1. Lecture 1 – What is this course

Commutative algebra is the study of commutative rings, and their associated structures. The goal of today's lecture is to remind ourselves what that means.

We'll never see noncommutative rings in this course, nor rings without multiplicative identities. So we will use the word **ring** for commutative rings with identity. Let's revise what that means.

Definition. A **ring** is a set A equipped with two binary operations. For $a, b \in A$, we have the operations of *addition*, denoted $a + b$, and *multiplication* denoted ab. These must satisfy axioms:

(1) $(A, +)$ is an abelian group, with identity element denoted $0 \in A$.
(2) Multiplication is associative: $(ab)c = a(bc)$.
(3) Multiplication is commutative: $ab = ba$.
(4) Given $a, b, c \in A$, we have
$$(a + b)c = ac + bc.$$
(5) There exists an element $1 \in A$, such that for all $a \in A$, we have
$$1a = a.$$

The algebraic rules we use to manipulate ordinary numbers mostly work arbitrary rings, in particular, for $a, b \in A$, we have

$$(-a)(-b) = ab, (-a)b = -ab \text{ and } 0a = 0$$

Example. The **0 ring** has one element 0, and addition and multiplication is defined in the only way it can be: $0 + 0 = 0 = 00$.

Example. Most things we call numbers form rings: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are rings with the standard addition and multiplication operations.

Example. The set of all functions $f \colon \mathbb{R} \to \mathbb{R}$ forms a ring with the usual operations of addition and multiplication of functions.

More generally, if X is a set and A a ring, the set of functions $f \colon X \to A$ form a ring by defining $(f + g)(x) = f(x) +_A g(x)$ for all $x \in X$.

Example. Given a ring A, the **ring of polynomials** (in one variable) over A is denoted $A[x]$. Its elements are formal polynomials, that is expressions like

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \qquad a_i \in A,$$

and the operations of addition and multiplication in $A[x]$ are defined in a straightforward way (e.g. think of how you add and multiply polynomials with real coefficients, then do the same thing except using the operations on the coefficients in A instead).

Example. More generally, given a ring A and an $n \geq 1$, we can defined $A[x_1, \ldots, x_n]$. This is the ring of polynomials in n variables. Its elements are expressions of the form

$$\sum_{i_1, \ldots, i_n \geq 0} a_{i_1 i_2 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}, \qquad a_{i_1 \ldots i_n} \in A$$

Again the ring operations are defined in a natural way which we won't write down.

We often write $A[x, y]$ instead of $A[x_1, x_2]$ and $A[x, y, z]$ instead of $A[x_1, x_2, x_3]$.

Example. In the ring $A[x, y]$, with chosen elements $a, b, c \in A$, say, we can compute

$$(1 + axy^2)(b + cxy) = 1b + 1cx + axy^2 b + axy^2 cx = b + cx + abxy^2 + acx^2 y^2$$

1.1. **Homomorphisms.**

Definition. Let A and B be rings. A map $\phi\colon A \to B$ is a **homomorphism** if it satisfies

(1) $\phi(1_A) = 1_B$
(2) For all $a, a' \in A$, we have
$$\phi(aa') = \phi(a)\phi(a').$$
(3) For all $a, a' \in A$, we have
$$\phi(a + a') = \phi(a) + \phi(a')$$

If ϕ is moreover bijective, then we say ϕ is an **isomorphism** and write $A \cong B$.

Example. The inclusion maps $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ preserve the identity element and both binary structures, so are homomorphisms.

Example. Let $a \in A$ be an element, then there is a **evaluation homomorphism** $\phi_a\colon A[x] \to A$ defined by (replace x with a everywhere!)
$$\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = a_n a^n + a_{n-1}a^{n-1} + \cdots + a_0$$

1.2. **Ideals.**

Definition. Let A be a ring. A subset $\mathfrak{a} \subset A$ is an **ideal** if it satisfies two conditions:

(1) $\mathfrak{a}$ forms a subgroup of $(R, +)$
(2) For every $x \in A$ and $a \in \mathfrak{a}$, we have $xa \in \mathfrak{a}$.

Example. In a ring A, the subsets A and $\{0\}$ are ideals.

Definition. Let $x \in A$. The **principal ideal** generated by x, denoted $(x) \subset A$, is defined as
$$\{ax \mid a \in A\} \subseteq A$$

Example. In any ring A, we have $\{0\} = (0)$ and $A = (1)$, so these are principal ideals.

Example. The ideals of $\mathbb{Z}$ are all principal, so are given by $(n) \subseteq \mathbb{Z}$ for $n \geq 0$.

1.3. **Quotient rings.**

Definition. If $\mathfrak{a} \subset A$ is an ideal, then we may form the **quotient ring** $A/\mathfrak{a}$, whose elements are the additive cosets of $\mathfrak{a}$ in A, with addition and multiplication defined by
$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$$
and
$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}.$$
The **quotient homomorphism** $\phi\colon A \to A/\mathfrak{a}$ is given by, for $x \in A$,
$$\phi(x) = x + \mathfrak{a}.$$

Example. The ring A/A has one element, A, and so is (isomorphic to) the zero ring.

Example. Let $n \geq 1$, then the ring $\mathbb{Z}/(n)$ is the **ring of integers modulo** n, and has n elements
$$\mathbb{Z}/(n) = \{0 + (n), 1 + (n), \ldots, n - 1 + (n)\}.$$

Example (A purely motivational example)**.** Let $f = \sum a_{ij} x^i y^j \in \mathbb{C}[x, y]$. The vanishing locus of f is the set of $(a, b) \in \mathbb{C}^2$ such that $f(a, b) = 0$, and a set of points defined in this way is what is called an algebraic curve. The ring

$$\mathbb{C}[x, y]/(f)$$

is interpreted as the ring of "algebraic functions" on the curve. In algebraic geometry, we study the geometry of this curve via the algebra of its ring of functions.

Definition. Let $\phi\colon A \to B$ be a homomorphism. The **kernel of** ϕ is given by

$$\ker \phi = \{x \in A \mid \phi(x) = 0\}.$$

Theorem. *Let $\phi\colon A \to B$ be a homomorphism. The kernel of ϕ is an ideal of A.*

Theorem (The fundamental homomorphism theorem)**.**

- *The image of ϕ, denoted $\phi(A) \subset B$, is a subring of B, and we have*

$$A/\ker \phi \cong \phi(A)$$

- *The homomorphism ϕ is injective if and only if* $\ker \phi = \{0\}$.

1.4. **The relation between ideals of a ring and a quotient ring.** Let $\mathfrak{a} \subset A$ be an ideal in a ring, and $\phi\colon A \to A/\mathfrak{a}$ the quotient homomorphism.

Theorem. *There is a bijective correspondence*

$$\{\textit{Ideals of } A/\mathfrak{a}\} \leftrightarrow \{\textit{Ideals of } A \textit{ containing } \mathfrak{a}\},$$

given by

$$\mathfrak{b} \subset A/\mathfrak{a} \mapsto \phi^{-1}(\mathfrak{b})$$

and the other way by

$$\mathfrak{a} \subseteq \mathfrak{b} \subset A \mapsto \phi(\mathfrak{b})$$

Sketch proof. First check ϕ^{-1} is well-defined, i.e. that if $\mathfrak{b} \subseteq A/\mathfrak{a}$ is an ideal, then $\phi^{-1}(\mathfrak{b})$ is an ideal containing $\mathfrak{a}$. Then check ϕ is well-defined, i.e. that if $\mathfrak{b} \subseteq A$ is an ideal containing $\mathfrak{a}$, then $\phi(\mathfrak{b})$ is an ideal of $A/\mathfrak{a}$. Finally check that $\phi(\phi^{-1}(\mathfrak{b})) = \mathfrak{b}$ and $\phi^{-1}(\phi(\mathfrak{b}) = \mathfrak{b}$ if $\mathfrak{b}$ contains $\mathfrak{a}$, so that ϕ and ϕ^{-1} are inverse operations. □

Definition. Let A be a ring.

- An element $x \in A$ is a **unit** if there exists a y such that $xy = 1$.[1]
- An element $0 \neq x \in A$ is a **zero-divisor** if there exists a $y \neq 0$ such that $xy = 0$.
- A ring is an **integral domain** if it has no zero-divisors
- A ring is a **field** if all its non-zero elements are units

Proposition. *Let $x \in A$. Then x is a unit $\Leftrightarrow (x) = (1) = A$.*

Proof. If x is a unit, there exists a $y \in A$ such that $xy = 1$, hence for every $z \in A$, we have $(zy)x = z(yx) = z1 = z \in (x)$, so $(x) = A$.

Conversely, if $(x) = A$, then there exists a y such that $yx = 1$. □

[1] Prove that the units of A form a group under multiplication.

Key concepts Lecture 1

- Rings
- Polynomial ring of a base ring
- Homomorphism
- Isomorphism
- Evaluation homomorphism
- Ideal
- Principal ideal
- Ideals of $\mathbb{Z}$
- Quotient rings
- Integers modulo n, $\mathbb{Z}_n$
- Kernel of a homomorphism
- Kernels are ideals
- The fundamental homomorphism theorem
- Relation between ideals of A and of $A/\mathfrak{a}$
- Unit
- Zero-divisor
- Integral domain
- Field

2. Lecture 2 – Prime and maximal ideals, radicals

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

(1) *A is a field.*
(2) *A has exactly two ideals, $(0) \neq (1)$.*
(3) *Every homomorphism $\phi\colon A \to B$ with $B \neq 0$ is injective.*

Proof. (1) $\Rightarrow$ (2), since if $I \subset A$ is an ideal with $I \neq (0)$, there is an $a \neq 0$ in I. Since A is a field, there is an element $b \in A$ with $ab = 1$, hence $1 \in I$. Then for every $c \in A$, we have $c = c1 \in I$, so $I = A = (1)$.

(2) $\Rightarrow$ (3) If $B \neq 0$, then $1 \neq 0$ in B. Since $\phi(1) = 1$, we have $1 \notin \ker\phi$, and so $\ker\phi \neq (1)$. Hence $\ker\phi = (0)$, which means ϕ is injective.

(3) $\Rightarrow$ (1) Omitted □

2.1. Prime and maximal ideals.

Definition. Let A be a ring, and let $\mathfrak{a} \subseteq A$ be an ideal. We say $\mathfrak{a}$ is a

- **prime** ideal if, for any $a, b \in A \setminus \mathfrak{a}$ we have $ab \notin \mathfrak{a}$
- **maximal** ideal if $\mathfrak{a} \neq (1)$, and the only ideal containing $\mathfrak{a}$ is (1).

We write $\mathrm{Spec}(A)$ for the set of prime ideals of A, called the **spectrum** of A.

Example. In $\mathbb{Z}$, the prime ideals are (0) and (p) for primes p. These are prime since

$$a, b \notin (0) \Leftrightarrow a, b \neq 0 \Rightarrow ab \neq 0 \Leftrightarrow ab \notin (0)$$

and

$$a, b \notin (p) \Leftrightarrow p \text{ does not divide } a, b \Rightarrow p \text{ does not divide } ab \Leftrightarrow ab \notin (p)$$

The maximal ideals are the ideals (p), for all primes p.

Example. Let k be a field. The ideals of $k[x]$ are all principal. An ideal $(f) \subseteq k[x]$ is

- prime if f is irreducible or $f = 0$.
- maximal if f is irreducible.

Proposition. (1) *An ideal $\mathfrak{a} \subseteq A$ is prime if and only if $A/\mathfrak{a}$ is an integral domain.*
(2) *It is maximal if and only if $A/\mathfrak{a}$ is a field.*

Proof. (1) If $\mathfrak{a}$ is prime, then given $a, b \in A \setminus \mathfrak{a}$, we have $ab \notin \mathfrak{a}$. Then $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} \neq 0 + \mathfrak{a} \in A/\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is not prime, there exist $a, b \in A \setminus \mathfrak{a}$ such that $ab \in \mathfrak{a}$, which gives that $(a + \mathfrak{a})(b + \mathfrak{a}) = 0$ in $A/\mathfrak{a}$, proving $A/\mathfrak{a}$ is not an integral domain.

(2) $A/\mathfrak{a}$ is a field $\Leftrightarrow$ $A/\mathfrak{a}$ has exactly two ideals $\Leftrightarrow$ There are exactly two ideals in A containing $\mathfrak{a}$ $\Leftrightarrow$ $\mathfrak{a}$ is maximal

□

Corollary. *Every maximal ideal is a prime ideal.*

Proof. $\mathfrak{a}$ maximal $\Leftrightarrow$ $A/\mathfrak{a}$ a field $\Rightarrow$ $A/\mathfrak{a}$ an integral domain $\Leftrightarrow$ $\mathfrak{a}$ a prime ideal. □

Example. Let k be a field, let $a_1, \ldots, a_n \in k$ and consider the homomorphism $\phi\colon k[x_1, \ldots, x_n] \to k$ given by $\phi(f) = f(a_1, \cdots, a_n)$, i.e. evaluate the polynomial f by substituting a_i for x_i. This ϕ is surjective, and the ideal $\ker\phi$ is maximal, since

$$k[x_1, \ldots, x_n]/\ker\phi \cong \mathrm{im}\,\phi = k,$$

which is a field.

2.2. **Existence of maximal ideals.**

Theorem. *Let A be a non-zero ring. There exists a maximal ideal $\mathfrak{m} \subseteq A$.*

Corollary. *If $\mathfrak{a} \subset A$ is an ideal and $\mathfrak{a} \neq (1)$, then there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.*

Proof. $A/\mathfrak{a}$ has a maximal ideal, which under the correspondence between ideals of A and those of $A/\mathfrak{a}$ gives a maximal ideal containing $\mathfrak{a}$. □

Corollary. *Let f be a ring. Then f is a non-unit if and only if f is contained in a maximal ideal.*

Proof. f a non-unit $\Leftrightarrow (f) \neq (1) \Leftrightarrow (f) \subseteq \mathfrak{m}$ for a maximal $\mathfrak{m} \Leftrightarrow f \in \mathfrak{m}$ for a maximal $\mathfrak{m}$. □

The proof of the theorem uses **Zorn's lemma**.

Definition. A **partially ordered set** is a set S and a binary relation $\leq$ on the elements of S such that

(1) For all $x \in S$, $x \leq x$.
(2) For $x, y, z \in S$ such that $x \leq y$ and $y \leq z$, we have $x \leq z$.
(3) If $x \leq y$ and $y \leq x$, then $x = y$.

Remark. Given x, y in a partially ordered set S, they may be incomparable in the sense that neither $x \leq y$ nor $y \leq x$.

Definition. Let R be a subset of a partially ordered set $(S, \leq)$. An element $x \in S$ is an **upper bound** for R if for every $y \in R$ we have $y \leq x$.

Definition. An element $x \in S$ is **maximal** if there is no $y \in S$ with $x < y$ (meaning $x \leq y$ and $y \neq x$).

Definition. A subset $R \subseteq S$ of a partially ordered set is a **chain** if for every $x, y \in R$ we have either $x \leq y$ or $y \leq x$.

Example. The set of positive integers admits a partial ordering with $m \leq n$ if and only if $n \mid m$. So e.g. $2 \geq 4 \geq 12$, while 2 and 3 are incomparable. The subset $R = \{2^n \mid n \geq 0\}$ is a chain, since every pair of elements is comparable. This set has a unique maximal element 1.

Theorem (Zorn's lemma)**.** *Let S be a partially ordered set, and assume that every chain $R \subseteq S$ has an upper bound. Then S has a maximal element.*

Proof of existence of maximal ideals. Let S be the set of ideals $\mathfrak{a} \subseteq A$ such that $\mathfrak{a} \neq (1)$. We claim that every chain in S admits an upper bound. Let $\{\mathfrak{a}_i\}_{i \in R}$ be a chain of ideals in S. Define $\mathfrak{a} = \bigcup_{i \in R} \mathfrak{a}_i$. We then have

(1) $\mathfrak{a}$ is a subgroup of $(A, +)$: If $a, b \in \mathfrak{a}$, there are $i, j \in R$ such that $a \in \mathfrak{a}_i$ and $b \in \mathfrak{a}_j$. Now as R is totally ordered, we have either $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$. In either case, we will have that $a + b$ is contained in the bigger of the two ideals, so $\mathfrak{a}$ is closed under addition. It's easy to check that $\mathfrak{a}$ is closed under additive inverses and multiplication from A, so $\mathfrak{a}$ is an ideal.
(2) $\mathfrak{a} \neq (1)$, since if $1 \in \mathfrak{a}$, we must have $1 \in \mathfrak{a}_i$ for some $i \in R$, contradicting the assumption that $\mathfrak{a}_i \in S$.

