ii*), suppose $S \subset \Sigma$ is nonempty with no maximal element. So for $s_1 \in S$ there must exist some $s_2 \in S$ such that $s_1 < s_2$, and for s_2 there must exist an s_3 with $s_2 < s_3$, and so forth, and since there is no maximal element in S this cannot stop, which is a contradiction since $s_1 < s_2 < s_2 < \ldots$ is a chain, which by (*i*) must be stationary.

For the converse, take a chain $x_1 \leq x_2 \leq x_3 \leq \ldots$ and let $S = \{ x_i \}_{i=1}^{\infty}$. Then by (*ii*) S has a maximal element, say x_n, and so $x_n = x_{n+1} = \ldots$, and we are finished. □

This can also be cone with $\geq$, in which case we consider the ***descending chain condition***, which is then equivalent with $S \neq \varnothing$ having a minimal element.

Definition 19.2.2 (Noetherian and Artinian rings)**.** Let Σ be the set of submodules of a module M, ordered by $\subset$ and $\supset$.

Then M is called ***Noetherian*** if Σ satisfies the ascending chain condition, and M is called ***Artinian*** if Σ satisfies the descending chain condition.

Example 19.2.3. A finite abelian group (read: $\mathbb{Z}$-module) satisfies both the ascending chain condition and the descending chain condition.

The ring $\mathbb{Z}$, seen as a $\mathbb{Z}$-module, satisfies the ascending chain condition but not the descending chain condition. This follows from $(n) \supset (m)$ being equivalent with $m \mid n$, and we couldn't keep on factoring distinct terms forever. However for $a \neq 0, \pm 1$, we have

$$(a) \supsetneq (a^2) \supsetneq (a^3) \supsetneq \dots$$

which never stops.

Let k be a field. The ring $k[x]$ satisfies the ascending chain condition but not the descending chain condition, for exactly the same reason as with $\mathbb{Z}$—it's a principal ideal domain, and

$$(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \dots. \qquad \blacktriangle$$

We think of a ring A as an A-module, wherein the submodules are the ideals of A. Therefore

Definition 19.2.4 (Notherian and Artinian rings)**.** A ring A is called ***Noetherian*** if it is Noetherian as an A-module. Similarly A is called ***Artinian*** if it is Artinian as an A-module.

Remark 19.2.5. We shall prove later on that if a ring A is Artinian (i.e. has the descending chain condition) then it is also Noetherian (meaning it has the ascending chain condition).

Proposition 19.2.6. *An A-module M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. For the forward direction, let N be a submodule of M. Let

$$\Sigma = \{\, N' \subset N \mid N' \text{ is a finitely generated submodule} \,\}.$$

Then $\Sigma \neq \varnothing$ since at least $0 \in \Sigma$. Hence Σ has a maximal element, say N_0. We claim that $N_0 = N$.

Suppose $N_0 \supsetneq N$. Then there exists $x \in N$ such that $x \notin N_0$. Consider the submodule $N' = N_0 + Ax$. This is finitely generated, and $N_0 \subsetneq N'$, which is a contradiction, since N_0 is maximal.

For the converse, let

$$M_1 \supset M_2 \subset M_3 \subset \dots$$

be a chain of submodules of M. Then

$$N = \bigcup_{n=1}^{\infty} M_n$$

is a submodule of M—note that unions of submodules aren't generally submodules, but due to the inclusions this is the case here. Hence N is finitely generated since every submodule is, say by $x_1, x_2, \dots, x_k$, with $x_i \in M_{n_i}$. Take $n = \max\{\, n_i \,\}$, whereby $x_1, x_2, \dots, x_k \in M_n$. This means that $M_n = M_{n+1} = \dots$, since M_n contains all of the generators, so the chain is stationary. $\square$

Proposition 19.2.7. *Let*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

be a short exact sequence of A-modules. Then

(*i*) *M is Noetherian if and only if L and N are Noetherian.*

(*ii*) *M is Artinian if and only if L and N are Artinian.*

Proof. For the forward direction of (i), we have that every ascending chain in L is ascending in M, and since α is injective we can think of L as submodules of M, whereby the chain is stationary, so L is Noetherian.

Next let $N_1 \subset N_2 \subset N_3 \subset \dots$ be an ascending chain in N. Taking the pullback, we have

$$\beta^{-1}(N_1) \subset \beta^{-1}(N_2) \subset \beta^{-1}(N_3) \subset \dots$$

as an ascending chain in M. Since this chain is in M, which is Noetherian, it is stationary, stopping at, say, $\beta^{-1}(N_k)$, i.e. $\beta^{-1}(N_k) = \beta^{-1}(N_{k+1}) = \dots$. Mapping back through β we have $\beta(\beta^{-1}(N_k)) = N_k$, and our chain is stationary in N as well.

For the converse, let $M_1 \subset M_2 \subset \dots$ be an ascending chain in M. Then $L \cap M_1 \subset L \cap M_2 \subset \dots$ is an ascending chain in L, whereby it's stationary.

Next consider $\beta(M_1) \subset \beta(M_2) \subset \dots$, an ascending chain in N, whereby it is stationary.

Now take the largest index n from the chain in L and N, and show that $M_n = M_{n+1}$. □

Lecture 20 Noetherian Rings

We start by finishing off the proof from last time.

Proof continued. We left off with trying to show that $M_n = M_{n+1} = \dots$, i.e. that our chain is stationary.

Since our chain is ascending by assumption, it suffices to show $M_{n+1} \subset M_n$. For $x \in M_{n+1}$, we have $\beta(x) \in \beta(M_{n+1}) = \beta(M_n)$. Therefore there exists some $y \in M_n$ such that $\beta(x) = \beta(y)$, meaning that $\beta(x - y) = 0$ since β is a homomorphism, and so $x - y \in \ker \beta = \operatorname{Im} \alpha = L$ by exactness. In other words $x \in M_{n+1}$, and $y \in M_n \subset M_{n+1}$, so $x - y \in L \cap M_{n+1} = L \cap M_n$, meaning that $x = (x - y) + y \in M_n$. □

20.1 When are Submodules Noetherian?

Corollary 20.1.1. *If $M_1, M_2, \dots, M_n$ are Noetherian (respectively Artinian) A-modules, then*

$$\bigoplus_{i=1}^{n} M_i$$

is Noetherian (respectively Artinian).

Date: October 31, 2017.

Proof. Since the sequence

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$

is exact, the previous proposition gives us the corollary for $n = 2$. For $n > 2$, we use induction on

$$0 \longrightarrow M_1 \longrightarrow \bigoplus_{n=1}^{n} M_i \longrightarrow \bigoplus_{i=2}^{n} M_i \longrightarrow 0. \qquad \square$$

Example 20.1.2. Any principal ideal domain is Noetherian, since all ideals—which we view as the submodules—are generated by a single element, hence finitely generated. ▲

Example 20.1.3. Let k be a field and consider $A = k[x_1, x_2, \ldots]$. This is not a Noetherian ring, since

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \ldots$$

isn't stationary.

But A is an integral domain, meaning that it has a quotient field K, which is Noetherian—it has only two ideals, (0) and $(1) = K$, both of which are clearly finitely generated. ▲

This serves to indicate that a subring of a Noetherian ring doesn't have to be Noetherian, essentially because they aren't necessarily ideals.

Proposition 20.1.4. *Let A be a Noetherian (respectively Artinian) ring. Let M be a finitely generated A-module. Then M is Noetherian (respectively Artinian).*

Proof. We think about what it means for a module to be finitely generated. If M is finitely generated, then $M \cong A^n/N$ for some n and submodule N. Then the sequence

$$0 \longrightarrow N \longrightarrow A^n \longrightarrow \tfrac{A_n}{N} \cong M \longrightarrow 0$$

is exact. By assumption A is Noetherian, meaning that A^n is Noetherian, and by our result from last time, then, $A^n/N \cong M$ is Noetherian. $\square$

Proposition 20.1.5. *Let A be a Noetherian ring and $I \subset A$ an ideal. Then A/I is a Noetherian ring.*

Proof. The sequence

$$0 \longrightarrow I \longrightarrow A \longrightarrow \tfrac{A}{I} \longrightarrow 0$$

is exact, meaning that A/I is Noetherian as an A-module. Since I annihilates it, we can carry this process over and view A/I as a Noetherian A/I-module, and thus as a ring. $\square$

Lecture 21 More on Noetherian Rings

21.1 Noetherian Rings Have Decomposable Ideals

Recall that we know by now that the ring A being Noetherian means that it satisfies the following equivalent conditions:

(i) Every nonempty set of ideals in A has a maximal element.

(ii) Every ascending chain of ideals in A is stationary.

(iii) Every ideal in A is finitely generated.