Thus $\mathfrak{a}$ is an upper bound for the chain R. Since every chain of ideals has an upper bound, Zorn's lemma tells us that maximal ideals exist. □

2.3. **Local rings.**

Definition. A ring A is **local** if it has precisely one maximal ideal.

Example. Every field is a local ring with maximal ideal (0).

Example. Let p be a prime, and let $k \geq 1$. Then the ideals of $\mathbb{Z}/(p^k)$ correspond to ideals of $\mathbb{Z}$ which contain (p^k). These are given by (n), where n divides p^k, and so the ideals of $\mathbb{Z}/(p^k)$ are the images of

$$(p^k) \subset (p^{k-1}) \subset \cdots \subset (p) \subset \mathbb{Z}.$$

The unique maximal ideal is the image of (p), so $\mathbb{Z}/(p^k)$ is local.

Example. Let k be a field, and let $A = k[x]/(x^2)$. The ideals of A are in bijection with the ideals of $k[x]$ which contain (x^2). Such an ideal is of the form (f) with f dividing x^2, which means that up to some scalar multiple it is either 1, x or x^2. So in $k[x]$ there are three ideals containing (x^2), namely $(1), (x)$ and (x^2). In A, if we let $\overline{x}$ be the image of x under the quotient map, we have three ideals total

$$(0) = (\bar{x}^2) \subset (\bar{x}) \subset (1) = A.$$

The ideal $(\bar{x})$ is the unique maximal element of A, so A is local.

Proposition. *In a local ring A with maximal ideal $\mathfrak{m}$, the set of units is $A \setminus \mathfrak{m}$.*

Proof. $f \in A$ is a unit $\Leftrightarrow$ f is not contained in a maximal ideal $\Leftrightarrow$ $f \notin \mathfrak{m}$. □

2.4. **Radicals.**

Definition. An element a of a ring A is **nilpotent** if there exists an $n \geq 1$ such that $x^n = 0$. The set of nilpotent elements of A is called the **nilradical** of A, denoted $\mathfrak{N}$.

Proposition. *The nilradical of A is an ideal.*

Proof. It is easy to see that if $a \in \mathfrak{N}$, and $x \in A$, then $-a \in \mathfrak{N}$ and $xa \in \mathfrak{N}$. To see that $\mathfrak{N}$ is closed under addition, observe that if $a, b \in \mathfrak{N}$, we have $m, n \geq 0$ such that $a^m = b^n = 0$. Now compute

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}.$$

If $i \geq m$, then $a^i = 0$, while if $i < m$, then $m + n - i \geq n$ so $b^{m+n-i} = 0$. Hence all terms vanish and so $a + b \in \mathfrak{N}$. □

Theorem. *The nilradical $\mathfrak{N}$ of A is the intersection of all prime ideals of A.*

Half of the proof. Easy half: If $f \in A$ is nilpotent and $\mathfrak{p}$ is prime ideal, then $f^n = 0 \Rightarrow f^n \in \mathfrak{p} \Leftrightarrow f \in \mathfrak{p}$. This gives us $\mathfrak{N} \subseteq \cap \mathfrak{p}$.

Hard half: If $f \in A$ is contained in all prime ideals of A, then f is nilpotent. □

Example. In any integral domain, obviously f is nilpotent if and only if $f = 0$, so $\mathfrak{N} = (0)$.

In $\mathbb{Z}/(p^k)$, we have just one prime ideal (p), so $\mathfrak{N} = (p)$.

Definition. Let A be a ring. The **Jacobson radical** of A, denoted $\mathfrak{R}$, is the intersection of all the maximal ideals of A.

Example. In $\mathbb{Z}$, a field k, and $k[x_1, \ldots, x_n]$, we have $\mathfrak{R} = (0)$, while in a local ring A, we by definition have $\mathfrak{R} = \mathfrak{m}$, the unique local ideal.

Key concepts Lecture 2

- Prime ideal
- Maximal ideal
- Prime and maximal ideals in $\mathbb{Z}$ and $k[x]$
- Quotient rings of prime and maximal ideals are integral domains and fields, respectively
- Theorem of existence of maximal ideals, statement and corollaries
- Theorem of existence of maximal ideals, main idea of proof
- Local ring
- Nilradical
- Description of nilradical via prime ideals
- Jacobson radical

Suggested problems week 1

(1) Prove that if A is a ring such that $1 = 0$, then A is the 0 ring.
(2) Prove Proposition 1.1. in [AM].
(3) Use the relation between ideals in $\mathbb{Z}$ and $\mathbb{Z}/(n) = \mathbb{Z}_n$ to show that the number of ideals in $\mathbb{Z}_n$ equals the number of positive integers dividing n.
(4) Let k be a field, and prove that the ideal
$$(x, y) = \{g_1 x + g_2 y \mid g_1, g_2 \in k[x, y]\} \subseteq k[x, y]$$
is not a principal ideal.
(5) Let $\mathfrak{a} \subset \mathbb{Z}[x]$ be the set of polynomials such that $f \in \mathfrak{a}$ if and only if $f(0)$ is even. Show that $\mathfrak{a}$ is an ideal, and that it is not a principal ideal.
(6) Prove that a ring A is an integral domain if and only if $A[x]$ is an integral domain.
(7) Convince yourself that for any ring A, we have an isomorphism $(A[x])[y] \cong A[x, y]$
(8) Let A be a ring. Prove that there exists some field k such that there is a surjective homomorphism $\phi\colon A \to k$.
(9) Let A be a ring. Prove that there exists a unique homomorphism $\phi\colon \mathbb{Z} \to A$.
(10) Let A be a ring, and let $a \in A$. Prove that there exists a unique homomorphism $\phi\colon \mathbb{Z}[x] \to A$ such that $\phi(x) = a$. Use this to describe the set of all homomorphisms $\phi\colon \mathbb{Z}[x] \to A$.

From Atiyah–Macdonald chapter 1: 1, 7, 8, 9, 10, 12, 15, 16.

3. Lecture 3 – Operations on ideals

Let A be a ring. We've seen two ways of constructing ideals, either as principal ideals $(f) \subseteq A$ for some $f \in A$, or by the general existence result giving us a maximal ideal $\mathfrak{m} \subset A$.

There are a few natural operations we have access to in order to build more ideals.

3.1. **Addition.**

Definition (Addition)**.** Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals. The set

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \subseteq A$$

is an ideal. Given a sequence $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$, the set

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = \{a_1 + \cdots + a_n \mid a_i \in \mathfrak{a}_i\}$$

is an ideal. Given an collection of ideals $\{\mathfrak{a}_i\}_{i \in I}$, the sum $\sum_{i \in I} \mathfrak{a}_i$ has as elements all finite sums $a_{i_1} + \cdots + a_{i_n}$, where $i_1, \ldots, i_n \in I$ and $a_{i_j} \in \mathfrak{a}_{i_j}$.

Remark. The ideal $\mathfrak{a} + \mathfrak{b}$ is the smallest ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$. Similar statements hold for the more general versions.

Example. In $\mathbb{Z}$, given ideals (m) and (n), with $m, n > 0$, we have the ideal

$$(m) + (n) = \{xm + yn \mid x, y \in \mathbb{Z}\}.$$

We know that $(m) + (n) = (k)$ for some integer k, and we know that $(m) + (n)$ is the smallest ideal containing (m) and (n). This means that k must be the biggest number dividing both m and n, and so $k = \gcd(m, n)$.

Definition. If $a_1, \ldots, a_n \in A$, then we write

$$(a_1, \ldots, a_n) = (a_1) + (a_2) + \cdots + (a_n) = \{x_1 a_1 + \cdots + x_n a_n \mid x_i \in A\}.$$

An ideal that can be written in this form is called **finitely generated**.

Example. In the ring $\mathbb{Q}[x, y]$, we have the ideal (x, y). This consists of all polynomials f which can be written in the form

$$f = xg_1 + yg_2 \qquad g_i \in \mathbb{Q}[x, y].$$

Writing

$$f = \sum_{i,j \geq 0} a_{ij} x^i y^j \qquad a_{ij} \in \mathbb{Q},$$

we have $f \in (x, y)$ if and only if $a_{00} = 0$. On the one hand, if $f = xg_1 + yg_2$, then clearly $a_{00} = 0$. On the other, if $a_{00} = 0$, we can write

$$f = x(\sum_{i \geq 1} \sum_{j \geq 0} a_{ij} x^{i-1} y^j) + y(\sum_{j \geq 1} a_{0j} y^{j-1}) \in (x, y).$$

Lemma (A computational trick)**.** *Let $a_1, a_2, b \in A$. Then we have an equality of ideals*

$$(a_1, a_2) = (a_1, a_2 + ba_1).$$

Proof. We clearly have $a_1 \in (a_1, a_2)$, and $a_2 + ba_1 \in (a_1, a_2)$. This means that $(a_1, a_2 + ba_1) \subseteq (a_1, a_2)$.

On the other hand, we have $a_1 \in (a_1, a_2 + ba_1)$, and, since $a_2 = -ba_1 + (a_2 + ba_1)$, that $a_2 \in (a_1, a_2 + ba_1)$. Thus $(a_1, a_2) \subseteq (a_1, a_2 + ba_1)$, and we are done. $\square$

Example. In the ring $\mathbb{Z}$, we have

$$(5,7) = (5,7-5) = (5,2) = (5-2\cdot 2,2) = (1,2) = (1,2-2\cdot 1) = (1,0) = (1).$$

You may recognize this as the Euclidean algorithm for finding the greatest common divisor of two integers.

Example. In $\mathbb{Q}[x]$, we have

$$(x-2,2x^2-2) = (x-2,(2x^2-2)-2x(x-2)) = (x-2,4x-2) = (x-2,4x-2-4(x-2)) = (x-2,6).$$

Since 6 lies in the ideal, so must $\frac{1}{6}6 = 1$, so $(x-2,2x^2-2) = (1)$.

Definition (Intersection)**.** Let $\mathfrak{a},\mathfrak{b} \subseteq A$ be ideals, then $\mathfrak{a}\cap\mathfrak{b} \subseteq A$ is also an ideal. Similarly given $\{\mathfrak{a}_i\} \subseteq A$, we have $\cap_{i\in I}\mathfrak{a}_i$ is an ideal.

Remark. The ideal $\mathfrak{a}\cap\mathfrak{b}$ is the biggest ideal contained in $\mathfrak{a}$ and in $\mathfrak{b}$.

Example. Given $m,n \geq 0$, we have $(m),(n) \subseteq \mathbb{Z}$, and moreover

$$(m)\cap(n) = \{k\in\mathbb{Z} \mid m|k \text{ and } n|k\} = \{k\in\mathbb{Z} \mid \operatorname{lcm}(m,n)|k\} = (\operatorname{lcm}(m,n)).$$

Example. Working in $\mathbb{Q}[x,y]$, we have that $(x)\cap(y)$ is the ideal consisting of those f which can be written both as xg and as yh. Writing $f = \sum a_{ij}x^iy^j$, $a_{ij}\in\mathbb{Q}$, the first condition becomes $a_{0j} = 0$ for all j, while the second becomes $a_{j0} = 0$ for all j. It follows that $f \in (x)\cap(y)$ if and only if $a_{ij} = 0$ whenever i or j is 0, which is the same as saying $f \in (xy)$, so $(x)\cap(y) = (xy)$.

Definition (Product)**.** Given two ideals $\mathfrak{a},\mathfrak{b}$, the **product ideal** is

$$\mathfrak{a}\mathfrak{b} = \{\sum_{i=1}^{n} a_ib_i \mid a_i\in\mathfrak{a}, b_i\in\mathfrak{b}\},$$

i.e. the set of elements which are finite sums of products of elements from $\mathfrak{a}$ and $\mathfrak{b}$. Given $\mathfrak{a}_1,\ldots,\mathfrak{a}_k$, the product $\mathfrak{a}_1\cdots\mathfrak{a}_k$ is defined similarly

$$\mathfrak{a}_1\cdots\mathfrak{a}_k = \{\sum_{i=1}^{n} a_{i1}\cdots a_{ik} \mid a_{ij}\in\mathfrak{a}_j\}.$$

Example. Let $m,n\in\mathbb{Z}$, then

$$(m)(n) = \{\sum_{i=1}^{k} a_ib_i \mid a_i\in(m), b_i\in(n)\} \overset{\substack{a_i=l_im\\ b_i=j_in}}{=} \{\sum_{i=1}^{n} l_imj_in \mid l_i,j_i\in\mathbb{Z}\} = (mn).$$

Example. More generally, given $a_1,a_2,\ldots,a_n\in A$, we have

$$(a_1)(a_2)\cdots(a_n) = (a_1a_2\cdots a_n) \subseteq A$$

Remark. We always have $\mathfrak{a}_1\cdots\mathfrak{a}_n \subseteq \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n$.

Example. The union of two ideals is usually not an ideal, e.g. $(2)\cup(3)$ is not an ideal of $\mathbb{Z}$.

There are various rules for manipulating these three operations (intersection, addition and multiplication) of ideals, e.g. $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}$. The set of ideals with operations of addition and multiplication forms a semiring, i.e. a structure with all the ring axioms except additive inverses.

3.2. **Coprime ideals.**

Definition. We say that two ideals $\mathfrak{a}, \mathfrak{b} \in A$ are **coprime** if $\mathfrak{a} + \mathfrak{b} = (1)$.

Remark. Since an ideal equals (1) if and only if it contains the element 1, we have that $\mathfrak{a} + \mathfrak{b}$ are coprime if and only if there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$.

Example. In $\mathbb{Z}$, we know that $(m)+(n) = (\gcd(m, n))$, so (m) and (n) are coprime if and only if $\gcd(m, n) = 1$, i.e. if the numbers m and n are coprime.

Example. We computed above that $(x - 2, 2x^2 - 2) = (1)$ in $\mathbb{Q}[x]$, so the ideals $(x - 2)$ and $(2x^2 - 2)$ in $\mathbb{Q}[x]$ are coprime.

Example. If $f \in (x) + (y) \subseteq \mathbb{Q}[x, y]$, then $f = \sum a_{ij} x^i y^j$ where we must have $a_{00} = 0$. This means that $1 \notin (x) + (y)$, so (x) and (y) are not coprime.

Proposition. *Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals. If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.*

Proof. If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, this means that we can find $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. Now if $x \in \mathfrak{a} \cap \mathfrak{b}$ we also have

$$x = 1x = ax + bx.$$

Since $x \in \mathfrak{b}$, we have $ax \in \mathfrak{ab}$, and since $x \in \mathfrak{a}$, we have $bx \in \mathfrak{ab}$. It follows that $x \in \mathfrak{ab}$. □

Example. If m, n are coprime, then $\operatorname{lcm}(m, n) = mn$, so $(m) \cap (n) = (\operatorname{lcm}(m, n)) = (mn) = (m)(n)$.

Recall that given rings $A_1, \ldots, A_n$, we have the **product ring**

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n,$$

whose elements are n-tuples $(a_1, \ldots, a_n)$, with addition and multiplication defined componentwise.

Given ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$, we have homomorphisms $A \to A/\mathfrak{a}_i$ for each i, and we can take a product homomorphism $\phi\colon A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$ given by

$$\phi(a) = (a + \mathfrak{a}_1, a + \mathfrak{a}_2, \ldots, a + \mathfrak{a}_n).$$

Theorem (Generalised Chinese remainder theorem)**.** *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$. Assume that the $\mathfrak{a}_i$ are pairwise coprime. Then the homomorphism $\phi\colon A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$ is surjective, and*

$$\ker \phi = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n,$$

hence we have an isomorphism

$$A/\prod \mathfrak{a}_i = A/\ker \phi \cong \phi(A) = \prod A/\mathfrak{a}_i.$$

Proof assuming $n = 2$: ϕ is surjective: It's enough to show that $(1, 0), (0, 1) \in \phi(A)$, since if $\phi(x_1) = (1, 0)$ and $\phi(x_2) = (0, 1)$, since every element $(b_1 + \mathfrak{a}_1, b_2 + \mathfrak{a}_2)$ is then equal to $\phi(b_1 x_1 + b_2 x_2)$.

Coprimality of $\mathfrak{a}_1$ and $\mathfrak{a}_2$ means there are $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. But now

$$\phi(a_1) = (a_1 + \mathfrak{a}_1, a_1 + \mathfrak{a}_2) = (a_1 + \mathfrak{a}_1, (1 - a_2) + \mathfrak{a}_2) = (0, 1),$$

and similarly we get $\phi(a_2) = (1, 0)$.

It is clear that $\phi(x) = 0$ is equivalent to $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, so $\ker \phi = \mathfrak{a}_1 \cap \mathfrak{a}_2$, and we know that $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1 \mathfrak{a}_2$. □

Example (Chinese remainder theorem)**.** If $k_1, \ldots, k_n$ are pairwise coprime integers, then $\mathbb{Z}/\prod k_i \cong \prod \mathbb{Z}/(k_i)$. In particular if $n = \prod p_1^{e_1} \ldots p_k^{e_k}$ is the prime factorisation of an integer n, we have

$$\mathbb{Z}/(n) = \prod \mathbb{Z}/(p_i^{e_i})$$

Example. In the example above, we showed $(x-2), (2x^2-2) \subseteq \mathbb{Q}[x]$ are coprime. We therefore have

$$\mathbb{Q}[x]/(x-2)(2x^2-2) = \mathbb{Q}[x]/((x-2)(2x^2-2)) = \mathbb{Q}[x]/(x-2) \times \mathbb{Q}[x]/(2x^2-2) \cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2}).$$

Main ideas:

- Sum of ideals
- Intersection of ideals
- Products of ideals
- The ideal $(a_1, \ldots, a_n)$
- Coprime ideals
- The Chinese remainder theorem

4. Lecture 4 – Further operations on ideals + modules

4.1. **Ideal quotient.**

Definition. Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals. The ideal quotient $(\mathfrak{a} : \mathfrak{b}) \subset A$ is the set of $x \in A$ such that $x\mathfrak{b} \subseteq \mathfrak{a}$, i.e. the set of x such that for every $b \in \mathfrak{b}$, we have $xb \in \mathfrak{a}$. (This is an ideal.)

Example. If $\mathfrak{a} \subseteq A$ is an ideal, then $(\mathfrak{a} : \mathfrak{a}) = (1)$, since $x \in (\mathfrak{a} : \mathfrak{a})$ means that $xa \in \mathfrak{a}$ for all $a \in \mathfrak{a}$. But since $\mathfrak{a}$ is closed under multiplication from A, this holds for all $x \in A = (1)$.

Example. If $\mathfrak{a} \subseteq A$ is an ideal and $b \in A$, then $x \in (\mathfrak{a} : (b))$ if and only if $xb \in \mathfrak{a}$.

Proof: If $x \in (\mathfrak{a} : (b))$, then since $b \in (b)$, we have $xb \in \mathfrak{a}$. Conversely, suppose $xb \in \mathfrak{a}$. The elements of (b) are all of the form yb with $y \in A$, and we then have $x(yb) = y(xb) \in \mathfrak{a}$, so $x \in (\mathfrak{a} : (b))$.

Example. If $m, n \geq 1$, then $x \in ((m) : (n))$ if and only if $xn \in (m)$, so

$$((m) : (n)) = \{x \mid xn \in (m)\} = \{x \mid m \text{ divides } xn\}.$$

This means that $((m) : (n)) = (k)$, we in particular have that k is the smallest positive integer such that m divides kn. In particular, if n divides m, then $k = m/n$.

Definition. The **annihilator** of an ideal $\mathfrak{a} \subseteq A$ is defined as

$$\mathrm{Ann}(\mathfrak{a}) = (0 : \mathfrak{a}) = \{x \in A \mid xa = 0 \qquad \forall a \in \mathfrak{a}\}$$

The annihilator of an element $a \in A$ is

$$\mathrm{Ann}(a) = \mathrm{Ann}((a)) = (0 : (a)) = \{x \in A \mid xa = 0\}.$$

Example. In an integral domain A, if $a \neq 0$, then $\mathrm{Ann}(a) = (0)$.

In any ring A, the set of zero-divisors is $\bigcup_{a \in A \setminus \{0\}} \mathrm{Ann}(a)$.

4.2. **Radicals.**

Definition. Let A be a ring, $\mathfrak{a} \subseteq A$ an ideal. The **radical** of $\mathfrak{a}$ is the set of $x \in A$ such that there is an $n \geq 1$ such that $x^n \in \mathfrak{a}$. We denote this by $\mathfrak{r}(\mathfrak{a})$, one occasionally sees $\sqrt{\mathfrak{a}}$.

Example. The radical $\mathfrak{r}((0))$ is exactly the same thing as the nilradical $\mathfrak{N} \subseteq A$, since $x^n \in (0)$ for some $n \Leftrightarrow x^n = 0$ for some $n \Leftrightarrow x \in N$.

Proposition. *The set $\mathfrak{r}(\mathfrak{a})$ is an ideal, and equals the intersection of the prime ideals containing $\mathfrak{a}$.*

The proofs are generalisations of the corresponding statements for the nilradical. Alternatively one can use the following:

Proposition. *Let $\mathfrak{N}$ be the nilradical of $A/\mathfrak{a}$, and let $\phi\colon A \to A/\mathfrak{a}$ be the quotient homomorphism. Then $\mathfrak{r}(\mathfrak{a}) = \phi^{-1}(\mathfrak{N})$.*

Proof. Let $x \in A$. Then if $x \in \mathfrak{r}(\mathfrak{a})$ we have for some $n \geq 1$ that

$$x^n \in \mathfrak{a} \Leftrightarrow \phi(x^n) = 0 \Leftrightarrow \phi(x)^n = 0 \Rightarrow \phi(x) \in \mathfrak{N}.$$

□

Example. Let $n \geq 1$ have prime factorisation $n = p_1^{e_1} \cdots p_k^{e_k}$. Then $m \in \mathbb{Z}$ lies in $\mathfrak{r}((n))$ if and only if there is an $l \geq 1$ such that $m^l \in (n)$, which is if and only if m^l is divisible by n. If every p_i divides m, then $m^{\max e_i}$ is divisible by n, while if some p_i does not divide m, then no power of m is divisible by n.

Summing up, m lies in $\mathfrak{r}((n))$ if and only if m is divisible by each p_i, which is the same as saying m is divisible by $p_1 \dots p_k$, and we thus get

$$\mathfrak{r}((n)) = (p_1 \cdots p_k).^2$$

Example. Consider $\mathbb{Q}[x]$ and the ideal (x^m). Then $f \in \mathfrak{r}((x^m))$ is equivalent to f^n is divisible by x^m for some $n \geq 1$. Let

$$f = a_0 + a_1 x + \cdots + a_d x^d.$$

Then if $a_0 \neq 0$, we have $f^n = a_0^n + x(\dots)$, so $f^n \notin (x^m)$ for all $n \geq 1$. If $a_0 = 0$, then $f^m = a_1^m x^m + x^{m+1}(\dots)$, so $f^m \in (x^m)$. Thus $f \in \mathfrak{r}((x^m))$ if and only if $a_0 = 0$, which is if and only if $f \in (x)$. We've shown

$$\mathfrak{r}((x^m)) = (x).$$

4.3. **Extension and contraction of ideals.**

Definition. Let $\phi\colon A \to B$ be a homomorphism, let $\mathfrak{a} \subseteq A$ and $\mathfrak{b} \subseteq B$ be ideals. The **extension** of $\mathfrak{a}$ is the smallest ideal in B containing $\phi(\mathfrak{a})$, denoted $\mathfrak{a}^e$. The **contraction** of $\mathfrak{b}$ is $\phi^{-1}(\mathfrak{b}) \subseteq A$, denoted $\mathfrak{b}^c$.

Both of these are ideals.

Remark. The image $\phi(\mathfrak{a}) \subseteq B$ is not itself an ideal, take e.g. the homomorphism $\phi\colon \mathbb{Q} \to \mathbb{R}$, where $\phi(\mathbb{Q})$ is not an ideal in $\mathbb{R}$.

Concretely, the elements of $\mathfrak{a}^e$ are all finite sums $\phi(a_1) + \cdots + \phi(a_n)$ with $a_i \in \mathfrak{a}$.

Proposition. *The operation of contraction sends prime ideals to prime ideals.*

Proof. Let $\mathfrak{p} \subset B$ be a prime ideal, and let $\phi\colon A \to B$ be a ring homomorphism. We must show that $\mathfrak{p}^c = \phi^{-1}(\mathfrak{p})$ is a prime ideal. If $a, a' \in A \setminus \phi^{-1}(\mathfrak{p})$, then $\phi(a), \phi(a') \notin \mathfrak{p}$, so $\phi(aa') = \phi(a)\phi(a') \notin \mathfrak{p}$, which means $aa' \notin \phi^{-1}(p)$, and that means $\phi^{-1}(\mathfrak{p})$ is prime. □

4.4. **Modules.** Informally, a module is a structure where you can add elements in the module, and multiply module elements by the ring elements.

Definition. Let A be a ring. A **module** over A (or "A-module") is an abelian group $(M, +)$ equipped with an operation $A \times M \to M$, denoted

$$(a, m) \mapsto am,$$

satisfying

(1) $1m = m \quad \forall m \in M.$
(2) $a(bm) = (ab)m \quad \forall a, b \in A, m \in M$
(3) $(a + b)m = am + bm \quad \forall a, b \in A, m \in M$
(4) $a(m + n) = am + bn \quad \forall a \in A, m + n \in M.$

Example. For any ring A, the 0-module has one element 0, and addition and multiplication are trivially defined.

[2] Look up the "abc conjecture" for a natural appearance of this operation in number theory.

Example. Let k be a field. Then a k-module is quite literally the same thing as a k-vector space.

Example. A $\mathbb{Z}$-module is the "same thing" as an abelian group, meaning any abelian group admits a unique structure as a $\mathbb{Z}$-module. To see this, let G be an abelian group. We define a $\mathbb{Z}$-module structure on G by, for $n \in \mathbb{Z}, g \in G$

$$ng = \begin{cases} \overbrace{g + \cdots + g}^{n} \text{ if } n > 0 \\ 0g = 0 \\ ng = \overbrace{(-g) + \cdots + (-g)}^{-n} \text{ if } n < 0. \end{cases}$$

One can check that this is a well-defined $\mathbb{Z}$-module structure. Moreover, this $\mathbb{Z}$-module structure is forced on us by the axioms: If $n > 0$ we must have

$$ng = (1 + \cdots + 1)g = 1g + 1g + \cdots + 1g = \overbrace{g + \cdots + g}^{n},$$

and similar considerations tell us what ng has to be for $n \leq 0$.

Example. Let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ is an A-module in a natural way, since given $x \in A$ and $a \in \mathfrak{a}$, we have $xa \in \mathfrak{a}$, and the operation $(x, a) \mapsto xa$ satisfies the axioms of the definition.

Example. Let $\phi\colon A \to B$ be a homomorphism. Then B has a natural structure of A-module, defined by

$$ab = \phi(a)b \qquad \forall a \in A, b \in B.$$

This generalises the useful fact from field theory that if $\phi\colon k \to k'$ is a homomorphism of fields, then k' is a k-vector space.

Definition. Let M and N be A-modules. A **homomorphism** of A-modules from M to N is a map $\phi\colon M \to N$ such that

$$\phi(m + m') = \phi(m) + \phi(m') \quad \forall m, m' \in M$$
$$\phi(am) = a\phi(m) \qquad \forall a \in A, m \in M$$

If ϕ is a bijection, we say it is an **isomorphism** of A-modules.

Example. For A-modules M and N, we always have a homomorphism $0\colon M \to N$ given by

$$0(m) = 0 \qquad \forall m \in M.$$

Example. Let k be a field, and let M and N be k-modules. Then a homomorphism $M \to N$ is the same thing as a linear map of vector spaces. So if M and N are finite-dimensional as vector spaces, we can choose bases and represent ϕ by a $(\dim N) \times (\dim M)$-matrix.

Example. A homomorphism of $\mathbb{Z}$-modules is the same thing as a homomorphism of (abelian) groups. This boils down to the fact that given a homomorphism $\phi\colon M \to N$ of abelian groups, the condition

$$\phi(nx) = n\phi(x)$$

is automatically satisfied.

Example. Let $a \in A$, and consider $(a) \subseteq A$ as an A-module. There is a homomorphism of A-modules

$$\phi\colon A \to (a)$$

given by

$$\phi(x) = xa.$$

This is surjective, with kernel equal to $\mathrm{Ann}(a)$.

Definition. Let M and N be A-modules, and let $\mathrm{Hom}_A(M, N)$ be the set of homomorphisms. This set has a structure of an A-module, where for $\phi, \psi \in \mathrm{Hom}_A(M, N), a \in A$ and $m \in M$, we have

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$
$$(a\phi)(m) = a\phi(m)$$

Example. Let k be a field, and consider the modules k^m, k^n. Then $\mathrm{Hom}_k(k^m, k^n)$ is naturally identified with the set of $(n \times m)$-matrices with entries in k, and the above states that this set has a natural structure of k-module (or k-vector space).

Main concepts lecture 4:

- Ideal quotients
- Annihilator of an ideal
- Radical of an ideal
- Extension and contraction of an ideal
- A-module
- Homomorphism between A-modules

Suggested problems week 2

(*) means I suspect a problem is difficult (and you're not likely to miss anything important by skipping it).

(1) Let A be a ring, let $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_m \in A$. Prove that

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) = (a_1 b_1, a_1 b_2, \ldots, a_n b_m),$$

where the sequence in the rightmost brackets contains every product $a_i b_j$ with $1 \leq i \leq n$ and $1 \leq j \leq m$.

(2) Let A be a ring, and let $a \in A$. Prove that $A[x]/(x-a) \cong A$.

(3) Let A be a ring, let $a, b \in A$. Prove that $A[x]/(x-a, b) \cong A/(b)$.

(4) Let k be a field, and let $f, g \in k[x]$. Prove that if (f) and (g) are coprime if and only if f and g have no common irreducible factor.[3]

(5) Let k be a field, and $0 \neq f \in k[x]$. Prove that $k[x]/(f)$ is isomorphic to a direct product of rings of the form $k[x]/(g^n)$, where g is irreducible.

(6) Let $(a_1, b_1) \neq (a_2, b_2) \in \mathbb{C}^2$. Prove that the ideals $(x - a_1, y - b_1)$ and $(x - a_2, y - b_2)$ in $\mathbb{C}[x, y]$ are coprime.

(7) Show that the ideals $(x-2)$ and $(2x^2 - 2)$ in $\mathbb{Z}[x]$ are not coprime.

(8) Let $a_1, \ldots, a_n, b \in A$, and let $1 \leq i, j \leq n$ with $i \neq j$. Prove that

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_{j-1}, a_j + b a_i, a_{j+1}, \ldots, a_n)$$

(9) Let $a_1, \ldots, a_n \in A$, let $1 \leq i \leq n$, and let $c \in A$ be a unit. Prove that

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_{i-1}, c a_i, a_{i+1}, \ldots, a_n).$$

(10) (*) Let $a_1, \ldots, a_n \in A$, and let $(b_{ij})_{1 \leq i,j \leq n}$ be an invertible matrix with coefficients in A.[4] Prove that

$$(a_1, \ldots, a_n) = \left(\sum_{j=1}^{n} b_{1j} a_j, \sum_{j=1}^{n} b_{2j} a_j, \ldots, \sum_{j=1}^{n} b_{nj} a_j \right).$$

(11) (*) Let $A = \mathbb{Z}[x]/(x^2 + 1)$, and let p be a prime. Show that the extension $(p)^e$ of (p) along $\phi \colon \mathbb{Z} \to A$ is a prime if and only if -1 is a quadratic residue modulo p, that is if and only if the equation $x^2 + 1$ admits solutions in $\mathbb{Z}/(p)$. *Hint:* Show that $A/(p)^e \cong \mathbb{Z}/(p)[x]/(x^2+1)$ and consider what it means for this ring to be an integral domain.

(12) Let $\mathfrak{a}, \mathfrak{p} \subseteq A$ be ideals with $\mathfrak{p}$ prime $\mathfrak{a}$ not contained in $\mathfrak{p}$. Prove that $(\mathfrak{p} : \mathfrak{a}) = \mathfrak{p}$.