Proposition 21.1.1. *Let $\phi\colon A \to B$ be a surjective ring homomorphism. If A is Noetherian, then B is Noetherian.*

Proof. Since ϕ is surjective, we have by the first isomorphism theorem that $B \cong A/\ker\phi$, and this quotient is Noetherian since all of its ideals come from ideals in A, which are finitely generated. □

Proposition 21.1.2. *Let $A \subset B$ be rings. Suppose A is Noetherian and B is finitely generated as an A-module. Then B is Noetherian.*

Proof. Since A is Noetherian, B is Noetherian as an A-module. Therefore every submodule of B is finitely generated over A, meaning that it is also fintely generated over A since $A \subset B$. Thus B is a Noetherian B-module as well, and so it's a Noetherian ring. □

Proposition 21.1.3. *Let A be a Noetherian ring and $S \subset A$ a multiplicative set. Then $S^{-1}A$ is Noetherian.*

Proof. Let $\varphi\colon A \to S^{-1}A$, and recall that we have a one-to-one correspondence between ideals I in A and $S^{-1}I = e(I)$ in $S^{-1}A$. Now $\varphi(I)$ is a generator of $e(I)$, and I itself is finitely generated, so $\varphi(I)$ is too. □

Corollary 21.1.4. *If A is Noetherian and $P \subset A$ a prime ideal, then A_P is Noetherian.*

Remark 21.1.5. The converse is false—though counterexamples are very much nontrivial—meaning that Noetherian is *not* a local property.

Recall how if k is a field, then $k[x]$ is a principle ideal domain, and therefore Noetherian. Surprisingly, the same is true for polynomial rings over Noetherian rings as well.

Theorem 21.1.6 (Hilbert basis theorem)**.** *If A is Noetherian, then $A[x]$ is Noetherian.*

Proof. Let $I \subset A[x]$ be an ideal and define

$$J_n = \{\, a \in A \mid \text{there exists } f(x) \in I \text{ such that } f(x) = ax^n + \dots \,\}.$$

In other words J_n is the set of coefficients $a \in A$ such that there are degree n polynomials in I with a as their leading coefficients. It is not hard to see that

Date: November 2, 2017.

J_n is an ideal in A, effectively since I itself is an ideal in $A[x]$. Moreover we have an ascending chain, since $J_n \subset J_{n+1}$ since I is an ideal, meaning that a polynomial in J_n will be in J_{n+1} by multiplying it by x.

Thus

$$J_1 \subset J_2 \subset J_3 \subset \dots$$

in A, which is Noetherian, so it is stationary. Thus $J_n = J_{n+1} = \dots$ for some n, and all J_m are finitely generated, say by $a_{m,1}, a_{m,2}, \dots, a_{m,k_m}$. So there exists $f_{m,j}(x) = a_{m,j}x^m + \dots$ in I.

We claim that the set

$$\{ f_{m,j}(x) \}_{\substack{1 \le m \le n \\ 1 \le j \le k_m}}$$

generates I.

To prove this, let $F(x) = ax^s + \dots \in I$. If $\deg f = s \ge n$, then $a \in J_s = J_n = (a_{n,1}, a_{n,2}, \dots, a_{n,k_n})$. Therefore

$$a = \sum_{i=1}^{k_n} b_i a_{n,i},$$

and therefore

$$f(x) - \sum_{i=1}^{k_n} b_i f_{n,i}(x) x^{s-n}$$

is a polynomial in I with smaller degree—specifically less than or equal to $s-1$. Repeat this until $s = n$.

Then, for $\deg f = s \le n$, we again have $a \in J_s = (a_{s,1}, a_{s,2}, \dots, a_{s,k_s})$, with

$$f(x) - \sum_{i=1}^{k_s} b_i f_{s,i}(x)$$

in I of degree less than or equal to $s-1$, so we can again continue inductively until $s = 0$, and so $f(x)$ is a linear combination of $f_{m,j}(x)$. □

We can extend this inductively:

Corollary 21.1.7. *If A is Noetherian, then $A[x_1, x_2, \dots, x_n]$ is Noetherian.*

Definition 21.1.8 (Algebra)**.** Let A and B be rings. Then B is an ***A-algebra*** if

(*i*) B is an A-module, and

(*ii*) $a(b_1 b_2) = (ab_1)b_2$ for $a \in A$ and $b_1, b_2 \in B$.

Basically, we want the operations in B to be compatible with those of A.

Corollary 21.1.9. *Let B be a finitely generated A-algebra. If A is Noetherian, then B is a Noetherian ring. In particular every finitely generated algebra over $\mathbb{Z}$ or a field k is Noetherian.*

Proof. Much like how a finitely generated module of A can be identified as A^n/N for some submodule N, we can identify B as $B \cong A[x_1, x_2, \dots, x_n]/N$ for some subalgebra, and this is Noetherian by the Hilbert basis theorem. □

A while ago we went through great pains to prove several interesting results about primary decompositions, but each theorem began with assuming decomposability. It turns out that if we work over Noetherian rings, this is not a problem:

Theorem 21.1.10. *Let A be a Noetherian ring. Then every ideal of A has a primary decomposition.*

We'll prove this by means of two lemmas, but first:

Definition 21.1.11 (Irreducible ideal)**.** An ideal $I \subset A$ is ***irreducible*** if $I = J_1 \cap J_2$, J_1 and J_2 ideals, then $I = J_1$ or $I = J_2$. An ideal which is not irreducible is called ***reducible***.

Lemma 21.1.12. *Let A be a Noetherian ring. Then every ideal in A is a finite intersection of irreducible ideals.*

Proof. Suppose this is not the case, and let Σ be the set of ideals in A that cannot be written as finite intersections of irreducible ideals. Then Σ is nonempty by our supposition, and since A is Noetherian, Σ has a maximal element, call it I. Then I is reducible, so $I = J_1 \cap J_2$ with $J_1 \supsetneq I$ and $J_2 \supsetneq I$.

By maximality of I, we have $J_1, J_2 \notin \Sigma$, meaning that J_1 and J_2 are finite intersections of irreducible ideals, and so $I = J_1 \cap J_2$ is as well, which is a contradiction. □

Lemma 21.1.13. *Let A be a Noetherian ring. Then every irreducible ideal in A is primary.*

Proof. First note that $I \subset A$ is irreducible if and only if (0) is irreducible in A/I. The forward direction of this is quite clear. The converse direction follows from noting that if $(0) = \bar{J}_1 \cap \bar{J}_2$, then $J_1 \cap J_2 = I$ since $I = (0)$ in the quotient.

Next, $I \subset A$ is primary if and only if (0) is primary. It suffices to show that if (0) in A is irreducible, then (0) is primary. Hence suppose $xy = 0$, and $y \neq 0$. We therefore need to show that $x^n = 0$ for some $n \geq 1$. Consider the ideals

$$\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \mathrm{Ann}(x^3) \subset \dots$$

which, since A is Noetherian, is stationary, so $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \dots$ for some n. We claim $(x^n) \cap (y) = (0)$. Suppose $a \in (x^n) \cap (y)$. Then $a \in (y)$ implies $a = by$ for some b, so $ax = byx = 0$ since $yx = 0$ Since $a \in (x^n)$, we also have $a = cx^n$ for some c, which means that if we multiply both sides by x, we get $ax = cx^{n+1} = 0$ by the above.

Thus $c \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$, meaning that $cx^n = 0 = a$, so $a = 0$, and therefore $(0) = (x^n) \cap (y)$, (0) is irreducible, and $(y) \neq (0)$, so we must have $(x^n) = 0$, meaning that $x^n = 0$, meaning that (0) is primary. □

Proposition 21.1.14. *Let A be Noetherian and $I \subset A$ an ideal. Then $I \supset \mathrm{rad}(I)^n$ for some $n \geq 0$.*

Since $I \subset \mathrm{rad}(I)$ for all I, thus means that in the particular case of Noetherian rings, we have

$$\mathrm{rad}(I)^n \subset I \subset \mathrm{rad}(I).$$

Proof. Since $\mathrm{rad}(I)$ is an ideal of A, which is Noetherian, $\mathrm{rad}(I)$ must be finitely generated, say by $x_1, x_2, \ldots, x_m$. Moreover since they are in the radical, we have $x_1^{a_1}, x_2^{a_2}, \ldots, x_m^{a_m} \in I$ for some powers a_i. Letting $n = a_1 + a_2 + \ldots + a_m$, we have that $\mathrm{rad}(I)$ is generated by $x_i^{r_i}$ with $r_1 + r_2 + \ldots + r_m = n$, and $x_i^{r_i} \in I$, so indeed $\mathrm{rad}(I)^n \subset I$. □

Corollary 21.1.15. *Let A be Noetherian. Then* $\mathrm{nilrad}(A)$ *is nilpotent.*

Proof. The proof is straight forward: $\mathrm{nilrad}(A) = \mathrm{rad}(0)$. □

Corollary 21.1.16. *Let A be Noetherian and $\mathfrak{m} \subset A$ be a maximal ideal. Let $Q \subset A$ be any ideal. Then the following are equivalent:*

(*i*) *Q is $\mathfrak{m}$-primary.*

(*ii*) $\mathrm{rad}(Q) = \mathfrak{m}$.