(13) Let G be an abelian group, and let $\phi \colon G \to G$ be a group homomorphism. Prove that there is a unique structure of $\mathbb{Z}[x]$-module on G such that $xg = \phi(g)$ for all $g \in G$.

---

[3] Recall that in $k[x]$ every ideal is principal, every polynomial can be factored into irreducible polynomials, and $h \in k[x] \setminus \{0\}$ is irreducible if and only if (h) is prime.

[4] This means that there exist $(c_{ij})_{1 \leq i,j \leq n}$ with $c_{ij} \in A$ such that

$$\sum_{k=1}^{n} b_{ik} c_{kj} = \sum_{k=1}^{n} c_{ik} b_{kj} = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}.$$

(14) Let G be an abelian group and $n \geq 1$. Show that G admits a structure of $\mathbb{Z}/(n)$-module if and only if $\overbrace{g + \cdots + g}^{n} = 0$ for all $g \in G$. Show that if this condition holds, then the structure of $\mathbb{Z}/(n)$-module on G is unique.

(15) Let A be an integral domain and $0 \neq a \in A$. Show that A and (a) are isomorphic as A-modules.

(16) Let M be an A-module. Show that the map $F\colon \operatorname{Hom}_A(A, M) \to M$ given by

$$F(\phi) = \phi(1)$$

is an isomorphism of A-modules.

5. Lecture 5 – Direct sums, submodules and quotient modules

Let A be a ring, and recall that an A-module is an abelian group M equipped with a multiplication map $A \times M \to M$ denoted $(a, m) \to am$, satisfying some axioms. Further, a map $\phi\colon M' \to M$ is a homomorphism if it respects addition and multiplication from A, meaning $\phi(x+y) = \phi(x) + \phi(y)$, and $\phi(ax) = a\phi(x)$.

Important special cases are $\mathbb{Z}$-modules, which are the same things as abelian groups, and k-modules for k a field, which are the same things as vector spaces over k.

5.1. **Direct sums.** Given a sequence of abelian groups $G_1, \ldots, G_n$, the product set $G_1 \times \cdots \times G_n$ is naturally an abelian group. This generalises directly to modules:

Definition. Let M_1, M_2 be A-modules. The direct sum of the M_1 and M_2 is the module

$$M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\},$$

with

$$(m_1, m_2) + (m_1', m_2') = (m_1 + m_1', m_2 + m_2'), \quad a(m_1, m_2) = (am_1, am_2).$$

Definition. Given A-modules $M_1, \ldots, M_n$, we have the direct sum

$$\bigoplus_{i=1}^{n} M_i = M_1 \oplus \cdots \oplus M_n = \{(m_1, \ldots, m_n) \mid m_i \in M_i\},$$

with addition and A-multiplication similar. If $M_1 = \cdots = M_n = M$, we may write $M^{\oplus n}$ instead.

Given a set of A-modules $\{M_i\}_{i \in S}$, their direct sum is

$$\oplus_{i \in S} M_i = \{(m_i)_{i \in S} \mid m_i \in M_i, \text{ only finitely many } m_i \neq 0\},$$

while their direct product is

$$\prod_{i \in S} M_i = \{(m_i)_{i \in S} \mid m_i \in M_i\},$$

If S is finite, then the direct sum and direct product are the same, but in general they differ.

Example. Let k be a field. Every vector space V over k has a basis, meaning there is a set $\{v_i\}_{i \in S}$ such that every $v \in V$ can be expressed uniquely as a sum

$$\sum_{i \in S} a_i v_i \qquad a_i \in k,$$

with only finitely many $a_i \neq 0$.

Define a homomorphism

$$\phi\colon \bigoplus_{i \in S} k \to V$$

by

$$\phi((a_i)) = \sum_{i \in S} a_i v_i.$$

Since $\{v_i\}_{i \in S}$ is a basis for V, every v equals $\phi((a_i))$ for a unique $(a_i) \in \bigoplus_{i \in S} k$, meaning ϕ is an isomorphism, and $\oplus_{i \in S} k \cong V$.

Example. Consider $\mathbb{R}[x, y]$, and define $T = \mathbb{R}[x, y] \oplus \mathbb{R}[x, y]$. Thus elements of T are pairs (f_1, f_2) with $f_1, f_2 \in \mathbb{R}[x, y]$. We may think of elements of T as vector fields on $\mathbb{R}^2$ with components given by polynomials.

Example. Let A be a ring, and consider $A[x]$ as an A-module, i.e. if $f = a_n x^n + \cdots + a_0 \in A[x]$ and $a \in A$, we have

$$af = aa_n x^n + \cdots aa_1 x + aa_0.$$

We have a homomorphism of A-modules

$$\phi\colon \bigoplus_{i \in \mathbb{N}} A \to A[x],$$

Note that this is just a module isomorphism; in fact the left hand side does not have a natural ring structure.

5.2. **Submodules.** If G is an abelian group, a subset $G' \subseteq G$ which is closed under addition and inverses is a subgroup. We can then form the quotient group $G'' = G/G'$, whose elements are the cosets of G' in G. This concept and most of the theory generalises neatly from abelian groups to modules, where we defined submodules as follows.

Definition. Let M be an A-module. A subset $M' \subseteq M$ is a **submodule** if it is a subgroup and for all $a \in A, m \in M'$, we have $am \in M'$.

Example.

- A submodule of A is the same thing as an ideal in A.
- A submodule of a $\mathbb{Z}$-module M is the same thing as a subgroup of M, since if $M' \subseteq M$ is a subgroup, $n \in \mathbb{Z}$ and $m' \in M'$, we automatically have $nm' = m' + \cdots + m' \in M'$ (when n is positive, similar arguments work when n is negative).

Given $M, M' \subseteq N$, we have their sum defined as $M + M' \subseteq N$, given by

$$M + M' = \{m + m' \mid m \in M, m' \in M\}.$$

This generalises the notion of sum of ideals.

Example. With ring $\mathbb{R}[x, y]$ and $T = \mathbb{R}[x, y]^{\oplus 2}$, we have the submodule $T' \subset T$ given by

$$T' = \{(fx, fy) \mid f \in \mathbb{R}[x, y]\}$$

Informally, this is the submodule of vector fields which point outwards from the origin at all points. We have $\phi\colon \mathbb{R}[x, y] \to T$ given by $\phi(f) = (fx, fy)$, and this is an isomorphism.

Let's take $T'' = \{(g, 0) \mid g \in \mathbb{R}[x, y]\} \subset T$, this is again a submodule, the horizontal vector fields.

We have

$$T' + T'' = \{(fx + g, fy) \mid f, g \in \mathbb{R}[x, y]\} = \{(h, fy) \mid h, f \in \mathbb{R}[x, y]\},$$

vector fields which are horizontal along the x-axis.

5.3. **Quotients.** If M' is a submodule of M, then the group M/M' has a natural structure of A-module such that $M \to M/M'$ is a homomorphism of A-modules. Concretely, we define the A-multiplication on M' by

$$a(m + M') = am + M'$$

In particular, for any ideal $\mathfrak{a}$, the quotient ring $A/\mathfrak{a}$ is an A-module.

5.4. **Kernels, images and cokernels.**

Definition. Let $\phi\colon M \to N$ be a homomorphism of A-modules. We have

- The **kernel** of ϕ,
$$\ker \phi \subseteq M,$$
a submodule of M.
- The **image** of ϕ,
$$\operatorname{im} \phi = \{\phi(m) \mid m \in M\} \subseteq N,$$
a submodule of N.
- The **cokernel** of ϕ,
$$\operatorname{cok} \phi = N/\operatorname{im} M.$$

Example. Let $a_1, \ldots, a_n \in A$, and define
$$\phi\colon \bigoplus_{i=1}^{n} A \to A$$
by
$$\phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i a_i.$$
Then
$$\operatorname{im}(\phi) = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in A\} = (a_1, \ldots, a_n) \subseteq A.$$

The following statements are "well known" for abelian groups, and the content of this proposition is that the natural isomorphisms respect the module structures as well.

Proposition ("Module isomorphism theorems")**.**

- *Let $\phi M \to N$ be a homomorphism of modules. We have*
$$\operatorname{im} M \cong M/\ker \phi.$$
- *Let $M'' \subseteq M' \subseteq M$ be A-modules and submodules. There is an isomorphism*
$$M/M'' \cong (M/M')/(M''/M')$$
- *Let M, N be submodules of P. We then have*
$$(M + N)/N \cong M/(M \cap N)$$

Definition. A module M is **finitely generated** if either of the following two equivalent conditions hold:

- There exists $m_1, \ldots, m_n \in M$ such that every $m \in M$ is of the form $x_1m_1 + \cdots + x_nm_n$, with $x_i \in A$.
- There exists a surjective homomorphism $\phi\colon \bigoplus_{i=1}^{n} A \to M$.

Example.

- An abelian group is finitely generated as a group if and only if it is finitely generated as a $\mathbb{Z}$-module.

  So every finitely generated $\mathbb{Z}$-module is isomorphic to one of the form
$$\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \mathbb{Z} \oplus \mathbb{Z}/(p_1^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p_n^{e_n}),$$
  while $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.
- If k is a field, then a finitely generated k-module is the same thing as a finite-dimensional k-vector space.

- An ideal $\mathfrak{a} \subseteq A$ is finitely generated as an A-module if and only if it is finitely generated as an ideal, i.e. it is of the form $(a_1, \ldots, a_n)$.

Main ideas:

- Direct sums and products of modules
- Submodules
- Sums and intersections of modules
- "The module isomorphism theorems"
- Kernels, images and cokernels
- The "module isomorphism theorems"

6. Lecture 6 – Nakayama's lemma & exact sequences

Recall the definitions of local ring and finitely generated module.

Example. Recall $\mathbb{R}(x)$, the field of real rational functions, which is the ring of expressions f/g with $f, g \in \mathbb{R}[x]$ and $g \neq 0$ (up to some equivalence relation). Let $A \subset \mathbb{R}(x)$ be the subring of those elements which can be written as

$$\frac{f}{g} \qquad f \in \mathbb{R}[x], g \in \mathbb{R}[x] \setminus (x).$$

So e.g.

$$\frac{x^2}{x+1}, \frac{x^3-2x}{5x+4}, \frac{x^3-x}{x^2-x} = \frac{x^2-1}{x-1} \in A$$

since $x+1, 5x+4, x-1 \notin (x)$, while e.g. $\frac{1}{x} \notin A$. Equivalently, A is the ring of the real rational functions which can be evaluated at 0, since we get a well-defined real number $f(0)/g(0)$ if and only if $f/g \in A$.

Claim: The ring A is local, with maximal ideal

$$\mathfrak{m} = \{f/g \in A \mid f(0)/g(0) = 0\} = \{f/g \mid f \in (x), g \in \mathbb{R}[x] \setminus (x)\}.$$

The homomorphism $A \to \mathbb{R}$ given by $f/g \mapsto f(0)/g(0)$ is surjective, with kernel $\mathfrak{m}$, so $\mathfrak{m}$ is a maximal ideal, and $A/\mathfrak{m} \cong \mathbb{R}$.[5]

Let's now recall that given an ideal $\mathfrak{a}$ and an A-module M, the submodule $\mathfrak{a}M \subset M$ is the module containing all sums

$$a_1 m_1 + \cdots + a_n m_n, \qquad a_i \in \mathfrak{a}, m_i \in M.$$

Lemma (Nakayama's lemma, local version)**.** [6] *Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated module. If $\mathfrak{m}M = M$, then $M = 0$.*

Definition. Let $T = (b_{ij})_{1 \leq i,j \leq n}$ be an $(n \times n)$-matrix with entries in A, and let T_{ij} be the $(n \times n)$-matrix obtained by deleting row i and column j. The **adjugate** of T is the matrix $\operatorname{adj}(T) = (c_{ij})_{1 \leq i,j \leq n}$, where

$$c_{ij} = (-1)^{i+j} \det(T_{ji}).$$

Example. The adjugate of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

Theorem. *We have $T \operatorname{adj}(T) = \operatorname{adj}(T) T = \det(T) I_n$, where I_n is the $(n \times n)$ identity matrix.*

Proof of Nakayama's lemma. Let M be a module, generated by $m_1, \ldots, m_n \in M$, meaning $M = \{a_1 m_1 + \cdots + a_n m_n \mid a_i \in A\}$. We know that $\mathfrak{m}M = M$, which means that for every m_i, we have $m_i \in \mathfrak{m}M$, which means we can write

$$m_i = \sum_{j=1}^{n} b_{ij} m_j,$$

[5] To see that A is local, note that if $f/g \notin \mathfrak{m}$, then $f(0)/g(0) \neq 0$, so $g/f \in A$, and so f/g is a unit. Since all non-units are contained in $\mathfrak{m}$, this means $\mathfrak{m}$ is the unique maximal ideal.

[6] The textbook states a more general version where A is not necessarily local, where $\mathfrak{m}$ is replaced with the Jacobson radical of A.

with $b_{ij} \in \mathfrak{m}$. Letting $T = I_n - (b_{ij})$, we then get that

$$T \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} = 0,$$

and so

$$\operatorname{adj}(T) T \begin{pmatrix} m_1 \\ \cdots \\ m_n \end{pmatrix} = 0,$$

which since $\operatorname{adj}(T)T = \det(T) I_n$ gives $\det(T) m_i = 0$ for all i. But looking at the cofactor expansion of $\det(T)$ shows that

$$\det(T) = 1 + X,$$

where all the terms of X are divisible by b_{ij}, which implies that $X \in \mathfrak{m}$. Hence $\det(T)$ is a unit, and so $\det(T) m_i = 0$ implies $m_i = 0$. Thus all the $m_i = 0$, and so $M = 0$. □

Corollary. *Let A be a local ring, and let $\phi\colon M \to N$ be a homomorphism of modules, such that $\widetilde{\phi}\colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Then ϕ is surjective.*

Proof. The trick is to reinterpret "ϕ is surjective" as $\operatorname{cok} \phi = N/\phi(M) = 0$. Assume that $\widetilde{\phi}$ is surjective. That means $N = \phi(M) + \mathfrak{m}N$ (after some thought). We get

$$\mathfrak{m}(N/\phi(M)) = (\mathfrak{m}N + \phi(M)/\phi(M)) = N/\phi(M),$$

Since N is finitely generated, so is $N/\phi(M)$. We can then apply Nakayama's lemma to $N/\phi(M)$, and get $N/\phi(M) = 0$. □

Example. Work in $A \subset \mathbb{R}(x)$ from before. Consider the matrix

$$B = \begin{pmatrix} \frac{1+x^2}{1-x^2} & \frac{x^2}{1-x^3} \\ \frac{x^4}{2-5x} & \frac{1+x}{1-x} \end{pmatrix}$$

which gives a homomorphism of A-modules $\phi\colon A^{\oplus 2} \to A^{\oplus 2}$ by

$$\phi(f, g) = B \begin{pmatrix} f \\ g \end{pmatrix}.$$

The associated homomorphism of $\widetilde{\phi}\colon A^{\oplus 2}/\mathfrak{m}A^{\oplus 2} \to A^{\oplus} 2/\mathfrak{m}A^{\oplus 2}$ can be identified with the linear map $\mathbb{R}^2 \to \mathbb{R}^2$ obtained by setting $x = 0$ in the above matrix. That map is clearly surjective, hence ϕ is.

6.1. **Exact sequences and additivity.** Given $\phi\colon M \to N$ a homomorphism, we know about $\ker \phi \subset M$, $\operatorname{im} \phi \subset N$, $\operatorname{cok} \phi = N/\operatorname{im} \phi$.

Definition. A sequence of morphisms $M_1 \overset{\phi_1}{\to} M_2 \to \cdots \to M_{n-1} \overset{\phi_{n-1}}{\to} M_n$ is **exact at** M_i, $2 \le i \le n-1$, if we have

$$\operatorname{im} \phi_i = \ker \phi_{i+1}.$$

It is **exact** A sequence of the form

$$0 \to M' \to M \to M'' \to 0$$

is called **short exact**.

Example. If $M_i = 0$, then we have $\operatorname{im}\phi_i = 0$, so $\ker\phi_{i+1}$, and exactness at M_{i+1} means simply that $\ker\phi_{i+1} = 0$, i.e. that ϕ_{i+1} is surjective. We also have $\ker\phi_{i-1} = M_{i-1}$, so exactness at M_{i-1} means that $\operatorname{im}\phi_{i-2} = M_{i-1}$, i.e. that $\operatorname{im}\phi_{i-2}$ is surjective.

Example. Let $M' \subseteq M$ be a submodule. Then the sequence

$$0 \to M' \to M \to M/M' \to 0$$

is exact, since (1) $M' \to M$ is injective, (2) $M \to M/M'$ is surjective, and (3) $\ker(M \to M/M') = \operatorname{im}(M' \to M)$.

"Up to isomorphism", every short exact sequence is of this form, meaning if

$$0 \to M_1 \to M \to M_2 \to 0$$

is short exact, them M_1 is isomorphic to some submodule $M' \subset M$, and M_2 is isomorphic to M/M'.

Example. The sequence $0 \to \mathbb{Z} \xrightarrow{\phi} \mathbb{Z} \to \mathbb{Z}/(n) \to 0$ is exact, where $\phi(k) = nk$.

Example. The sequence $0 \to \mathbb{Z}/(2) \to \mathbb{Z}/(4) \to \mathbb{Z}/(2) \to 0$ is exact, where $\mathbb{Z}/(2)$ is the inclusion $1 \mapsto 2$.

Example. Let V be the $\mathbb{R}$-vector space of all smooth vector fields on $\mathbb{R}^3$, and let W be the $\mathbb{R}$-vector space of all functions on $\mathbb{R}^3$. The sequence

$$0 \to \mathbb{R} \xrightarrow{a \mapsto f(x)=a} W \xrightarrow{\nabla} V \xrightarrow{\nabla\times} V \xrightarrow{\nabla\cdot} W \to 0$$

is exact.

Example. For any modules M and N, the sequence

$$0 \to M \to M \oplus N \to N \to 0$$

is exact, where $M \to M \oplus N$ is the map $m \mapsto (m, 0)$ and $M \oplus N \to N$ is the map $(m, n) \to n$.

We can break up exact sequences into short ones, as follows: If $M_{i-1} \to M_i \to M_{i+1}$ is an exact sequence, we can take $0 \to \operatorname{im}(\phi_{i-1}) \to M_i \to \operatorname{im}(\phi_i) \to 0$ as a short exact sequence. This motivates the following definition

Definition. A function from some set of modules to an abelian group G is called **additive** if for all short exact sequences

$$0 \to M' \to M \to M'' \to 0$$

we have $\nu(M) = \nu(M') + \nu(M'')$.

Example. If M', M, M'' are finite-dimensional vector spaces, then $\dim(-)$ is additive, since we can extend a basis for M' to a basis for M, and the new elements give a basis for M'' after projection.

Example. If M', M, M'' are finite abelian groups, then $\nu(M) = |M|$, the number of elements of M, is an additive function to the group $\mathbb{Q}_{>0}$ with the operation of multiplication, since Lagrange's theorem says that for subgroups $M' \subset M$ we always have

$$|M| = |M'||M/M'|.$$

Theorem. *Let* $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ *be an exact sequence, and let* ν *be an additive function. Then*

$$\sum (-1)^i \nu(M_i) = 0$$

Proof. We have $\nu(M_i) = \nu(\operatorname{im} \phi_i) + \nu \operatorname{im}(\phi_{i-1})$. Inserting this in $\sum(-1)^i \nu(M_i)$ everything cancels to give 0. □

Example. In an exact sequence of vector spaces $0 \to V_1 \to V_2 \to \cdots \to V_n \to 0$, we have $\sum(-1)^i \dim V_i = 0$.

Example. Given an exact sequence

$$0 \to M_1 \to \cdots \to M_n \to 0$$

of finite $\mathbb{Z}$-modules, we have

$$\prod_{i=1}^{n} |M_i|^{(-1)^i} = 1.$$

Definition. A diagram of modules and homomorphisms between them is called **commutative** if the composed maps between any two modules agree.

Example. The diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle g} \\ N & \xrightarrow{h} & N' \end{array}$$

is commutative if $g \circ f = h \circ i$.

Lemma (The snake lemma)**.** *Given modules and homomorphisms that fit into the following commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0, \end{array}$$

we get an exact sequence of modules

$$0 \to \ker \phi' \to \ker \phi \to \ker \phi'' \to \operatorname{cok} \phi' \to \operatorname{cok} \phi \to \operatorname{cok} \phi'' \to 0$$

Suggested problems week 3

(1) Let A be a ring and $A[[x]]$ be the ring of power series with coefficients in A. Think of $A[[x]]$ as an A-module via the homomorphism Prove that $\prod_{i\in\mathbb{N}} A$

(2) Let $M_1, \ldots, M_n$ and N be A-modules. Prove that $\mathrm{Hom}(M_1 \oplus \cdot \oplus M_n, N)$ is isomorphic as an A-module to $\mathrm{Hom}(M_1, N) \oplus \cdots \oplus \mathrm{Hom}(M_n, N)$.

(3) Let $\{M_i\}_{i\in S}$ and N be A-modules. Prove that

$$\mathrm{Hom}(\bigoplus_{i\in S} M_i, N) \cong \prod_{i\in S} \mathrm{Hom}(M_i, N)$$

and

$$\mathrm{Hom}(N, \prod_{i\in S} M_i) \cong \prod_{i\in S} \mathrm{Hom}(N, M_i)$$

as A-modules.

(4) Let A be a ring, let $M = A \oplus A$, and let $\phi\colon M \to M$ be the homomorphism given by $\phi(x, y) = (0, x)$. Prove that the sequence

$$\cdots \xrightarrow{\phi} M \xrightarrow{\phi} M \xrightarrow{\phi} M \xrightarrow{\phi} \cdots$$

is exact.

(5) Let k be a field, let $n \geq 3$

$$0 \to V_1 \to \cdots \to V_n \to 0$$

be an exact sequence of finite-dimensional vector spaces. Prove that the homomorphism $V_{n-2} \to V_{n-1}$ is surjective if and only if $\sum_{i=1}^{n-1} (-1)^i \dim V_i = 0$.

(6) Let $A \subset \mathbb{R}(x)$ be the ring of rational functions defined at 0 as in the lecture notes, with maximal ideal $\mathfrak{m} \subset A$. Thinking of $\mathbb{R}(x)$ as an A-module, prove that $\mathbb{R}(x) = \mathfrak{m}\mathbb{R}(x)$. Why does this not contradict Nakayama's lemma?

(7) Let A be a local ring with maximal ideal $\mathfrak{m}$, let $\phi\colon N \to M$ be a homomorphism of A-modules with M finitely generated. Use the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{m}N & \longrightarrow & N & \longrightarrow & N/\mathfrak{m}N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow & & \\ 0 & \longrightarrow & \mathfrak{m}M & \longrightarrow & M & \longrightarrow & M/\mathfrak{m}M & \longrightarrow & 0, \end{array},$$

to show that if $N/\mathfrak{m}N \to M/\mathfrak{m}M$ is an isomorphism, then $\mathfrak{m}M \subseteq \phi(\mathfrak{m}N)$.

Suggested exercises week 4

From Atiyah–Macdonald Chapter 2: Problems 1, 2, 4, 5, 8, 9, 12.

(1) Let M and N be vector spaces over k, with $e_1, \ldots, e_m$ a basis for M and $f_1, \ldots f_n$ a basis for N. Prove that $M \otimes_k N$ has a basis given by

$$e_1 \otimes f_1, \ldots, e_m \otimes f_n.$$

Hint: Use the "distributive law" (Prop. 2.14 (iii)) of $\oplus$ and $\otimes$.

(2) Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Q}$ and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/(n) = 0$.

(3) An inclusion of A-modules

$$i \colon N' \to N$$

is called a **split** inclusion if there exists a homomorphism $p \colon N \to N'$ such that $p \circ i = 1_{N'}$. Prove that if M is an A-module and an inclusion i as above is split, then the homomorphism

$$i \otimes 1_M \colon N' \otimes_A M \to N \otimes_A M$$

is injective.

(4) Prove that if N is a free A-module and $i \colon N' \to N$ is injective, then i is a split inclusion.

(5) Let k be a field. Prove that every injective map of k-modules is a split inclusion, and use this to show (as we saw in the lecture) that every k-module is flat.

(6) Let A be an integral domain, and let $k(A)$ be its fraction field. Prove that if $0 \neq I \subseteq A$ is an ideal, then $A/I \otimes_A k(A) \cong 0$.

(7) Let A be an integral domain. Prove that A/I is a flat A-module if and only if $I = 0$ or $I = A$. *Hint:* Consider the injection of A-modules $A \to k(A)$.

(8) Show that the A-module $M \oplus N$ is flat if and only if both M and N are flat.

Lecture 9 – Exactness of the tensor product and algebras

Let A be a ring, let M and N be A-modules. Recall we then have a module

$$M \otimes_A N,$$

the **tensor product** of M and N over A, which has the property that for an A-module P, we have

$$\mathrm{Hom}(M \otimes_A N, P) \leftrightarrow \{A - \text{bilinear maps } M \times N \to P\}.$$

Elements of $M \otimes_A N$ are of the form

$$\sum_{i=1}^{n} x_i \otimes y_i, \qquad x_i \in M, y_i \in N.$$

These satisfy relations, for all $x, x' \in M, y, y' \in N, a \in A$, that

$$(x + x') \otimes y = x \otimes y + x' \otimes y$$
$$x \otimes (y + y') = x \otimes y + x \otimes y'$$
$$ax \otimes y = x \otimes ay$$

Two expressions $\sum x_i \otimes y_i$ and $\sum x_i' \otimes y_i'$ are equal if and only if one of them can be rewritten into the other by using these relations.

Recall also that if I is an ideal in A and M is an A-module, then

$$A/I \otimes_A M \cong M/IM,$$

where the isomorphism is given by

$$(a + I) \otimes m \mapsto am + IM$$

As a special case of $I = (0)$, we get $A \otimes_A M \cong M$.

6.2. Flat A-modules.

Proposition. *If M is an A-module and*

$$N' \to N \to N'' \to 0$$

is an exact sequence of A-modules, then the induced sequence

$$N' \otimes M \to N \otimes M \to N'' \otimes M \to 0$$

is exact.

In categorical language, this proposition says that the functor of modules $N \mapsto M \otimes_A N$ is **right exact**.

Example. Consider the $\mathbb{Z}$-module $\mathbb{Z}/(2)$, and the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/(2) \to 0.$$

We have $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \cong \mathbb{Z}/(2)$, and $\mathbb{Z}/(2) \otimes \mathbb{Z}/2 \cong \mathbb{Z}/2$. The sequence

$$\mathbb{Z} \otimes \mathbb{Z}/(2) \to \mathbb{Z} \otimes \mathbb{Z}/(2) \to \mathbb{Z}/(2) \otimes \mathbb{Z}/(2) \to 0$$

then becomes, after replacing each tensor product with its isomorphic module

$$\mathbb{Z}/(2) \xrightarrow{0} \mathbb{Z}/(2) \to \mathbb{Z}/(2) \to 0.$$

In particular, since the leftmost map is not injective, the sequence

$$0 \to \mathbb{Z}/(2) \xrightarrow{0} \mathbb{Z}/(2) \to \mathbb{Z}/(2) \to 0$$

is not exact.

To be even more concrete, note that the element $1 \otimes 1 \in \mathbb{Z} \otimes \mathbb{Z}/(2)$ is mapped to

$$2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0 \otimes 0 = 0,$$

and so lies in the kernel of $\mathbb{Z} \otimes \mathbb{Z}/2 \to \mathbb{Z} \otimes \mathbb{Z}/2$.

Definition. An A-module M is **flat** if for all injective homomorphisms $N' \to N$, the induced homomorphism $M \otimes N' \to M \otimes N$ is injective.

Remark. Equivalently, M is flat if for every short exact sequence

$$0 \to N' \to N \to N'' \to 0,$$

the sequence

$$0 \to N' \otimes M \to N \otimes M \to N'' \otimes M \to 0$$

is exact.

Example. The previous example shows that $\mathbb{Z}/(2)$ is not flat as a $\mathbb{Z}$-module.

Example. For any ring A, and A-module N, we have that $A \otimes N \cong N$. If $N' \to N$ is injective, then clearly $A \otimes N' \to A \otimes N$ is injective, so A is flat as an A-module.

Example. Given a collection of modules $\{M_i\}_{i \in S}$ and a module N, we have natural isomorphism

$$(\oplus_{i \in S} M_i) \otimes N \cong \oplus_{i \in S} M_i \otimes N.$$

Now if $N' \to N$ is injective and all the M_i are flat, then the morphism

$$\oplus_{i \in S} M_i \otimes N' \to \oplus_{i \in S} M_i \otimes N$$

is injective. This means $\oplus_{i \in S} M_i$ is also flat.

Example. If k is a field, then every k-module M is isomorphic to $\bigoplus_{i \in S} k$, which we know is flat. In other words, every k-module is flat.

Example. The $\mathbb{Z}$-module $\mathbb{Q}$ is flat, but we won't show this quite yet.

6.3. **Algebras.**

Definition. A pair (B, ϕ) of a ring B and a ring homomorphism $\phi\colon A \to B$ is called an A-**algebra**.

If (B, ϕ) and (C, ψ) are A-algebras, then a ring homomorphism $\chi\colon B \to C$ is a **homomorphism of A-algebras** if $\chi \circ \phi = \psi$.

We usually omit the homomorphism $\phi\colon A \to B$ from the notation, and just say "B is an A-algebra".

Example. For any ring A, the polynomial ring $A[x_1, \ldots, x_n]$ is naturally an A-algebra, as are all its quotients $A[x_1, \ldots, x_n]/I$.

Example. For any ring A, there is a unique ring homomorphism $\phi\colon \mathbb{Z} \to A$ given by $\phi(n) = n1_A$, so every ring is a $\mathbb{Z}$-algebra in precisely one way.

Definition. Let B be an A-algebra. We say B is a

- **finite** A-algebra if B is finitely generated as an A-module, i.e. if there exist finitely many elements $b_1, \ldots, b_n \in B$ such that every element of B can be written as

$$\sum_{i=1}^{n} a_i b_i \qquad a_i \in A, b_i \in B$$

- **finite type** A-algebra if there exist a finite set of elements $b_1, \ldots, b_n \in B$ such that every element in B can be written on the form

$$\sum_{i_j \geq 0} a_{i_1,\ldots,i_n} b_1^{i_1} \cdots b_n^{i_n}$$

Remark. An A-algebra B is of finite type if and only if it is isomorphic as an A-algebra to

$$A[x_1, \ldots, x_n]/I$$

for some ideal $I \subseteq A[x_1, \ldots, x_n]$.

Proof: If B is isomorphic as an A-algebra to $A[x_1, \cdots, x_n]/I$ via $\phi\colon A[x_1, \ldots, x_n]/I$, then we also have a surjection of A-algebras

$$\psi\colon A[x_1, \ldots, x_n] \to A[x_1, \ldots, x_n]/I \to B.$$

Taking $b_i = \psi(x_i)$, we have that every element $b \in B$ can be written

$$b = \psi(\sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}) = \sum a_{i_1,\ldots,i_n} b_1^{i_1} \cdots b_n^{i_n},$$

proving that B is finitely generated.

Conversely, if B is generated by $b_1, \ldots, b_n$, then there is a surjective A-algebra homomorphism $\phi\colon A[x_1, \ldots, x_n] \to B$ given by

$$\phi\left(\sum_{i_j \geq 0} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}\right) = \sum_{i_j \geq 0} a_{i_1,\ldots,i_n} b_1^{i_1} \cdots b_n^{i_n}$$

Remark. A finite A-algebra is finite type, but not vice versa, e.g. $A[x]$ is not a finite A-algebra.

Lecture 10 – Tensor product of algebras

Definition. Let B and C be A-algebras. The A-module $B \otimes_A C$ is an A-algebra, with multiplication defined by

$$(b \otimes c)(b' \otimes c') = bb' \otimes cc',$$

and more generally by

$$(\sum_i b_i \otimes c_i)(\sum_j b'_j \otimes c'_j) = \sum_{i,j} b_i b'_j \otimes c_i c'_j.$$

Remark. The unit element in the ring $B \otimes_A C$ is $1 \otimes 1$.

Remark. It is not obvious that this multiplication is well-defined. One way to see this is to observe that any time we rewrite the sums by using the relations

$$b \otimes (c + c') = b \otimes c + b \otimes c',$$

and

$$ab \otimes c = b \otimes ac,$$

the expression on the right hand side can also be rewritten using these relations.