(*iii*) $\mathfrak{m}^n \subset Q \subset \mathfrak{m}$ *for some $n > 0$.*

Proof. We have proved in the past that (*i*) and (*ii*) are equivalent. That (*ii*) implies (*iii*) is the previous proposition, and if we assume (*iii*) then (*ii*) follows by taking radicals. □

Lecture 22 Artinian Rings

22.1 Length of Modules

The goal of this and the next lecture is to prove that a ring is Artinian if and only if it is a Noetherian ring of dimension 0.

To accomplish this we first, of course, need to explain what the dimension means, and to that end we need to establish a fair amount of results on Artinian rings:

Proposition 22.1.1. *Let A be an Artinian ring. Then every prime ideal of A is maximal.*

Proof. Let $P \subset A$ be a prime ideal. Then A/P is an Artinian integral domain—the former because quotient maintains Artinian, and the latter because P is prime. For $x \neq 0$ in A/P, we have the descending chain

$$(x) \supset (x^2) \supset (x^3) \supset \ldots$$

which must therefore have a minimal element, i.e. $(x^n) = (x^{n+1}) = \ldots$ for some n. Thus $x^n = yx^{n+1}$, and we are in an integral domain, meaning that we have cancellation laws, so $1 = yx$, making x a unit, thus finally A/P is a field and P is a maximal ideal. □

An immediate corollary of this is

Corollary 22.1.2. *Let A be Artinian. Then* $\mathrm{nilrad}(A) = J(A)$.

Date: November 7, 2017.

Proof. This follows directly since the former is the intersection of all prime ideals, and the latter is the intersection of all maximal ideals, but these are the same in an Artinian ring. □

Proposition 22.1.3. *Let A be Artinian. Then A has only finitely many maximal ideals.*

Proof. Let Σ be the set of all finite intersections

$$\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \cap \ldots \cap \mathfrak{m}_r$$

where $\mathfrak{m}_i$ are maximal ideals. Then since this is nonempty, Σ has a minimal element since A is Artinian, say

$$M_1 \cap M_2 \cap M_3 \cap \ldots \cap M_n.$$

We claim that $M_1, M_2, \ldots, M_n$ are all the maximal ideals in A.

To prove this, take any maximal ideal $\mathfrak{m}$ and consider

$$\mathfrak{m} \cap M_1 \cap M_2 \cap M_3 \cap \ldots \cap M_n \subset M_1 \cap M_2 \cap M_3 \cap \ldots \cap M_n,$$

which by minimality of the latter means that

$$\mathfrak{m} \cap M_1 \cap M_2 \cap M_3 \cap \ldots \cap M_n = M_1 \cap M_2 \cap M_3 \cap \ldots \cap M_n.$$

Now since all ideals here are maximal, they are in particular prime, so

$$\mathfrak{m} \supset M_1 \cap M_2 \cap M_3 \cap \ldots \cap M_n$$

and thus $\mathfrak{m} \supset M_i$ for some i, but since M_i is maximal we must then have $\mathfrak{m} = M_i$.

Thus there are only finitely many maximal ideals. □

Example 22.1.4. We have discussed this before in view of a descending chain, but we now have two new ways of demonstrating that $\mathbb{Z}$ is not Artinian: first, (0) is a prime ideal that is not maximal. Secondly, (p) is a prime ideal for all prime numbers p, and there are infinitely many of them. ▲

Proposition 22.1.5. *Let A be Artinian. Then* $\operatorname{nilrad}(A)$ *is nilpotent.*

Proof. By the descending chain condition we have

$$\operatorname{nilrad}(A) \supset \operatorname{nilrad}(A)^2 \supset \ldots$$

being stationary, meaning that

$$I = \operatorname{nilrad}(A)^n = \operatorname{nilrad}(A)^{n+1} = \ldots$$

for some n.

Now if $I = (0)$ we are done, since we have then demonstrated that $\operatorname{nilrad}(A)$ to some power is 0, i.e. it is nilpotent.

Assume, therefore, that $I \neq (0)$, and consider

$$\Sigma = \{\, J \subset A \text{ ideal} \mid IJ \neq (0) \,\}.$$

Now at the very least $I \in \Sigma$ since $I^2 = I \neq (0)$, so Σ is nonempty, so it has a minimal element, say J. Then there exists $x \in J$ such that $xI \neq 0$, whereby $(x)I \neq (0)$. But $(x) \subset J$, meaning that $(x) = J$ by the minimality of J, and so $(xI)I = xI^2 = xI \neq 0$, ergo

$$xI \subset (x) = xA = J.$$

Therefore $x = xy$ for $y \in I = \text{nilrad}(A)^n$, meaning that y is nilpotent, say $y^m = 0$. Now consider

$$x = xy = (xy)y = xy^2 = \ldots = xy^m = 0,$$

so $x = 0$, which is a contradiction since we assumed $xI \neq 0$, and we are done. □

Definition 22.1.6 (Chain, length, and composition series)**.** (*i*) A ***chain*** of submodules of a module M is a sequence

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots \supsetneq M_n = 0.$$

The ***chain!length*** of this chain is n.

(*ii*) A ***composition series*** of M is a maximal chain, i.e. M_{i-1}/M_i is ***simple***, i.e. has no submodules except 0 and itself.

Example 22.1.7. The prototypical example to keep in mind is a finite dimensional vector space V, which thus have a basis, say $v_1, v_2, \ldots, v_n$. Then

$$V = V_0 \supset V_1 \supset V_2 \supset \ldots \supset V_{n-1} \supset V_n = 0$$

where V_i is the subspace generated but the last i basis vectors is a composition series of length n. If we skip some of the intermediate subspaces, we have a chain that is not a composition series. ▲

Proposition 22.1.8. *Suppose M has a composition series of length n. Then every composition series of M has length n.*

Moreover every chain in M can be extended to a composition series.

Proof. Let $\ell(M)$ denote the least length of a composition series (we let $\ell(M) = +\infty$ if M has no composition series).

We will prove the proposition by means of two claims.

First: If $N \subsetneq M$ is a proper submodule, then $\ell(N) < \ell(M) = n$.

To see this, let $\{ M_i \}$ be a composition series of M of minimal length, and consider the submodules $N_i = N \cap M_i$ of N. Then $\{ N_i \}$ is a chain for N. Moreover

$$\frac{N_{i-1}}{N_i} = \frac{N \cap M_{i-1}}{N \cap M_i} = \frac{N \cap M_{i-1}}{N \cap M_i \cap M_{i-1}}$$

since M_{i-1} is contained in M_i. Now this is isomorphic to

$$\frac{(N \cap M_{i-1}) + M_i}{M_i} \subset \frac{M_{i-1}}{M_i},$$

which is simple. Therefore N_{i-1}/N_i is a submodule of a simple module, so it must either be 0 or isomorphic to M_{i-1}/M_i itself. In the former case, $N_{i-1} = N_i$, so we remove one of them from the chain. In the latter case, N_{i-1}/N_i is simple

Thereby we obtain a composition series with $\ell(N) \leq \ell(M)$. Suppose now $\ell(N) = \ell(M)$. Then $N_{i-1}/N_i \cong M_{i-1}/M_i$ for every i. Consider the last term, $N_{n-1}/N_n \cong M_{n-1}/M_n$, with $M_n = 0 = N_n$, implying that $N_{n-1} = M_{n-1}$. Then look at the previous term $N_{n-2}/N_{n-1} \cong M_{n-2}/M_{n-1}$ implying that $N_{n-2} = M_{n-2}$, and so on, finally implying that $N = M$, which is a contradiction since $N \subsetneq M$, so $\ell(N) < \ell(M)$ as claimed.

For the second claim which finishes the proof, we claim that any chain in M has length less than or equal to $\ell(M)$. Hence by minimality of $\ell(M)$ we have that all composition series of M have the same length.

To prove the claim, let

$$M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_k = 0$$

be a chain of length k. By claim 1, $\ell(M) > \ell(M_1) > \ell(M_2) > \ldots > \ell(M_k) = 0$. Since each step must increase the length by at least 1, we must have $\ell(M) \geq k$. □

Proposition 22.1.9. *A module M has a composition series if and only if M satisfies both the ascending chain condition and the descending chain condition.*

Proof. The forward direction is trivial since $\ell(M) < \infty$, meaning that any chain is finite, and so must stop.

The reverse direction requires a little more work. We construct a composition series of M as follows: Let $M_0 = M$, and consider $\Sigma = \{\, N \subsetneq M \text{ submodules} \,\}$. By the ascending chain condition Σ has a maximal element, say M_1, and similarly M_1 has a maximal submodule M_2, and so on, with

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots$$

which by the descending chain condition is stationary—hence we have a composition series of M. □

Definition 22.1.10 (Module of finite length)**.** A module satisfying both the ascending chain condition and the descending chain condition is called a ***module of finite length***. The length $\ell(M)$ is the length of any composition series of M.