The other way is to use the defining property of the tensor product, see the textbook for details.

Example. Let A be a ring, consider $B = A[x]$ and $C = A[y]$. Then, as A-modules, we have isomorphisms

$$B = \bigoplus_{i \geq 0} Ax^i, \qquad C = \bigoplus_{i \geq 0} Ay^i,$$

or in words, B (resp. C) is the free A-module generated by $1, x, x^2 \ldots$ (resp. by $1, y, y^2, \ldots$). We then find a module isomorphism

$$B \otimes_A C \cong (\bigoplus_{i \geq 0} Ax^i) \otimes (\bigoplus_{j \geq 0} Ay^j) = \bigoplus_{i,j \geq 0} Ax^i \otimes y^j.$$

For the multiplication, we have

$$(x^{i_1} \otimes y^{j_1})(x^{i_2} \otimes y^{j_2}) = (x^{i_1} x^{i_2} \otimes y^{j_1} y^{j_2}) = x^{i_1 + i_2} \otimes y^{j_1 + j_2}.$$

From this we see that there is an isomorphism of A-algebras $B \otimes_A C \to A[x, y]$, given by $\sum a_{ij} x^i \otimes y^j \mapsto \sum a_{ij} x^i y^j$.

Example. Consider $\mathbb{C}$ as an $\mathbb{R}$-algebra. We have a natural basis $1, i \in \mathbb{C}$ as an $\mathbb{R}$-module, so $\mathbb{C} \cong \mathbb{R}1 \oplus \mathbb{R}i$. We have

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = (\mathbb{R}1 \oplus \mathbb{R}i) \otimes (\mathbb{R}1 \oplus \mathbb{R}i) = (\mathbb{R}1 \otimes 1 \oplus \mathbb{R}i \otimes 1 \oplus \mathbb{R}1 \otimes i \oplus \mathbb{R}i \otimes i).$$

In other words $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is an $\mathbb{R}$-vector space with basis $1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i$. The multiplication table is easy to write down in this basis, if $x = 1 \otimes i$, $y = i \otimes 1$, $z = i \otimes i$, then we have

$$x^2 = y^2 = z^2 = -1$$

and

$$xy = z, yz = -x, zx = -y.$$

6.4. **Rings of fractions.** Recall from a previous course (hopefully), that given any integral domain A, we can produce a field $K(A)$, whose elements are written a/b, with $a, b \in A$, the **fraction field** of A.

Example. We have $K(\mathbb{Z}) = \mathbb{Q}$ and, if k is a field, $K(k[x]) = k(x)$, the field of rational functions.

Formally, the field $K(A)$ is constructed as follows

(1) Consider all pairs $(a, b) \in A \times A$ with $b \neq 0$.
(2) Declare that $(a, b) \simeq (a', b')$ if
$$ab' - ba' = 0$$
(3) Check that this is an equivalence relation.
(4) Let $k(A)$ be the set of equivalence classes of pairs $(a, b) \in A \times A$.
(5) Define addition and multiplication, check all's well defined and gives a field.

Example. It is essential that A is an integral domain, otherwise $\sim$ is not an equivalence relation. E.g. in $\mathbb{Z}/(4)$, we find
$$(2, 2) \sim (1, 1) \qquad 2 \cdot 1 - 1 \cdot 2 = 0$$
and
$$(2, 2) \sim (0, 2) \qquad 2 \cdot 2 - 0 \cdot 2 = 0$$
but
$$(1, 1) \not\sim (0, 2) \qquad 2 \cdot 1 - 1 \cdot 0 = 2 \neq 0.$$

We may think of the construction as follows: Given an integral domain A, we build a "smallest" ring $K(A)$ from A such that every non-zero element in A has an inverse.

Generalised question: Given a ring A, and $S \subseteq A$, construct a new ring $S^{-1}A$ where elements of s have inverses.

Note that, if $s_1, s_2 \in S$, and s_1 and s_2 has inverses, then also $s_1 s_2$ must have an inverse. The element $1 \in A$ already has an inverse, so we can always add it in to S. We will therefore assume S is **multiplicatively closed**, meaning $1 \in S$ and $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.

Definition. Given a ring A and a multiplicatively closed subset $S \subseteq A$, define the **ring of fractions of** A with respect to S as follows.

- The set $S^{-1}A$ are equivalence classes of pairs
$$(a, s) \qquad a \in A, s \in S,$$
under the equivalence relation that
$$(a, s) \sim (b, t)$$
if and only if there exists a $u \in S$ such that
$$(at - sb)u = 0.$$
- Addition and multiplication is defined by
$$(a, s) + (b, t) = (at + bs, st)$$
$$(a, s)(b, t) = (ab, st).$$

Remark. The proof that this is a ring is almost exactly the same as the construction of the fraction field of an integral domain.

Remark. We will always write a/s instead of (a, s). The formulas for addition and multiplication of these fractions are the same as the usual ones. The only thing that is harder is the new criterion for when two fractions are equal, i.e.

$$\frac{a}{s} = \frac{b}{t} \Leftrightarrow (at - bs)u = 0 \text{ for some } u \in S.$$

Remark. The unit element in $S^{-1}A$ is $1/1$, and the zero element is $0/1$.

Remark. There is a ring homomorphism $\phi\colon A \to S^{-1}A$ defined by $\phi(a) = \frac{a}{1}$.

Proposition. *Let $\psi\colon A \to B$ be a ring homomorphism such that every $s \in S$, we have $\psi(s)$ is a unit in B. Then there exists a unique homomorphism $\rho\colon S^{-1}A \to B$ such that $\psi = \rho \circ \phi$.*

Proof. Uniqueness: Let $a \in A$. We must have

$$\rho(a/1) = \rho(\phi(a)) = \psi(a).$$

Let $s \in S$. We must have

$$\rho(1/s) = \rho((s/1)^{-1}) = \rho(\phi(s)^{-1}) = (\rho(\phi(s)))^{-1} = \psi(s)^{-1}.$$

Then

$$\rho(a/s) = \rho(a/1)\rho(1/s) = \psi(a)\psi(s)^{-1}.$$

Existence: Define $\rho(a/s) = \psi(a)\psi(s)^{-1}$, and check that this is well-defined. □

Example. Let A be an integral domain, and let $S = A \setminus \{0\}$. Then $S^{-1}A = K(A)$. To see this, observe that the equivalence relation

$$(a, s) \sim (b, t) \Leftrightarrow (as - bt)u = 0 \text{ for some } u \in S$$

used in the construction of $S^{-1}A$, and

$$(a, s) \sim (b, t) \Leftrightarrow as - bt = 0$$

used in the construction of $K(A)$, are in fact the same ones, since A is an integral domain.

Example. Let A be a ring $S \subseteq A$ multiplicatively closed, and assume that $0 \in S$. Then we have, for all $a, b \in A$, $s, t \in S$, that

$$\frac{a}{s} = \frac{b}{t},$$

since

$$(ta - bs)0 = 0.$$

Thus $S^{-1}A$ has one element and is the zero ring.

In particular, the homomorphism $\phi\colon A \to S^{-1}A$ is not necessarily injective.

Example. Let $f \in A$, and let $S = \{f^n \mid n \geq 0\} \subseteq A$. We then write $A_f = S^{-1}A$, the ring A with f inverted.

Example. Let $\mathfrak{p} \subset A$ be a prime ideal. Let $S = A \setminus \mathfrak{p}$. Then S is multiplicatively closed, and we write $A_{\mathfrak{p}} = S^{-1}A$.

Proposition. *The ring $A_{\mathfrak{p}}$ is local, with maximal ideal*

$$\mathfrak{m} = \{a/s \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}.$$

Proof. Recall a ring A is local if and only if its non-units form an ideal, and the set of non-units are then the maximal ideal of the ring.

One checks the set above $\mathfrak{m}$ is an ideal. It does not contain $1/1$, since

$$1/1 = a/s \Rightarrow (s-a)u = 0 \text{ for some u} \notin \mathfrak{p},$$

If $a \in \mathfrak{p}$ and $s \notin \mathfrak{p}$, then $(s-a) \notin \mathfrak{p}$, and so $(s-a)u \notin \mathfrak{p}$, and in particular $(s-a)u \neq 0$. Therefore the elements of $\mathfrak{m}$ are non-units.

Assume next that $a/s \notin \mathfrak{m}$. Then $a \notin \mathfrak{p}$, so a/s has inverse s/a, and hence a/s is a unit. Thus $\mathfrak{m}$ is precisely the set of non-units in $A_{\mathfrak{p}}$, so $A_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{m}$. □

Example. Let $\mathfrak{p} = (p) \subseteq \mathbb{Z}$ for some prime number p. Then

$$\mathbb{Z}_{(p)} = \{m/n \mid p \text{ does not divide } n\},$$

and the maximal ideal is

$$\mathfrak{m} = \{pm/n \mid p \text{ does not divide } n\}.$$

Example. Take $\mathfrak{p} = (x) \subset \mathbb{R}[x]$. Then

$$\mathbb{R}[x]_{(x)} = \{f/g \mid g \notin (x)\},$$

the local ring from the lecture on Nakayama's lemma.

Suggested exercises week 5

(1) Let B be an A-algebra, and let $I \subset B$ be an ideal. Prove that if B is a finite A-algebra, then so is B/I.

(2) Let B be an A-algebra, and let $I \subset B$ be an ideal. Prove that if B is a finite type A-algebra, then so is B/I.

(3) Let A be a ring, and let $I \subseteq A$ an ideal. Prove that if A/I is a flat A-module, then $I = I^2$. *Hint:* Consider the inclusion of A-modules $I \to A$.

(4) Prove that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathbb{Q}$ as a ring.

(5) Let B be an A-algebra. Prove that

$$A[x] \otimes_A B \cong B[x]$$

(6) Let A be a ring and $I, J \subseteq A$ ideals. Prove that we have an isomorphism of A-algebras

$$A/I \otimes A/J \to A/(I+J).$$

(7) Let A be a ring, let B and C be A-algebras, with A-algebra structure given by

$$\psi_B \colon A \to B \text{ and } \psi_C \colon A \to C.$$

Let $\phi_B \colon B \to B \otimes_A C$ and $\phi_C \colon C \to B \otimes_A C$ be given by $\phi_B(b) = b \otimes 1$ and $\phi_C(c) = 1 \otimes c$. Verify that the following diagram of ring homomorphisms is commutative.

$$\begin{array}{ccc} A & \xrightarrow{\psi_B} & B \\ \downarrow{\scriptstyle \psi_C} & & \downarrow{\scriptstyle \phi_B} \\ C & \xrightarrow{\phi_C} & B \otimes_A C, \end{array}$$

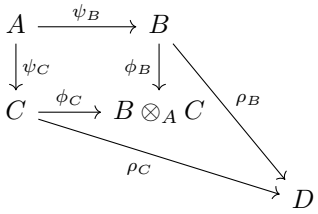
that is, that $\phi_B \circ \phi_B = \phi_C \circ \psi_C$.

(8) (*) With notation as above, let D be a ring, and let $\rho_B \colon B \to D$ and $\rho_C \colon C \to D$ be ring homomorphisms such that $\rho_B \circ \psi_B = \rho_C \circ \psi_C$. Prove that there is a unique ring homomorphism

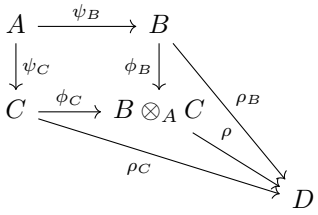
$$\rho \colon B \otimes_A C \to D$$

such that $\rho_B = \rho \circ \phi_B$ and $\rho_C = \rho \circ \phi_C$.

In diagrams: Prove that the commutative diagram of ring homomorphisms



can be extended uniquely to a commutative diagram



(9) Let $S \subseteq A$ be a multiplicatively closed subset. Show that the kernel of the homomorphism $\phi\colon A \to S^{-1}A$ is the set

$$\bigcup_{s \in S} \operatorname{Ann}(s) \subseteq A$$

(10) Let A be a ring and $f \in A$. Prove that $A[x]/(fx-1) \cong A_f$.

(11) Let A be a ring and let $S \subseteq A$ be a multiplicatively closed subset. Prove that if $S^{-1}A = 0$, then $0 \in S$.

Lecture 11 – Modules on rings of fractions

Let A be a ring and let $S \subseteq A$ be a multiplicatively closed subset.

Definition. If M is an A-module, then define an $S^{-1}A$-module $S^{-1}M$ as the set of equivalence classes of pairs

$$(m, s) \qquad m \in M, s \in S,$$

under the equivalence relation

$$(m, s) \sim (n, q) \text{ if } \exists u \in S \mid (qm - sn)u = 0.$$

The module structure is

$$(m, s) + (n, q) = (qm + sn, sq)$$

and, if $a \in A$

$$(a, s)(m, q) = (am, sq).$$

Remark. We always write m/s instead of (m, s).

Example. Take $A = \mathbb{Z}$, $S = \mathbb{Z} \setminus \{0\}$, so that $S^{-1}\mathbb{Z} = \mathbb{Q}$.

Let $M = \mathbb{Z}$, then $S^{-1}M = \mathbb{Q}$.

Let $M = \mathbb{Z}/n$, then we have the following equalities in $S^{-1}M$:

$$a/s = na/ns = 0/s = 0,$$

so $S^{-1}M = 0$.

Remark. As special notational cases:

- If $S = A \setminus \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, so that $S^{-1}A = A_{\mathfrak{p}}$, we write $M_{\mathfrak{p}}$ for $S^{-1}M$.
- If $S = \{1, f, f^2, \cdots$, so that $S^{-1}A = A_f$, we write M_f for $S^{-1}M$.

Remark. Given a homomorphism of A-modules $\phi\colon M \to N$, there is an induced homomorphism of $S^{-1}A$-modules $S^{-1}\phi\colon S^{-1}M \to S^{-1}N$ given by

$$S^{-1}\phi(m/s) = \phi(m)/s.$$

Proposition. *The $S^{-1}A$-module $S^{-1}M$ is isomorphic to $M \otimes_A S^{-1}A$, under the homomorphism ϕ given by*

$$a/s \otimes m \mapsto am/s$$

Proof. To see that ϕ is well-defined, check (which is easy) that $(a/s, m) \mapsto am/s$ is A-bilinear. The map ϕ is clearly surjective since for any $m/s \in S^{-1}M$ we have $\phi(1/s \otimes m) = m/s$. To see that it is injective, note that there is a well-defined inverse

$$\psi\colon S^{-1}M \to S^{-1}A \otimes_A M,$$

given by

$$\psi(m/s) = 1/s \otimes m.$$

Here if $m/s = n/q$, we have an $u \in S$ such that $u(qm - sn) = 0$, which implies that

$$1/s \otimes m = 1/uqs \otimes uqm = 1/uqs \otimes usn = 1/q \otimes n,$$

so ψ is well-defined. One checks that it is a homomorphism of $S^{-1}A$-modules, and that $\psi \circ \phi$ and $\phi \circ \psi$ are both the identities. $\square$

Example. In the examples above, $S^{-1}M = \mathbb{Q} \otimes_{\mathbb{Z}} M$, so our computations recover previous computations of these tensor products.

Proposition. *If $M' \to M \to M''$ is exact, then so is $S^{-1}M' \to S^{-1}M \to S^{-1}M''$.*

Proof. Let m/s be such that $S^{-1}\psi(m/s) = 0$. We must show that there exists an m'/s' such that $S^{-1}\phi(m'/s') = m/s$.

We have

$$S^{-1}\psi(m/s) = \psi(m)/s = 0/1,$$

which by definition means that there is an $u \in S$ such that $u\psi(m) = 0$.

Then $\psi(um) = 0$, and exactness implies there is an n such that $\phi(n) = um$. It follows that

$$S^{-1}\phi(n/su) = \phi(n)/su = um/su = m/s.$$

□

Corollary. *The ring $S^{-1}A$ is flat as an A-module.*

Proof. The operation $S^{-1}-$ preserves exactness, and so preserves injections, hence the operation $S^{-1} \otimes_A -$ preserives injections, which by definition means that $S^{-1}A$ is flat. □

Example. For any integral domain A, $K(A)$ is flat as an A-module.