Proposition 22.1.11. *Let k be a field. For a k-vector space, the following conditions are equivalent:*

(*i*) *Having finite dimension.*

(*ii*) *Having finite length.*

(*iii*) *Satisfying the ascending chain condition.*

(*iv*) *Satisfying the descending chain condition.*

Corollary 22.1.12. *Let A be a ring. Suppose $M_1 M_2 \ldots M_n = 0$ for some maximal ideals $M_i \subset A$, not necessarily distinct. Then A is Noetherian if and only if A is Artinian.*

Proof. Consider

$$A \supset M_1 \supset M_1M_2 \supset \ldots \supset M_1M_2 \ldots M_n = 0.$$

Then

$$\frac{M_1M_2 \ldots M_{i-1}}{M_1M_2 \ldots M_n}$$

is an A/M_i module, so a vector space, since M_i contains the annihilator of the module. Hence the ascending chain condition and the descending chain condition are equivalent in this quotient, as an A-module. Next consider the exact sequence

$$0 \longrightarrow M_1M_2 \ldots M_{n-1} \longrightarrow M_1M_2 \ldots M_{n-2} \longrightarrow \tfrac{M_1M_2 \ldots M_{n-2}}{M_1M_2 \ldots M_{n-1}} \longrightarrow 0.$$

Now we can quotient the left-side of this by $M_1M_2 \ldots M_n = 0$, since that changes nothing, but in doing so we see that we have another vector space, so the ascending and descending chain conditions are equivalent on both sides of $M_1M_2 \ldots M_{n-2}$, and so they are equivalent in it as well.

Repeat this with smaller indices, and inductively we get that the ascending and descending chain conditions are equivalent in A itself. □

Lecture 23 Structure of Artinian Rings

23.1 Dimension of Ring

Recall that our goal is to prove that a ring A is Artinian if and only if it is Noetherian and of dimension 0.

We are now ready to define what we mean by the dimension of a ring.

Definition 23.1.1 (Dimension of a ring)**.** Let A be a ring. A ***chain of prime ideals*** of a ring A is a sequence

$$P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n$$

where P_i are prime ideals of A. The length of this chain is n—note that there are $n+1$ prime ideals; we count one less.

The ***dimension*** of A is is the maximal length of all chains of prime ideals in A.

Example 23.1.2. Let k be a field. Then $\dim k = 0$ since there are only two ideals, of which 0 is prime.

We have $\dim \mathbb{Z} = 1$, since the longest chain of prime ideals we can make is $(0) \subset (p)$ for p a prime.

We have $\dim k[x_1, x_2, \ldots, x_n] = n$, since

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, x_2, \ldots, x_n)$$

is the longest chain of primes we can muster.

On the other hand $\dim \mathbb{Z}[x_1, x_2, \ldots, x_n] = n+1$, because we can do almost as above, but also include $I = (p)$;

$$(0) \subset I \subset I[x_1] \subset I[x_1, x_2] \subset \ldots \subset I[x_1, x_2, \ldots, x_n].$$ ▲

Date: November 9, 2017.

Theorem 23.1.3. *The ring A is Artinian if and only if A is Noetherian and* $\dim A = 0$.

Proof. For the forward direction we assume that A is Artinian. Therefore every prime ideal in A is maximal, so $\dim A = 0$ since we can't have any nontrivial chain of prime ideals. Let $M_1, M_2, \ldots, M_n$ be all distinct maximal ideals in A. Then

$$\prod_{i=1}^{n} M_i^k \subset \Big(\bigcap_{i=1}^{n} M_i\Big)^k = J(A)^k = (\text{nilrad}\, A)^k = 0$$

for some k, since the nilradical of an Artinian ring is nilpotent. Hence we have a product of maximal ideals that equals the zero ideal, which means that the ascending chain condition and the descending chain condition are equivalent, which means that A is Noetherian.

For the reverse direction, we make the following claim: since A is Noetherian, it has only finitely many minimal prime ideals.

To prove this, note that (0) has a primary decomposition—every ideal is decomposable in a Noetherian ring. Say $0 = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ is a minimal primary decomposition, with $\text{rad}(Q_i) = P_i$ all distinct by the first uniqueness theorem. Taking radicals we therefore have $\text{rad}(0) = P_1 \cap P_2 \cap \ldots \cap P_n$. Now let P be a minimal prime ideal of A, meaning that $0 \subset P$ implies $\text{rad}(0) \subset P$, further implying

$$P_1 \cap P_2 \cap \ldots \cap P_n \subset P.$$

Hence $P_i \subset P$ for some i, and so by minimality of P we have $P_i = P$. That is to say, all minimal prime ideals of A appear in the primary decomposition of 0.

Now let $P_1, P_2, \ldots, P_n$ be all of the minimal prime ideals in A. Since $\dim A = 0$, we must have that all of these primes are also maximal, since we couldn't form a chain of them any longer than just the one prime. Therefore

$$\text{nilrad}(A) = \cap_{i=1}^{n} P_i,$$

where it suffices to consider only the minimal primes since others wouldn't contribute to the intersection, since they contain the above. Thus

$$\prod_{i=1}^{n} P_i^k \subset \Big(\bigcap_{i=1}^{n} P_i\Big)^k = (\text{nilrad}\, A)^k = 0$$

for some k, since A is Noetherian, meaning that the nilradical is nilpotent. (Note for the record that strictly speaking the inclusion above is an equality since the prime powers are pairwise coprime, but we don't require equality for this argument.)

Hence some product of maximal ideals is 0, making the ascending and descending chain conditions equivalent, and we are finished. □

23.2 Structure of Artinian Rings

Let A be an Artinian local ring with maximal ideal M. Then $\text{nilrad}(A) = J(A) = M$. We know that in a local ring

$$A = A^\times \sqcup M.$$

Thus in the case of an Artinian local ring, everything in the maximal ideal M is nilpotent, i.e. every non-unit is nilpotent. One might then ask oneself what the relation is between M and dimensionality of 0.

Proposition 23.2.1. *Let A be a Noetherian local ring with maximal ideal M. Then exactly one of the following statements is true:*

(*i*) *$M^n \neq M^{n+1}$ for all $n = 1, 2, \ldots$, in which case A is not Artinian (we have an infinite descending chain).*

(*ii*) *$M^n = 0$ for some n, in which case A is Artinian.*

Proof. Suppose $M^n = M^{n+1}$ for some n—if not we clearly have (i). Then since $J(A) = M$ we have

$$M^n = M^{n+1} = J(A)M^n,$$

which by Nakayama's lemma means that $M^n = 0$.

Hence also a finite product of maximal ideals is 0, so A is Artinian. Another way to see this is to consider any prime ideal P of A. Then $M^n = 0 \subset P \subset M$, which if we take radicals yields $\operatorname{rad}(M^n) \subset P \subset \operatorname{rad}(M)$ which is the same as $M \subset P \subset M$, so $P = M$ which makes $\dim A = 0$, and again A is Artinian. □

The reason we want to understand Artinian local rings is this:

Theorem 23.2.2 (Structure theorem for Artinian rings)**.** *An Artinian ring A is isomorphic to a finite direct product of Artinian local rings. In other words,*

$$A \cong \prod_{i=1}^{n} A_i,$$

where A_i are Artinian local rings.

Proof. Let $M_1, M_2, \ldots, M_n$ be the distinct maximal ideals of A. Then

$$\prod_{i=1}^{n} M_i^k = 0$$

for some k, and M_i^k are pairwise coprime. Consider the map

$$\varphi\colon A \to \prod_{i=1}^{n} A/M_i^k.$$

This is clearly surjective, so

$$\ker\varphi = \bigcap_{i=1}^{n} M_i^k = \prod_{i=1}^{n} M_i^k = 0$$

by coprimality. But then φ is also injective, having a trivial kernel, so φ is an isomorphism.

If we can show that $A_i \coloneqq A/M_i^k$ is an Artinian local ring, we are done.

Certainly it is Artinian, since quotient preserves the property of being Artinian (and Noetherian, for that matter). Let $\psi\colon A \to A/M_i^k$. There is a one-to-one correspondence between ideals $I \supset M_i^k$ in A and ideals in A/M_i^k.

Thus if $\bar{M}$ is a maximal ideal in A/M_i^k, then M is a maximal ideal in A such that $M \supset M_i^k$. Now since M and M_i are prime ideals, we have $M_i \subset M$, and therefore $M_i = M$ since both are maximal.

Therefore the only maximal ideal comes from M_i/M_i^k, so A/M_i^k has a unique maximal ideal M_i/M_i^k, making it local. □

Example 23.2.3. The trivial example of a local Artinian ring is $\mathbb{Z}/p^n\mathbb{Z}$, with maximal ideal $p\mathbb{Z}/p^n\mathbb{Z}$. ▲

Consider the following situation. Let A be a local ring with maximal ideal M and residue field $k = A/M$. Consider the A-module M/M^2. Since $M(M/M^2) = 0$, M contains its annihilator, meaning that we can view it as an A/M-module.

But A/M is a field, so then M/M^2 is a vector space over k.

Now if M is a finitely generated A-module, then $\dim_k(M/M^2) < \infty$, and in fact $\{ \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_k \}$ spans M/M^2 if and only if $\{ x_1, x_2, \ldots, x_k \}$ generate M.

Let us now relate these considerations with the idea of local Artinian rings:

Theorem 23.2.4. *Let A be an Artinian local ring with maximal ideal M. Then the following are equivalent:*

(*i*) *Every ideal in A is principal.*

(*ii*) *The maximal ideal M is principal.*

(*iii*) $\dim_k(M/M^2) \leq 1$.