Proposition (The operation $M \mapsto S^{-1}M$ commutes with everything)**.** *Let M be an A-module.*

- *If M' is an A-submodule of M, then $S^{-1}M'$ is an $S^{-1}A$-submodule of $S^{-1}M$, and we have $S^{-1}M/S^{-1}M' \cong S^{-1}(M/M')$.*
- *If $M', M'' \subset M$, then $S^{-1}(M' + M'') = S^{-1}M' + S^{-1}M''$, and $S^{-1}M' \cap S^{-1}M'' = S^{-1}(M' \cap M'')$.*
- *If N is an A-module, then*

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N).$$

Proof. Let's only prove the last one. We use the $S^{-1}A \otimes_A M = S^{-1}M$ to rewrite the left hand side as

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\cong M \otimes_A S^{-1}A \otimes_{S^{-1}A} S^{-1}A \otimes_A N \\ &\cong M \otimes_A S^{-1}A \otimes_A N \cong S^{-1}A \otimes_A M \otimes_A N \cong S^{-1}(M \otimes_A N). \end{aligned}$$

□

Remark. All of the above hold more generally for the operation $M \mapsto M \otimes_A B$ whenever B is a flat A-algebra.

6.5. **Local properties.** Let P be a property of module. We say (somewhat informally) that the property P is **local** if

$$\begin{array}{c} P \text{ holds for } M \\ \Updownarrow \\ P \text{ holds for all localisations } M_{\mathfrak{p}}. \end{array}$$

Proposition ("Being 0 is local")**.** *Let M be an A-module. The following are equivalent*

(1) $M = 0$

(2) $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p}$
(3) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are obvious.

To prove (3) $\Rightarrow$ (1), assume $M \neq 0$, and for a contradiction that $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$. Let $0 \neq m \in M$. Then

$$\operatorname{Ann}(m) = \{x \in A \mid xm = 0\} \subset A$$

is an ideal, and $\operatorname{Ann}(m) \neq (1)$. Hence there is a maximal ideal $\mathfrak{m} \supseteq \operatorname{Ann}(m)$. Now, since $M_{\mathfrak{m}} = 0$, we have

$$\frac{m}{1} = 0 \Leftrightarrow \exists u \in A \setminus \mathfrak{m} \mid um = 0,$$

but $\operatorname{Ann}(m) \subseteq \mathfrak{m}$, so this is a contradiction. □

Proposition. *Let* $\phi\colon M \to N$ *be a homomorphism of* A*-modules. Then the following are equivalent:*

(1) ϕ *is injective.*
(2) *For all prime ideals* $\mathfrak{p}$*, the map* $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective.*
(3) *For all maximal ideals* $\mathfrak{m}$*, the map* $\phi_{\mathfrak{p}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective.*

Proof. The sequence $0 \to \ker\phi \to M \to N$ is exact. Since localisation is exact, we have for every prime $\mathfrak{p}$ that

$$0 \to (\ker\phi)_{\mathfrak{p}} \to M_{\mathfrak{p}} \xrightarrow{\phi_{\mathfrak{p}}} N_{\mathfrak{p}}$$

is exact. But that implies $(\ker\phi)_{\mathfrak{p}} \cong \ker\phi_{\mathfrak{p}}$.

We have ϕ injective if and only if $\ker\phi = 0$. By the above, we have $\phi_{\mathfrak{p}}$ injective if and only if $(\ker\phi)_{\mathfrak{p}} = 0$. Combining with the previous proposition gives what we want. □

Remark. The same result holds with "injective" replaced by "surjective" throughout.

Proposition. *Being flat is a local property.*

7. Lecture 12 – Extension and contraction of ideals in the ring of fractions

Recall that for a quotient ring A/I, we have a bijection between the set of ideals of A/I and the set of ideals of A containing I. If $\phi\colon A \to A/I$, and superscripts e and c denote extension and contraction along ϕ, the correspondence is given by

$$\mathfrak{a} \subseteq A \mapsto \mathfrak{a}^e = \mathfrak{a}/I \subseteq A/I$$

and

$$\mathfrak{a} \subseteq A/I \mapsto \mathfrak{a}^c = \phi^{-1}(\mathfrak{a}) \subseteq A.$$

A similar, but more complicated story, holds for the fractions rings $S^{-1}A$. Recall that given a multiplicatively closed subset $S \subseteq A$, we have a homomorphism $\phi\colon A \to S^{-1}A$, and we let now let superscripts c and e denote contraction and extension along this homomorphism. We begin by analysing concretely what these operations do.

Lemma. *Let $\mathfrak{a} \subset A$ be an ideal. Then*

$$\mathfrak{a}^e = \{\frac{a}{s} \mid a \in \mathfrak{a}\}$$

Proof. By definition, $\mathfrak{a}^e = \{\sum b_i/s_i\phi(a_i) \mid b_i \in A, s_i \in S, a_i \in \mathfrak{a}\}$, where we look at all finite sums. The inclusion $\supseteq$ is then clear. Conversely, $\mathfrak{a}^e$ is generated by elements of the form

$$\frac{b}{s}\phi(a) = \frac{ba}{s},$$

with $a \in \mathfrak{a}$. Then $ba \in \mathfrak{a}$, which gives the inclusion $\subseteq$. □

Lemma. *Let $\mathfrak{a} \subseteq S^{-1}A$ be an ideal. Then $\mathfrak{a}^c = \{a \in A \mid a/1 \in \mathfrak{a}\}$.*

Proof. $a \in \mathfrak{a}^c \Leftrightarrow \phi(a) \in \mathfrak{a}$ by definition, and $\phi(a) = a/1$. □

Proposition. *For any ideal $\mathfrak{a} \subset S^{-1}A$, we have $\mathfrak{a}^{ce} = \mathfrak{a}$.*

Proof. Using the lemmas above, we find

$$a/s \in \mathfrak{a} \Rightarrow (s/1)(a/s) = a/1 \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}^c \Rightarrow a/s \in \mathfrak{a}^{ce},$$

and

$$a/s \in \mathfrak{a}^{ce} \Rightarrow a/s = b/q, b \in \mathfrak{a}^c \Rightarrow b/1 \in \mathfrak{a} \rightarrow (1/q)(b/1) = b/q = a/s \in \mathfrak{a}.$$

□

Corollary. *The operation $\mathfrak{a} \to \mathfrak{a}^c$ gives an inclusion of the set of ideals of $S^{-1}A$ into the set of ideals of A.*

Proof. If $\mathfrak{a}^c = \mathfrak{b}^c$, then $\mathfrak{a} = \mathfrak{a}^{ce} = \mathfrak{b}^{ce} = \mathfrak{b}$. □

Corollary. *Every ideal of $S^{-1}A$ is of the form $\mathfrak{a}^e$ for some $\mathfrak{a} \subseteq A$.*

Example. The ideals of $\mathbb{Z}_{(2)}$ are all extensions of ideals from $\mathbb{Z}$. Every ideal of $\mathbb{Z}$ is of the form (n) for some $n \geq 0$, and we have

$$(n)^e = \{\frac{nk}{s} \mid k \in \mathbb{Z}, s \notin (2)\} = (n/1)$$

If $n = 2^f q$ with q odd, then $2^f/1 = n/q \in (n/1)$, so $(2^f/1) \subseteq (n/1)$, while $n/1 = (2^f/1)(q/1) \in (2^f/1)$, so $(n/1) \subseteq (2^f/1)$. It follows that $(n/1) = (2^f/1)$. Thus the complete set of ideals in $\mathbb{Z}_{(2)}$ is

$$(1) \supsetneq (2/1) \supsetneq (2^2/1) \supsetneq \cdots$$

and (0).

Let's focus now on the case of prime ideals.

Proposition. *The operations of extension and contraction give a bijection between the prime ideals of $S^{-1}A$ and the prime ideals $\mathfrak{p}$ of A such that $\mathfrak{p} \cap S = \varnothing$.*

Proof. Let $\mathfrak{p} \subset S^{-1}A$ be a prime ideal. Then $\mathfrak{p}^c \subset A$ is a prime ideal (*Contraction always preserves prime ideals*). Moreover, $\mathfrak{p}^c \cap S = \varnothing$, since if $a \in \mathfrak{p}^c \cap S$, then

$$a/1 \in \mathfrak{p} \Rightarrow a/a = 1 \in \mathfrak{p} \Rightarrow \mathfrak{p} = (1),$$

contradicting primality of $\mathfrak{p}$.

If $\mathfrak{q} \subset A$ is a prime ideal with $\mathfrak{q} \cap S = \varnothing$, then we claim (1) $\mathfrak{q}^e$ is a prime ideal, and (2) $\mathfrak{q}^{ec} = \mathfrak{q}$.

For (1), if $\mathfrak{q}^e$ is not a prime ideal, we can find $a/s, b/q$ such that $a, b \notin \mathfrak{q}$ with

$$\frac{ab}{qs} = \frac{c}{t},$$

with $c \in \mathfrak{q}$. That implies $(abt - qsc)u = 0$ for some $u \in S$, but $a, b, t \notin \mathfrak{q}, c \in \mathfrak{q}$ and $u \notin \mathfrak{q}$ makes this impossible, since $\mathfrak{q}$ is prime.

For (2), $\mathfrak{q}^{ec} \supseteq \mathfrak{q}$ always holds, so we only need to prove that $\mathfrak{q}^{ec} \subseteq \mathfrak{q}$. An element of $\mathfrak{q}^{ec}$ is an $a \in A$ such that

$$a/1 = b/s$$

with $b \in \mathfrak{q}$ and $s \in S$. This implies that $(as - b)u = 0$ for some $u \in S$, which since $b \in \mathfrak{q}$, $s, u \notin \mathfrak{q}$, can only happen if $a \in \mathfrak{q}$.

We have now shown that the operations $(-)^e$ and $(-)^c$ gives maps between the sets

$$\{\text{prime ideals in } A \text{ not intersecting } S\}$$

and

$$\{\text{prime ideals in } S^{-1}A\},$$

such that $\mathfrak{p}^{ec} = \mathfrak{p}$ and $\mathfrak{q}^{ce} = \mathfrak{q}$, which means that these maps are bijections. □

Corollary. *Let $\mathfrak{p} \subseteq A$ be a prime ideal. The prime ideals of $A_\mathfrak{p}$ are precisely the ideals $\mathfrak{q}^e$, where $\mathfrak{q} \subseteq \mathfrak{p}$ is a prime ideal.*

Proof. The condition $\mathfrak{q} \cap S \setminus \mathfrak{p}$ is equivalent to $\mathfrak{q} \subseteq \mathfrak{p}$. □

Example. The prime ideals of $\mathbb{Z}_{(2)}$ are exactly $(2)^e = (2/1)$ and $(0)^e = (0/1)$.

Note that the bijection proposition above fails here for non-prime ideals, i.e. $(6) \subset (2) \subset \mathbb{Z}$, but $(6)^e = (2)^e = (2/1)$, and there is no ideal $I \subseteq \mathbb{Z}_{(2)}$ such that $I^c = (6)$.

Corollary. *Let $f \in A$. The prime ideals of A_f are precisely the ideals $\mathfrak{q}^e$, where $\mathfrak{q} \subset A$ is a prime ideal not containing f.*

Proof. Since $A_f = S^{-1}A$ with $S = \{f^k\}_{k \geq 0}$, the prime ideals of A_f are the $\mathfrak{q}^c$ which don't intersect S. Now $f \in \mathfrak{q} \Leftrightarrow f^k$ for some $k \geq 0$ by primality of $\mathfrak{q}$, so this is the set of prime ideals in A which don't contain f. □

Example. The prime ideals of $\mathbb{Z}_2$ are $(3/1), (5/1), (7/1), (11/1), \ldots$.

We can give better proofs of a few things we've seen before.

Corollary. *The ring $A_{\mathfrak{p}}$ is local.*

Proof. Every prime ideal $\mathfrak{q} \subset A_{\mathfrak{p}}$ is contained in $\mathfrak{p}^e$. □

Proposition. *The nilradical of A is the intersection of all the prime ideals of A.*

Proof. If f is nilpotent, then it must lie in every prime ideal. The hard part is to see that if f lies in every prime ideal, then f is nilpotent. Consider the ring A_f. A ring without prime ideals must be the zero ring, and $S^{-1}A$ is the zero ring if and only if $0 \in S$, which is if and only if f is nilpotent. □

Geometric interlude

Let k be an algebraically closed field, and for concreteness we may as well take $k = \mathbb{C}$. We are interested in the ring $k[x_1, \dots, x_n]$, and want to know what its maximal ideals are. There is a very natural source of such maximal ideals: Let $(a_1, \dots, a_n) \in k^n$, and let

$$\phi_{(a_1,\dots,a_n)} \colon k[x_1, \dots, x_n] \to k$$

be given by

$$\phi_{(a_1,\dots,a_n)}(f) = f(a_1, \dots, a_n).$$

This homomorphism is surjective onto k, so $k = \operatorname{im} \phi = k[x_1, \dots, x_n]/\ker \phi$, which means that $\ker \phi$ is maximal. It's easy to check that $\ker \phi = (x_1 - a_1, \dots, x_n - a_n)$.

We will see later the following theorem:

Theorem (Nullstellensatz (special case))**.** *The maximal ideals of the ring $k[x_1, \dots, x_n]$ are precisely the ideals*

$$(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n),$$

where $(a_1, a_2, \dots, a_n) \in k^n$.

We are in principle interested in subsets of k^n defined as the zero sets of polynomials $f_1, f_2, \dots, f_m \in k[x_1, \dots, x_n]$. We write

$$V(f_1, \dots, f_m) = \{(a_1, \dots, a_n) \in k^n \mid f_1(a_1, \dots, a_n) = \cdots = f_m(a_1, \dots, a_n) = 0\}.$$

A set $V \subseteq k^n$ which can be expressed in this form is called **algebraic**.

Example. The set $\{(a_1, a_2) \mid a_1^2 + a_2^2 = 1\} \subseteq k^2$ is an algebraic subset (which if $k = \mathbb{R}$ is of course a circle).

Lemma. *Let $f \in k[x_1, \dots, x_n]$. Then $f(a_1, \dots, a_n) = 0$ if and only if $f \in (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. $f(a_i) = 0 \Leftrightarrow f \in \ker \phi_{(a_i)} \Leftrightarrow f \in (x_i - a_i)$. □

Lemma. *Given $f_1, \dots, f_n \in k[x_1, \dots, x_n]$, we have that $(a_1, \dots, a_n) \subseteq V(f_1, \dots, f_n)$ if and only if $(f_1, \dots, f_n) \subseteq (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. By definition, we have $V(f_1, \dots, f_n) = V(f_1) \cap V(f_2) \cap \cdots V(f_n)$. □

Corollary. *The set $V(f_1, \dots, f_n)$ are in natural bijection with the maximal ideals of the ring $k[x_1, \dots, x_n]/(f_1, \dots, f_n)$.*

Proof. The maximal ideals of the quotient ring are in bijection with the maximal ideals of $k[x_1, \dots, x_n]$ containing $(f_1, \dots, f_n)$, which is in bijection with $V(f_1, \dots, f_n)$. □

Example. To find the maximal ideals of the ring $A = k[x, y]/(x^2 + y^2 - 1, x)$, we simply solve the set of equation

$$x^2 + y^2 - 1 = 0$$
$$x = 0,$$

giving $(x, y) = (0, 1)$ and $(x, y) = (0, -1)$. This means that A has two maximal ideals. Letting $\bar{x} = x + (x^2 + y^2 - 1), \bar{y} = y + (x^2 + y^2 - 1, x) \in A$, the maximal ideals of A are

$$(\bar{x}, \bar{y} - 1) \text{ and } (\bar{x}, \bar{y} + 1).$$

Motivated by this, for any ideal $I \subseteq k[x_1, \ldots, x_n]$, we define $V(I) \subseteq k^n$ to be the subset $(a_1, \ldots, a_n)$ such that $I \subseteq (x_1 - a_1, \ldots, x_n - a_n)$. Sets of the form $V(I)$ are called **algebraic subsets** of k^n.

Proposition. *The operation $I \mapsto V(I)$ satisfies the following properties*

(1) $I \subseteq J \Rightarrow V(J) \subseteq V(I)$.
(2) $V(0) = k^n$
(3) $V(1) = \varnothing$.
(4) $V(I + J) = V(I) \cap V(J)$.
(5) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.
(6) $V(\mathfrak{r}(I)) = V(I)$.