Proof. That (*i*) implies (*ii*) is trivial, since the maximal ideal is an ideal. Likewise (*ii*) implies (*iii*), since M is generated by a single element, and so certainly the dimension of M/M^2 is at most 1.

The only nontrivial part is (*iii*) implying (*i*), thus. First let $\dim_k(M/M^2) = 0$. Then $M = M^2 = J(A)M$, which by Nakayama's lemma means that $M = 0$. Hence the only maximal ideal of A is trivial, making A a field. In a field (0) and $(1) = A$ are the only ideals, which are both clearly principal.

If $\dim_k(M/M^2) = 1$ instead, then $M = (x)$. For any ideal $I \subset A$ with $I \neq (0)$ we have $0 = M^k \subset I \subset M$ for some k. Let $r \in \mathbb{N}$ such that $I \subset M^r = (x^r)$ but $I \not\subset M^{r+1}$.

Then there exists some $y \in I$ with $y \notin M^{r+1}$, meaning that $y = ax^r$ with $a \in A$ and $a \notin M$. Therefore since $A = A^\times \sqcup M$, a must be a unit. Thus $x^r = a^{-1}y \in I$, so $I = (x^r) = M^r$. □

So not only are all ideals principal in Artinian local rings, but in fact every ideal is a power of the maximal ideal.

23.3 Discrete Valuation Rings and Dedekind Domains

When classifying rings, in some sense fields are the easiest case—everything works well, and we understand them quite well.

The next easiest situation is Artinian rings, which we know is the same as Noetherian rings of dimension 0. In here we have shown that every prime ideal is maximal.

The next simplest case is a Noetherian *domain* with dimension 1. In other words we have $(0) = P_0 \subset P_1$ as the prototypical chain of prime ideals, and in here therefore every *nonzero* prime ideal is maximal.

In such a ring we have the remarkable property that we can factor every ideal uniquely.

Proposition 23.3.1. *Let A be a Noetherian domain of dimension 1. Then for any ideal $I \neq 0$ in A,*

$$I = \prod_{i-1}^{n} Q_i$$

where Q_i are primary ideals and $\operatorname{rad}(Q_i) = P_i$ are all distinct. Moreover such an expression is unique.

Proof. The ring A being Noetherian implies that any ideal I has a primary decomposition, say

$$I = \bigcap_{i=1}^{n} Q_i$$

is a minimal primary decomposition with $\operatorname{rad}(Q_i) = P_i$. Since $\dim A = 1$, P_i are maximal, and so P_i are distinct and pairwise coprime. This in turn make Q_i pairwise coprime, and so

$$I = \bigcap_{i=1}^{n} Q_i = \prod_{i=1}^{n} Q_i.$$

Now for the uniqueness: since P_i are maximal ideals, all P_i in $\{ P_1, P_2, \ldots, P_n \}$ are minimal (since one couldn't be contained in the other due to maximality). This means that all P_i are isolated primes, and so all Q_i are uniquely determined by I according to the second uniqueness theorem of primary decompositions. □

Example 23.3.2. In $\mathbb{Z}$ we have $Q_i = P_i^k$. This is not true in general.

However if we assume $Q = P^k$, then $A \to A_P$ then every ideal in in the latter is a power of $PA_P = M$, and by the one-to-one correspondence $I \subset P$ corresponding to I_P must be $I = P^k$. ▲

Lecture 24 Discrete Valuation Rings

24.1 Connections between Discrete Valuation Rings and Noetherian Rings

We previously discussed Noetherian domains of dimension 1. We established that in such a domain A we have that every nonzero prime ideal is maximal, and given $I \neq 0$ an ideal in A we have

$$I = \prod_{i} Q_i$$

where Q_i are primary ideals, and this factorisation is unique. Moreover calling $P_i = \operatorname{rad}(Q_i)$, in general we do *not* have $Q_i = P_i^k$, unlike in the integers or algebraic extensions of them.

However if we assume that $Q_i = P_i^k$, then the localisation A_P of A has only ideals of the form M_k, where $M = PA_P$. We want to classify this kind of local ring:

Date: November 28, 2017.

Definition 24.1.1 (Discrete valuation)**.** Let k be a field. A ***discrete valuation*** on k is a surjective map $v\colon k^* \to \mathbb{Z}$ such that

(*i*) $v(xy) = v(x) + v(y)$, i.e. v is a group homomorphism,

(*ii*) $v(x+y) \geq \min\{\, v(x), v(y) \,\}$.

Note that this doesn't give us a valuation of 0—the convention is to let $v(0) = +\infty$.

Example 24.1.2. Let $k = \mathbb{Q}$, and let p be a prime. For $x \in \mathbb{Q}$, write $x = p^a \cdot y$, where $a \in \mathbb{Z}$ and $y \in Q$, with both numerator and denominator coprime to p. For example, if we let $p = 2$, we have $x = 3/4 = 2^{-2}\cdot 3$, and, say, $x = 5/6 = 2^{-1}\cdot 5/3$. Then we define the valuation $v_p(x) = a$.

Hence

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, \gcd(a,b) = 1,\ p \nmid b \right\} = \{\, x \in \mathbb{Q} \mid v_p(x) \geq 0 \,\}.$$

In this localisation, the unique maximal ideal is

$$M = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \,\middle|\, p \mid a \right\} = \{\, x \in \mathbb{Q} \mid v_p(x) \geq 1 \,\}. \qquad \blacktriangle$$

This is true in general:

Proposition 24.1.3. *Let v be a discrete valuation on the field k. Then $A = \{\, a \in k \mid v(a) \geq 0 \,\}$ is a valuation ring with the unique maximal ideal $M = \{\, a \in k \mid v(a) \geq 1 \,\}$.*

Proof. The two properties of v, along with the convention $v(0) = +\infty \geq 0$, guarantee that A is a ring. To see that it's a valuation ring, note that v is a group homomorphism, so $v(a^{-1}) = -v(a)$, so if $v(a) \geq 0$ we're happy, and if not $v(a^{-1}) > 0$ instead, so either way each nonzero element or its inverse is in A.

Next, if $u \in A$ is a unit, i.e. $u^{-1} \in A$, then $v(u) \geq 0$ and $v(u^{-1}) \geq 0$, meaning that $v(u) = 0$. Indeed the converse is true: if $v(u) = 0$, then u is a unit—this too follows from $v(a^{-1}) = -v(a)$ as discussed above.

Hence M is the set of all non-units in A, so it's the unique maximal ideal. □

Definition 24.1.4 (Discrete valuation ring)**.** An integral domain A is a ***discrete valuation ring*** if there is a discrete valuation v of its field of fractions k such taht A is the valuation ring of v. In other words, $A = \{\, x \in k \mid v(x) \geq 0 \,\}$.

An element $\pi \in A$ with $v(\pi) = 1$ is called a ***uniformiser*** or ***prime element***.

Proposition 24.1.5. *Let A be a discrete valuation ring and let π be a uniformiser. Then the maximal ideal is $M = (\pi)$, meaning in particular that M is principal. Conversely, if $M = (\pi')$, then π' is a uniformiser.*

Proof. Since M is the unique maximal ideal we clearly have $(\pi) \subset M$. Now for any $x \in M$ we have $v(x) \geq 1$, meaning that $v(x\pi^{-1}) = v(x) - v(\pi) \geq 1 - 1 = 0$, so $x\pi^{-1} = a \in A$. Hence $x = \pi \cdot a \in (\pi)$, so $M \subset (\pi)$ as well, and thus $M = (\pi)$.

Now suppose $M = (\pi')$. We wish to show that $v(\pi') = 1$. We know that $M = (\pi)$, so $v(\pi) = 1$, and since the ideals (π) and (π') are equal by assumption,

we have $\pi = a \cdot \pi'$ for some $a \in A$. Hence $v(\pi) = 1 = v(a) + v(\pi')$, and since $v(a) \geq 0$ and $v(\pi') \geq 0$, we have only two options: either $v(a) = 0$ and $v(\pi') = 1$, or $v(a) = 1$ and $v(\pi') = 0$.

But in the latter case, π' is a unit since it has valuation 0, but this is a contradiction since $\pi' \in M$ but M is the set of all non-units and nothing else. □

Proposition 24.1.6. *Let A be a discrete valuation ring and k its field of fractions. Let π be a uniformiser of A. Then every nonzero element $x \in k$ can be expressed uniquely as $x = u \cdot \pi^n$, with u a unit and $n \in \mathbb{Z}$. Hence $k = S^{-1}A$ where $S^{-1} = \{1, \pi, \pi^2, \dots\}$.*

Proof. Let $n = v(x)$. Then $v(x\pi^{-n}) = v(x) - nv(\pi) = 0$ since $v(\pi) = 1$ by definition. Therefore $x\pi^{-n} = u \in A$ is a unit, and multiplying by π^n we have $x = u \cdot \pi^n$.

For uniqueness, if $x = u_1\pi^m = u_2\pi^n$, then $v(x) = m = n$, and moreover $u_1\pi^n = u_2\pi^n$ implues $u_1 = u_2$ since we are in an integral domain, which means we have cancellation laws. □

Proposition 24.1.7. *Let A be a discrete valuation ring with maximal ideal M. Then every ideal $I \neq 0$ in A is of the form $I = M^n$, with $n \geq 0$ being unique. We write $v(I) = n$.*

Proof. Take $a \in I$ such that $n = v(a) \leq v(x)$ for all $x \in I$, i.e. the smallest possible element in the ideal I, as per the valuation. Then $a = u \cdot \pi^n$, taking π to be a uniformiser of A, and u being a unit in A. Hence $\pi^n = u^{-1}a \in I$, meaning that $(\pi^n) = M^n \subset I$.

On the other hand, for $x \in I$ we have $v(x) = k \geq n$ and so $x = u_1\pi^k$ with u_1 a unit in A. Now write $x = u_1\pi^{k-n}\pi^n \subset (\pi^n) = M^n$, so $I = M^n$.

To establish uniqueness, suppose $I = M^n = M^{n+1}$. In that case, since we are in a local ring, we have $J(A) = M$, and $M^n = J(A)M^n$, so by Nakayama's lemma $M^n = 0$, which is a contradiction since we assumed $I \neq 0$. □

Remark 24.1.8. Note that if A is a discrete valuation ring we therefore have

$$A \supset M \supset M^2 \supset M^3 \supset \dots$$

which is a complete list of all the ideals. Thus in particular A is Noetherian, since any ascending sequence of ideals must end in what we have above.

Lecture 25 Dedekind Domains

25.1 Toward the Definition of Dedekind Domains

We want to classify rings in which every ideal is the power of maximal ideals.

Proposition 25.1.1. *Let A be a Noetherian local ring of dimension 1 with maximal ideal M and residue field $k = A/M$. The following are equivalent:*

(*i*) *A is a discrete valuation ring.*

Date: November 30, 2017.

(*ii*) *A is integrally closed.*

(*iii*) *M is principal.*

(*iv*) $\dim_k(M/M^2) = 1$.

(*v*) *Every nonzero ideal is of the form M^k, $k \geq 0$.*

(*vi*) *There exists $\pi \in A$ such that every nonzero ideal is of the form (π^k), $k \geq 0$.*

Proof. Recall two properties of A. First, if $I \neq 0$ is an ideal in A, then I is M-primary since M is the only nonzero prime ideal, and therefore the radical of I, which is prime, must be M. Moreover $I \supset M^n$ for some n.

Second, $M^n \neq M^{n+1}$ for all $n \geq 0$, for otherwise by Nakayama's lemma we'd have $M^n = J(A)M^n$, implying $M^n = 0$, and in turn $M = 0$.

We start with (*i*) implying (*ii*): Since A is a discrete valuation ring, A is a valuation ring, and so A is integrally closed.

Next (*ii*) implies (*iii*): Let $a \neq 0$, $a \in M$. If $M = (a)$, we're done. If $M \neq (a)$, then by the first property above we have $M^n \subset (a)$ for some n, and $M^{n-1} \not\subset (a)$, by choosing the smallest n. Now take $b \in M^{n-1}$ and $b \notin (a)$, and consider $\pi = a/b \in K$, the field of fractions of A. Then $\pi^{-1} \in A$, since otherwise $\pi^{-1} = b/a \in A$, implying that $b \in (a)$, a contradiction.

Hence since A is integrally closed, π^{-1} is not integral over A, meaning that $\pi^{-1}M \not\subset M$. Otherwise M is a faithful $A[\pi^{-1}]$-module, and M is finitely generated since A is Noetherian, and so π^{-1} is integral over A, which is a contradiction.

But $\pi^{-1}M = b/aM \subset 1/aM^n \subset A$, meaning that $\pi^{-1}M = A$ since M is the unique maximal ideal, and thus $M = \pi A = (\pi)$.

For (*iii*) implying (*iv*), take $M = (\pi)$ and so $\dim_k(M/M^2)$ is either 0 or 1. The former happens only if $M = M^2$, but by the second property this cannot be, and so the dimension is 1.

Now in somewhat of a twist we prove that (*iv*) implies (*iii*). Since by (*iv*), $\dim_k(M/M^2) = 1$, we have a generator $\pi + M^2$ of the k-vector space M/M^2, and therefore $M = (\pi)$.

We have proved (*i*) implying (*v*) before.

To prove (*v*) implying (*iii*), take $\pi \in M/M^2$, which exists by the second property, and so by (*v*) we have $(\pi) = M^k$ for some k, but by choice of $\pi \in M$ we don't have $\pi \in M^2$, so $k = 1$.

Next (*iii*) implies (*vi*). Assume $M = (\pi)$, and let $I \neq 0$ be an ideal in A. Then there exists some n such that $I \subset M^n$ and $I \not\subset M^{n+1}$ by the first property, and so take $x \in I \setminus M^{n+1}$. This means that $x \in M^n$, meaning that $x = u\pi^n$ with $u \notin M$ and $u \in A$, so u is a unit. Hence $\pi^n = u^{-1}x \in I$ since $x \in I$. Therefore $(\pi^n) \subset I \subset M^n = (\pi^n)$, so $I = (\pi^n)$.

Finally (*vi*) implies (*i*): Take $M = (\pi)$ and $(\pi^k) \neq (\pi^{k+1})$. For $a \neq 0$, $a \in A$, we have $(a) = (\pi^k)$. Define $v\colon K^* \to \mathbb{Z}$ by $v(a) = k$ if $a \in A$, and moreover define $v(a/b) = v(a) - v(b)$. Then v is a discrete valuation on K^* and A is the valuation ring of v since $a \in A$ if and only if $v(a) \geq 0$. □

25.2 Dedekind Domain

We now consider the same result as above, except with the condition of locality dropped.

Theorem 25.2.1. *Let A be a Noetherian domain of dimension 1. The following are equivalent:*

(*i*) *A is integrally closed.*

(*ii*) *Every primary ideal is a prime power.*

(*iii*) *A_P is a discrete valuation ring for every prime ideal $P \neq 0$ in A.*

Definition 25.2.2 (Dedekind domain)**.** A ring satisfying these equivalent conditions is called a ***Dedekind domain***.

Proof. First (*i*) is equivalent to (*iii*), since A is integrally closed if and only if A_P is integrally closed for all prime ideals P (since integrally closed is a local property), which in turn is equivalent to A_P being a discrete valuation ring for every P by the previous classification.

Next (*ii*) is equivalent to (*iii*) since every idael in A is a prime power if and only if every primary ideal in A_P is a prime power for all P by the one-to-one correspondence between primary ideals contained in P in A and primary ideals in A_P, which in turn is equivalent to A_P being a discrete valuation ring by the previous classification. □

Corollary 25.2.3. *Let A be a Dedekind domain. Then every nonzero ideal in A has a unique factorisation as a product of prime ideals.*

Proof. In a Noetherian domain of dimension 1 we have

$$I = \prod_i Q_i$$

where Q_i are primary ideals, and this factorisation is unique by dimension 1. Moreover since A is Dedekind, each of these primary ideals is a prime power, so

$$I = \prod_i P_i^{k_i}.$$ □

Example 25.2.4. Any principal ideal domain is Dedekind. ▲

Example 25.2.5. Let A be a Dedekind domain. Then A is a principal ideal domain if and only if A is a unique factorisation domain.

Of particular interest for number theorists, therefore, is this: If K is a finite extension of $\mathbb{Q}$, i.e. a number field, then $\mathcal{O}$ is the integral closure of $\mathbb{Z}$ over K, called the ring of integers of K.

In $\mathbb{Z}$ we have $n = p_1^{a_1} \cdots p_k^{a_k}$ uniquely, but a more useful way to write the same property is

$$(n) = (p_1)^{a_1} \cdots (p_k)^{a_k}$$

because this property generalises to $\mathcal{O}$. ▲

25.3 Completions

Definition 25.3.1 (Topological abelian group)**.** We say that G is a ***topological abelian group*** if G is both a topological space and an abelian group such that $G \times G \to G$ defined by $(a, b) \mapsto a + b$ and $G \to G$ defined by $a \mapsto -a$ are continuous, i.e. the group structure preserves the topological structure.

Definition 25.3.2. A topological space X is called ***complete*** if every Cauchy sequence converges to a point in X.

Note that whilst we don't necessarily have a metric, we do have a group structure compatible with our topology, so by $\{ x_n \}$ being Cauchy we mean that $x_n - x_m$ is in a neighbourhood of 0 for all m and n.

Example 25.3.3. Consider $\mathbb{Q}$ with the usual absolute value $|\cdot|$, inducing the metric $d(x, y) = |x - y|$. Then $(\mathbb{Q}, +)$ is a topological abelian group, but $\mathbb{Q}$ is not complete, since there are Cauchy sequences that converge to irrational numbers. Its completion is well-known, namely $\mathbb{R}$. ▲

A very useful property when trying to establish a topology in this way is this: if G is a topological abelian group, fix $a \in G$ and define $T_a \colon G \to G$ by $T_a(g) = g + a$. Then T_a is a homeomorphism of G onto G, i.e. T_a and its inverse are both continuous. So if U is a neighbourhood of 0 in G, then $a + U$ is a neighbourhood of a in G, and conversely every neighbourhood in G is of this form.

Hence the topology of G is uniquely determined by the neighbourhoods of 0 in G.

Lecture 26 Graded Rings and Filtrations

26.1 Graded Rings and Modules

Definition 26.1.1 (Graded ring)**.** A ***graded ring*** is a ring A such that

(*i*) $A = \bigoplus_{n=0}^{\infty} A_n$, where A_n are subgroups of A and

(*ii*) $A_m A_n \subset A_{m+n}$ for $m, n \geq 0$.

Hence A_0 is a subring of A and A_n is an A_0-module.

Example 26.1.2. Perhaps the simplest example is $A = k[x_1, x_2, \ldots, x_n]$. Let A_n be the set of all homogeneous polynomials of degree n. Then $A = \bigoplus_{n=0}^{\infty} A_n$ and $A_n A_m \subset A_{n+m}$, so A is a graded ring. For instance,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0,$$

where $a_n x^n \in A_n$, $a_{n-1} x^{n-1} \in A_{n-1}$, et cetera. Similarly,

$$g(x_1, x_2) = a_1 x_1 x_2 + a_2 x_1^2 + a_3 x_1 + a_4 x_2,$$

wherein $a_1 x_1 x_2 + a_2 x_1^2 \in A_2$, and $a_3 x_1 + a_4 x_2 \in A_1$. ▲

Date: December 5, 2017.

Definition 26.1.3 (Graded module)**.** Let A be a graded ring. A ***graded A-module*** M is expressible as

$$M = \bigoplus_{n=0}^{\infty} M_n$$

with $A_m M_n \subset M_{n+m}$.

An element $x \in M$ is called ***homogeneous*** if $x \in M_n$ for some n. We call n the ***degree*** of x.

Note that any element $y \in M$ can be written uniquely as $y = \sum_{n \geq 0} x_n$, with $x_n \in M_n$, where $x_n = 0$ for all but finitely many n.

Definition 26.1.4 (Filtration of a ring)**.** Let A be a ring. Then $\{ A_n \}$ is a ***filtration*** of A if

$$A = A_0 \supset A_1 \supset A_2 \supset A_3 \supset \dots$$

are subgroups with $A_m A_n \subset A_{m+n}$.

Definition 26.1.5 (Filtration of a module)**.** Let M be a module over the filtered ring A. Then $\{ M_n \}$ is a ***filtration*** of M if

$$M = M_0 \supset M_1 \supset M_2 \supset M_3 \supset \dots$$

are submodules with $A_m M_n \subset M_{m+n}$.

Example 26.1.6. Let I be an ideal of a ring A, and let M be an A-module. The ***I-adic filtration*** of A and M are given by $A_0 = A = I^0$, $A_n = I^n$ for $n \geq 1$, and $M_0 = M$ with $M_n = I^n M$ for $n \geq 1$. Hence $A_m N_n = I^m I^n M = I^{m+n} M = M_{m+n}$. ▲

Proposition 26.1.7. *Let $A = \bigoplus_{n \geq 0} A_n$ be a graded ring. The following are equivalent:*

(*i*) *A is Noetherian.*

(*ii*) *A_0 is Noetherian and A is finitely generated as an A_0-algebra.*

Proof. First show that (*i*) implies (*ii*). Let $I = \bigoplus_{n \geq 1} A_n$, which is an ideal of A, and $A_0 \cong A/I$. Hence A being Noetherian implies A_0 is Noetherian, since the quotient of a Noetherian ring remains Noetherian. Now I is finitely generated since it is an ideal of a Noetherian ring A, say by $x_1, x_2, \dots, x_k$, which we may take to be homogeneous of degree $m_1, m_2, \dots, m_k$ (if not, take linear combinations to make them). Let $A' = A_0[x_1, x_2, \dots, x_k] \subset A$, an A_0-algebra—think of it as a subring.

We claim that $A' = A$. By construction it suffices to show $A_n \subset A'$ for all n. First, therefore, note that for $n = 0$ we have $A_0 \subset A'$, which is fine. Next assume $A_m \subset A'$ for all $m \leq n - 1$, and consider n. Then if $y \in A_n \subset I$, we have

$$y = a_1 x_1 + a_2 x_2 + \dots + a_k x_k,$$

with $a_i \in A$. Note that y is homogeneous, so since $x_i \in A_{n_i}$, we must have $a_i \in A_{n - n_i}$. Now since the degree of a_i is less than n, we have by the induction hypothesis that

$$a_i = b_{i1} x_1 + b_{i2} x_2 + \dots + b_{ik} x_k$$

with $b_{ij} \in A_0$. Hence y is a polynomial in $x_1, x_2, \ldots, x_n$ with coefficients in A_0, meaning that $y \in A'$, so $A = A'$ as claimed.

Now for (ii) implying (i), note that A is a finitely generated A_0-algebra implies that A is some quotient of $A_0[x_1, x_2, \ldots, x_n]$. Now A_0 is Noetherian, so by Hilbert basis theorem $A_0[x_1, x_2, \ldots, x_n]$ is Noetherian as well, and since A is some quotient of this, A in turn must also be Noetherian. □

Definition 26.1.8 (I-filtration)**.** Let M be a filtered A-module with filtration $\{ M_n \}$. Let $I \subset A$ be an ideal. Then $\{ M_n \}$ is called an ***I-filtration*** if $IM_n \subset M_{n+1}$.

Moreover an I-filtration $\{ M_n \}$ with $IM_n = M_{n+1}$ for $n \geq N$ for some N is called ***I-stable***.

Remark 26.1.9. The I-adic filtration is I-stable.

Proposition 26.1.10. *Let A be a Noetherian ring and let M be a finitely generated A-module. Suppose $\{ M_n \}$ is an I-filtration of M. The following are equivalent:*

- (i) *$\{ M_n \}$ is I-stable.*
- (ii) *Define a graded ring A^* and a graded A^*-module M^* by $A^* = \bigoplus_{n \geq 0} I^n$ and $M^* = \bigoplus_{n \geq 0} M_n$. Then M^* is a finitely generated A^*-module.*

Proof. Let $Q_n = \bigoplus_{i=0}^{n} M_i \subset M^*$. Since M_i are finitely generated A-modules from the hypotheses of the proposition, we have that Q_n are finitely generated A-modules. In general Q_n is *not* an A^*-submodule of M^*. But Q_n does generate

$$Q_n^* = M_0 \oplus M_1 \oplus M_2 \oplus \ldots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \ldots.$$

Having I-stability implies that this stops, so this is a finitely generated A^*-submodule of M^* with the same generators as Q_n over A.

Note moreover that

$$M^* = \bigcup_{n \geq 0} Q_n^*$$

where $Q_0^* \subset Q_1^* \subset Q_2^* \subset \ldots$.

Therefore (ii) is equivalent with M^* being a finitely generated A^*-module; since A is Noetherian, A^* is Noetherian, so M^* is a Noetherian module. This is true if and only if the chain of Q_i^* stops, if and only if $M^* = Q_m^*$ for some m, if and only if $M_{m+k} = I_k M_n$ for all $k \geq 1$. This finally is the same as $\{ M_n \}$ being I-stable, i.e. (i). □

The example to keep in mind with discussing these things is usually the I-adic filtration.

Proposition 26.1.11 (Artin-Rees lemma)**.** *Let A be a Noetherian ring and $I \subset A$ an ideal. Let M be a finitely generated A-module and $\{ M_n \}$ be an I-stable filtration. Let N be a submodule of M. Then $\{ N_n = N \cap M_n \}$ is an I-stable filtration of N.*

Proof. Let $A^* = \bigoplus_{n \geq 0} I^n$ and $M^* = \bigoplus_{n \geq 0} M_n$, as above. Finally let $N^* = \bigoplus_{n \geq 0} N_n$.

The filtration $\{ M_n \}$ being I-stable, by the above proposition, implies that M^* is a finitely generated A^*-module, with A^* being Noetherian. This in turn implies that M^* is a Noetherian A^*-module, so all of its submodules are finitely generated.

Now in particular N^* is a submodule, so it is finitely generated over A^*. The converse direction of the proposition therefore implies that $\{ N_n \}$ is I-stable. □

Corollary 26.1.12. *There exists $m \in \mathbb{N}$ such that*

$$(I^{m+k}M) \cap N = I^k((I^m M) \cap N)$$

for all $k \geq 0$.

Proof. Take the filtration $M_m = I^m M$. Then

$$(I^{m+k}M) = M_{m+k} \cap N = N_{m+k} = I^k N_m = I^k((I^m M) \cap N). \qquad \square$$

Remark 26.1.13. There is a topological interpretation of this. Let M be an A-module, and $I \subset A$ an ideal. Consider the I-adic filtration $\{ I^n M \}$, where

$$M \supset IM \supset I^2 M \supset I^3 M \supset \ldots \supset (0),$$

so we use these to define open neighbourhoods of 0—we let them be a basis for the neighbourhoods of 0. By translation we moreover let $\{ x + I^n M \}$ be a basis for the neighbourhoods of x.

These induce a topology on M where module operations are continuous. The topology is called the ***I-adic topology*** on M.

The corollary says that the I-adic topology on N coindices with the topology on N induced by the I-adic topology on M.

This can be generalised beyond just the I-adig filtration:

Remark 26.1.14. Let M be a filtered A-module with filtration $\{ M_n \}$. The filtration determines a topology on M with $\{ M_n \}$ forming a basis for the neighbourhoods of 0.

26.2 Inverse Systems

Definition 26.2.1 (Inverse system)**.** Suppose we have $\{ M_n \}_{n \geq 0}$, a collection of A-modules, with A-module homomorphisms $\vartheta_n \colon M_n \to M_{n-1}$ for $n \geq 1$. The collection of modules and homomorphisms is called an ***inverse system***.

A sequence $(x_n) \in \prod_n M_n$ is called ***coherent*** if $\vartheta_{n+1}(x_{n+1}) = x_n$ for all $n \geq 0$. In other words, we have the diagrammatic picture

$$M_0 \xleftarrow{\vartheta_1} M_1 \xleftarrow{\vartheta_2} M_2 \xleftarrow{\vartheta_3} M_3 \xleftarrow{\vartheta_4} M_4 \xleftarrow{\vartheta_5} \cdots$$

$$x_0 \longmapsto x_1 \longmapsto x_2 \longmapsto x_3 \longmapsto x_4 \longmapsto \cdots$$

The collection M of all coeherent sequences is called the ***inverse limit*** of the inverse system, denoted

$$M = \varprojlim M_n.$$

The inverse limit M is an A-module with coordinatewise addition, $(x_n)+(y_n) = (x_n+y_n)$, which is also coherent since ϑ_n is a homomorphism, and likewise scalar multiplication is coordinatewise, $a(x_n) = (ax_n)$, which again is coherent.

Lecture 27 Closure

27.1 Closure and Completion

Proposition 27.1.1. *Let M be a filtered A-module with filtration $\{ M_n \}$. If N is a submodule of M, the* **closure** *of N (in M) is*

$$\overline{N} = \bigcap_{n=0}^{\infty} N + M_n.$$

Proof. Let $x \in M$. Then $x \notin \overline{N}$ if and only of $(x + M_n) \cap N \neq \varnothing$ for some n, since $\overline{N}$ is closed, and so its complement is open.

We claim that this is equivalent with $x \notin N + M_n$ for some N. This in turn is equivalent with $\overline{N} = \bigcap_{n=0}^{\infty}(N + M_n)$, so it's all down to the claim.

For the forward direction of the claim, let us assume $(x + M_n) \cap N = \varnothing$. If $x \in N + M_n$, then $x = y + z$ with $y \in N$ and $z \in M_n$, hence $x + (-z) = y$ is in $x + M_n$ and also in N, so $x + (-z) \in N \cap (x + M_n)$, but this is empty, so this is a contradiction. Hence $x \notin N + M_n$.

For the reverse direction, assume $x \notin N + M_n$. If $y \in (x + M_n) \cap N \neq \varnothing$, then $y = x + z$, with $z \in M_n$, meaning that $x = y - z \in N + M_n$, another contradiction. □

Corollary 27.1.2. *The topology induced from this filtration is* **Hausdorff** *if and only if*

$$\bigcap_{n=0}^{\infty} M_n = \{ 0 \}.$$

Recall that a topology is called Hausdorff if for any two points x and y, we can find a neighbourhood U of x and a neighbourhood V of y such that $U \cap V = \varnothing$.

Proof. A topological space is Hausdorff if and only if every singleton is closed, but our topology is induced by the neighbourhoods of 0, so this is true if and only if $\{ 0 \}$ is closed, which is true if and only if

$$\{ 0 \} = \overline{\{ 0 \}} = \bigcap_{n=0}^{\infty} M_n.$$ □

Definition 27.1.3 (Completion)**.** Let $\{ M_n \}$ be a filtration of the A-module M, meaning that we have an induced topology on M.

A sequence $\{ x_n \}$ in M is called ***Cauchy*** if for every $k \in \mathbb{N}$ there exists some $N \in \mathbb{N}$ such that $x_n - x_m \in M_k$ for every $n, m \geq N$.

Moreover if $\{ x_n \}$ and $\{ y_n \}$ are two Cauchy sequences in M, we call them ***equivalent*** if for every $k \in \mathbb{N}$ there exists some $N \in \mathbb{N}$ such that $x_n - y_n \in M_k$ for every $n \geq N$.

Finally the ***completion*** of M is the equivalence classes of Cauchy sequences in M, denoted by $\widehat{M}$.

Date: December 7, 2017.

Note that if $\{ x_m \}$ is a Cauchy sequence in M, then $\{ x_m \}$ in M/M_n is ultimately constant, say ξ_n, since $x_m - x_k \in M_n$ is equivalent to $x_m + M_n = x_k + M_n$. Now define $\vartheta_{n+1} \colon M/M_{n+1} \to M/M_n$ by $\vartheta_{n+1}(\xi_{n+1}) = \xi_n$. We therefore have

$$M/M_0 \xleftarrow{\vartheta_1} M/M_1 \xleftarrow{\vartheta_2} M/M_2 \xleftarrow{\vartheta_3} M/M_3 \xleftarrow{\vartheta_4} M/M_4 \xleftarrow{\vartheta_5} \cdots$$

$$\xi_0 \longleftarrow\!\shortmid\ \xi_1 \longleftarrow\!\shortmid\ \xi_2 \longleftarrow\!\shortmid\ \xi_3 \longleftarrow\!\shortmid\ \xi_4 \longleftarrow\!\shortmid\ \cdots$$

Then $\{ \xi_n \}$ is a coherent sequence in the inverse system $(M/M_n, \vartheta_n)$.

Remark 27.1.4. If $\{ x_n \}$ and $\{ y_n \}$ are equivalent Cauchy sequences in M, then they define the same coherent sequence $\{ \xi_n \}$.

On the other hand, given any coherent sequence $\{ \xi_n \}$ in the inverse system $(M/M_n, \vartheta_n)$, take x_n to be any element in $\xi_n + M_n$. Then $\{ x_n \}$ is Cauchy in M.

Hence

$$\widehat{M} = \varprojlim \frac{M}{M_n}.$$

Example 27.1.5. Let $A = M = \mathbb{Z}$, and $I = (p)$, with p being prime. Let $M_n = I^n = p^n\mathbb{Z}$, and $\vartheta_{n+1} \colon M/M_{n+1} \to M/M_n$ defined by $\vartheta_{n+1}(a + I^{n+1}) = a + I^n$.

Then the inverse limit

$$\varprojlim \frac{M}{M_n} = \varprojlim \frac{\mathbb{Z}}{p^n\mathbb{Z}} = \widehat{Z_p}$$

is the p-adic integers. ▲

Proposition 27.1.6. *Suppose*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

is an exact sequence of A-modules. Let $\{ M_n \}$ be a filtration of M such that $\{ M_n \}$ induces a filtration $\{ L \cap f^{-1}(M_n) \}$ on L and $\{ g(M_n) \}$ on N. Then

$$0 \longrightarrow \widehat{L} \longrightarrow \widehat{M} \longrightarrow \widehat{N} \longrightarrow 0,$$

where of course the completions are under the respective induced topologies, is exact.

27.2 Consequences of the Krull Intersection Theorem

We close off this course by mentioning, without proof, some consequences of the Krull intersection theorem.

Corollary 27.2.1. *Let A be a Noetherian domain and $I \subset A$ an ideal. Then*

$$\bigcap_{n=0}^{\infty} I^n = \{ 0 \}$$

meaning that the I-adic topology induced by I is Hausdorff.

Corollary 27.2.2. *Let A be a Noetherian ring and $I \subset J(A)$ an idael. Let M be a finitely generated A-module. Then*

$$\bigcap_{n=0}^{\infty} I^n M = \{ 0 \},$$

meaning that the I-adic topology on M is Hausdorff.

Theorem 27.2.3. *Let A be a Noetherian ring and I an ideal. Then the I-adic completion $\widehat{A}$ of A is Noetherian.*

Corollary 27.2.4. *Let A be a Noetherian ring. Then $A[[x_1, x_2, \ldots, x_n]]$ is Noetherian.*

We have proven this directly before, but in the interest of fun we provide a very quick proof as a consequence of the above:

Proof. By Hilbert basis theorem $A[x_1, x_2, \ldots, x_n]$ is Noetherian. Consider $I = (x_1, x_2, \ldots, x_n)$. The I-adic completion of $A[x_1, x_2, \ldots, x_n]$ is $A[[x_1, x_2, \ldots, x_n]]$, and by the above it is Noetherian. □

References

[AM94] M. F. Atiyah, I. G. MacDonald. *Introduction To Commutative Algebra.* Westview Press, 138 pages, 1994.

Index