Proof. (1), (2) and (3) are obvious.

(4): A maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$ contains I and J if and only if it contains $I + J$.

(5): From $IJ \subseteq I \cap J$ and (1) follows $V(IJ) \supseteq V(I \cap J)$. If a maximal ideal contains I or J, then it contains $I \cap J$, which gives $V(I \cap J) \supseteq V(I) \cap V(J)$. If a maximal ideal $\mathfrak{m}$ contains I, J, then it contains either I or J, since otherwise we can find $f \in I \setminus \mathfrak{m}$, $g \in J \setminus \mathfrak{m}$, from which we get $fg \in IJ \setminus \mathfrak{m}$, since $\mathfrak{m}$ is prime. It follows that $V(I) \cap V(J) \supseteq V(IJ)$.

(6): From (1) and $I \subseteq \mathfrak{r}(I)$ we get $V(\mathfrak{r}(I)) \subseteq V(I)$. If a maximal ideal $\mathfrak{m}$ contains I, then it also contains $\mathfrak{r}(I)$, since $f^n \in I \Rightarrow f^n \in \mathfrak{m} \Rightarrow f \in \mathfrak{m}$. Hence $V(\mathfrak{r}(I)) \supseteq V(I)$. □

Let now $V = V(I) \subseteq k^n$ be an algebraic subset. We say that V is **irreducible** if there is no way to write $V(I)$ as the union of two strictly smaller algebraic subsets.

Example. For every maximal $\mathfrak{m}$, we have $V(\mathfrak{m})$, so points are irreducible.

Proposition. *If $\mathfrak{p} \subset k[x_1, \ldots, x_n]$ is a prime ideal, then $V(\mathfrak{p})$ is an irreducible subset.*

Moreover, every irreducible algebraic subset of k^n is of the form $V(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$.

Proof. These claims rely on the Nullstellensatz, which we don't know yet, so we won't prove this. □

Example. For every irreducible $f \in k[x_1, \ldots, x_n]$, the set

$$V(f) = \{(a_1, \ldots, a_n) \mid f(a_1, \ldots, a_n) = 0\}$$

is irreducible, since (f) is a prime ideal.

Example. The fact that $xy \in k[x, y]$ is not irreducible is equivalent to (xy) not being a prime ideal, which is equivalent to $V(xy)$ not being irreducible. Concretely, $V(xy) = V(x) \cup V(y)$ shows that $V(xy)$ is not irreducible.

Suggested problems week 6

(1) Let $\mathfrak{a} \subseteq A$ be an ideal, and let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{a}$ is not contained in $\mathfrak{p}$. Prove that $(A/\mathfrak{a})_\mathfrak{p} = 0$ and that $\mathfrak{a}_\mathfrak{p} \cong A_\mathfrak{p}$ as $A_\mathfrak{p}$-modules.

(2) An A-module is **torsion free** if the map $\phi_a \colon M \to M$ given by $\phi_a(m) = am$ is injective for all $a \neq 0$. Prove that the property of being torsion free is local.

(3) Show that "being finitely generated" is not a local property of A-modules, i.e. give an example of a ring A and a module M such that all localisations $M_\mathfrak{p}$ are finitely generated $A_\mathfrak{p}$-modules, but M is not a finitely generated A-module.

(4) Prove that the operation $M \mapsto S^{-1}M$ does not commute with infinite intersections of submodules. More precisely, give an example of a ring A, a multiplicatively closed subset $S \subseteq A$, an A-module M, and an infinite set of submodules $\{M_i\}_{i \in T}$ of M such that

$$\bigcap_{i \in T} S^{-1}M_i \neq S^{-1}(\bigcap_{i \in T} M_i).$$

Lecture 13 – Primary ideals

Some rings, such as $\mathbb{Z}$ and $k[x_1, \ldots, x_n]$ where k is a field, are **unique factorisation domains**, meaning every element x can be factored uniquely (up to reordering and multiplication by units) as a product

$$x = p_1 p_2 \cdots p_k$$

with p_i irreducible ring elements.

For most rings A, this is not the case:

Example.
- In $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z}[x]/(x^2+5)$, we have $6 = 2\cdot 3 = (1+i\sqrt{5})(1-\sqrt{5})$, where $2, 3, 1+i\sqrt{5}$ and $1-i\sqrt{5}$ are all irreducible.
- Let k be a field. In the ring $A = k[x,y]/(y^2 - x^3 + x)$, we have

  $$y^2 = y \cdot y = x(x-1)(x+1),$$

  and y, x, $(x-1)$, $(x+1)$ are all irreducible.

The best we can hope for in general is some kind of factorisation of *ideals*. A reasonable way to formalise this turns out to be that of factoring into **primary ideals**.

Definition. An ideal $\mathfrak{a} \subseteq A$ is primary if $\mathfrak{a} \neq (1)$, and $fg \in \mathfrak{a}$ implies either $f \in \mathfrak{a}$ or $g^n \in \mathfrak{a}$ for some $n \geq 1$.

Remark. An equivalent formulation is: An ideal $\mathfrak{a}$ is primary if $A/\mathfrak{a} \neq 0$, and every 0-divisor in $A/\mathfrak{a}$ is nilpotent.

Example. Every prime ideal is primary.

Example. In $\mathbb{Z}$, the primary ideals are (0) and (p^i) for p a prime.

Example. If a ring A has unique factorisation, then (x^n) is primary for any irreducible x. Here $fg \in (x^n)$ is equivalent to "x^n divides fg". If x divides g, then $g^n \in (x^n)$, and if not, we must have that x^n divides f.

Proposition. *If $\mathfrak{a}$ is primary, then $\sqrt{\mathfrak{a}}$ is prime.*

Proof. Assume $fg \in \sqrt{\mathfrak{a}}$. Then there's some n such that $f^n g^n \in \mathfrak{a}$, so that either $f^n \in \mathfrak{a}$, or there's some m such that $(g^n)^m \in \mathfrak{a}$. In either case one of f and g must lie in $\sqrt{\mathfrak{a}}$, so $\sqrt{\mathfrak{a}}$ is prime. □

We say that $\mathfrak{a}$ is $\mathfrak{p}$-primary if $\sqrt{\mathfrak{a}} = \mathfrak{p}$.

Remark. Let $\mathfrak{a} = (xy, y^2)$. Then $\sqrt{\mathfrak{a}} = (y)$, which is prime, but $\mathfrak{a}$ is not primary, since $yx \in \mathfrak{a}$, but $x \notin \sqrt{\mathfrak{a}}$. So being primary is a stronger condition than having prime radical.

Proposition. *If $\mathfrak{m} \subset A$ is maximal, and $\sqrt{\mathfrak{a}} = \mathfrak{m}$, then $\mathfrak{a}$ is primary.*

Proof. The ring $A/\mathfrak{a}$ has the property that the nilradical $\sqrt{(0)} = \mathfrak{m}/\mathfrak{a}$ is a maximal ideal. Since the nilradical is the intersection of all prime ideals, we must have that $\mathfrak{m}/\mathfrak{a}$ is the unique prime ideal of $A/\mathfrak{a}$. Every element outside of $\mathfrak{m}/\mathfrak{a}$ is then a unit, so every 0-divisor lies in $\mathfrak{m}/\mathfrak{a} = \sqrt{(0)}$, which means $\mathfrak{a}$ is primary. □

Definition. A **primary decomposition** of an ideal $\mathfrak{a} \subseteq A$ is an expression

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

with the $\mathfrak{q}_i$ primary. It is said to be minimal if the $\sqrt{\mathfrak{q}_i}$ are distinct, and if there is no i such that

$$\mathfrak{q}_i \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n.$$

Remark. A nonminimal primary decomposition easily gives a minimal one. If $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}_j}$, just replace $\mathfrak{q}_i$ and $\mathfrak{q}_j$ by $\mathfrak{q}_i \cap \mathfrak{q}_j$, which is primary by the lemma below.

If

$$\mathfrak{q}_i \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n,$$

just remove $\mathfrak{q}_i$.

Lemma. *If $\mathfrak{q}, \mathfrak{q}'$ are $\mathfrak{p}$-primary, then so is $\mathfrak{q} \cap \mathfrak{q}'$.*

There are two natural questions to ask of these primary decompositions

(1) Do they exist, i.e. does every ideal have such a decomposition?
(2) Are they unique?

The answers are

(1) No in general, but for "Noetherian rings", then yes. In particular the answer is yes for all rings of the form $k[x_1, \ldots, x_n]/I$ and $\mathbb{Z}[x_1, \ldots, x_n]/I$. We'll prove this later.
(2) No in general, but certain aspects are preserved.

Example. In the ring $\mathbb{Z}[i\sqrt{5}]$, one can check that (6) is written as an intersection

$$(6) = (2) \cap (3, 1 - i\sqrt{5}) \cap (3, 1 + i\sqrt{5})$$

The ideal (2) is $(2, 1 - i\sqrt{5})$-primary, and $(3, 1 \pm i\sqrt{5})$ are prime ideals. The ideals involved are coprime, so we also have

$$(6) = (2)(3, 1 - i\sqrt{5})(3, 1 + i\sqrt{5}).$$

This decomposition is (we'll see) unique.

Example. The ideal $(xy) \subseteq k[x, y]$ admits a minimal primary decomposition $(xy) = (x) \cap (y)$, which is also unique.

Example. Let's compute a primary decomposition of $(xy, y^2) \subset k[x, y]$. Firstly, note that (xy, y^2) is not primary, since $yx \in (xy, y^2)$, but $y \notin (xy, y^2)$ and no power of x lies in (xy, y^2).

A reasonable candidate for one primary ideal is (y), which is a prime ideal, and clearly $(xy, y^2) \subseteq (y)$. A second possible ideal is $(x^2, xy, y^2) = (x, y)^2$. This is (x, y)-primary since (x, y) is maximal.

Now to see

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

note that

$$(xy, y^2) = \{\sum a_{ij} x^i y^j \mid a_{i0} = 0 \text{ and } a_{01} = 0\}$$

while

$$(y) = \{\sum a_{ij} x^i y^j \mid a_{i0} = 0\}$$

and

$$(x^2, xy, y^2) = \{\sum a_{ij}x^i y^j \mid a_{00} = a_{10} = a_{01} = 0\}.$$

This is a minimal primary decomposition since $(y) \neq (x, y)$ and neither of the ideals (y) and (x^2, xy, y^2) are contained in the other.

In this case, the primary decomposition is *not* unique, in particular we can also write

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

for any $n \geq 1$, or

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

for any $a \in k$.

Recall $(\mathfrak{a} : x) = \{y \in A \mid yx \in \mathfrak{a}\}$.

Theorem (Uniqueness 1)**.** *Let $\mathfrak{a}$ be a decomposable ideal, with minimal decomposition*

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

The prime ideals $\sqrt{\mathfrak{q}_i}$ are precisely the prime ideals which can be written as $\sqrt{(\mathfrak{a} : x)}$.

Corollary. *Every minimal primary decomposition of $\mathfrak{a}$ gives the same set of prime ideals.*

Definition. The ideals of the form $\sqrt{\mathfrak{q}_i}$ are the prime ideals **associated with** $\mathfrak{a}$.

Suggested problems week 7

From Atiyah–Macdonald chapter 4, problems 2 (assume $\mathfrak{a}$ is decomposable), 4, 5.

(1) Let $A = \mathbb{Z}[x]/(x^2+5)$.
   (a) Let p be a prime. Show that the ideal $(p) \subseteq A$ is a prime ideal if and only if the congruence equation $t^2 + 5 \equiv 0 \pmod{p}$ has no solutions.
   (b) Prove that (2) is a primary ideal in A.
   (c) Prove that $(3) = (3, x-1) \cap (3, x+1)$ is a minimal primary decomposition of (3).
   (d) Compute the primary decomposition of (6) as given in the lecture notes.

(2) An integral domain has dimension 1 if it is not a field and every non-zero prime ideal is maximal.
   (a) Prove that $\mathbb{Z}$ and $k[x]$ have dimension 1.
   (b) For the rest of the problem, let A be an integral domain of dimension 1. Prove that an ideal $\mathfrak{a} \subseteq A$ is primary if and only if $\sqrt{\mathfrak{a}}$ is prime.
   (c) Let $\mathfrak{q}, \mathfrak{q}'$ be non-zero primary ideals with different radicals. Prove that $\mathfrak{q}$ and $\mathfrak{q}'$ are coprime.
   (d) Prove that if $\mathfrak{a} \subseteq A$ admits a primary decomposition, then it admits a product decomposition
   $$\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_n,$$
   with each $\mathfrak{q}_i$ primary.
   (e) With $\mathfrak{a}$ as above, prove that every prime associated with $\mathfrak{a}$ is minimal.

(3) (*) Let $A = k[x,y]/(y^2 - x^3 + x)$. We want to prove that y, x, $x-1$, $x+1 \in A$ are irreducible, to show that A does not have unique factorisation.
   (a) Prove that every $f \in A$ can be expressed uniquely as
   $$f = g_0 + y g_1 \qquad g_i \in k[x].$$
   (b) Prove that the map $\phi\colon A \to k[x]$ defined by
   $$\phi(g_0 + y g_1) = g_0^2 - (x^3 - x) g_1^2$$
   is multiplicative, that is
   $$\phi(f f') = \phi(f)\phi(f')$$
   for all $f, f' \in A$.
   (c) Prove that for any $g_0, g_1 \in k[x]$, we have
   $$\deg \phi(g_0 + y g_1) \neq 1.$$
   (d) Prove that if $\deg(g_0 + y g_1) = 0$, then $g_0 + y g_1$ is a unit in A.
   (e) Prove that if $y = f f'$, then either f or f' is a unit.
   (f) Prove the same thing for x, $x-1$ and $x+1$ instead of y.

Lecture 14 – Primary ideals II

Recall $(\mathfrak{a} : x) = \{y \in A \mid yx \in \mathfrak{a}\}$.

Theorem (Uniqueness 1)**.** *Let $\mathfrak{a}$ be a decomposable ideal, with minimal decomposition*

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

The prime ideals $\sqrt{\mathfrak{q}_i}$ are precisely the prime ideals which can be written as $\sqrt{(\mathfrak{a} : x)}$.

Corollary. *Every minimal primary decomposition of $\mathfrak{a}$ gives the same set of prime ideals.*

Definition. The ideals of the form $\sqrt{\mathfrak{q}_i}$ are the prime ideals **associated with** $\mathfrak{a}$.

Proof of Uniqueness theorem. The proof requires two reasonably simple lemmas.

Lemma (AM, Prop. 1.11)**.** *If $\mathfrak{p}$ is a prime ideal, and $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n \subset A$ are prime ideals such that*

$$\mathfrak{p} \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n,$$

then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i. If moreover

$$\mathfrak{p} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n,$$

then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

To motivate the second one, note that if

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i,$$

then

$$\sqrt{(\mathfrak{a} : x)} = \sqrt{(\cap \mathfrak{q}_i : x)} = \sqrt{\cap (\mathfrak{q}_i : x)} = \bigcap_{i=1}^{n} \sqrt{(\mathfrak{q}_i : x)},$$

so we need to analyse $(\mathfrak{q}_i : x)$.

Lemma. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then*

$$\sqrt{(\mathfrak{q} : x)} = \begin{cases} \mathfrak{p} & \text{if } x \notin \mathfrak{q} \\ (1) & \text{if } x \in \mathfrak{q} \end{cases}$$

Proof. If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = (1)$.

If $x \notin \mathfrak{q}$ and $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$. Since $\mathfrak{q}$ is primary, this implies that $y^n \in \mathfrak{q}$ for some n, so $y \in \mathfrak{p}$. Conversely, if $x \notin \mathfrak{q}$ and $y \in \mathfrak{p}$, then for some $n \geq 1$ we have

$$y^n \in \mathfrak{q} \Rightarrow xy^n \in \mathfrak{q} \Rightarrow y^n \in (\mathfrak{q} : x) \Rightarrow y \in \sqrt{(\mathfrak{q} : x)}.$$

□

Now to prove the Uniquness theorem, assume that $\mathfrak{a} = \cap \mathfrak{q}_i$ is a minimal primary decomposition and that $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Now assume that $\mathfrak{p} = \sqrt{\mathfrak{a} : x)}$ is a prime ideal – we must show that $\mathfrak{p} = \mathfrak{p}_i$ for some i. We have, using Lemma 2, that

$$\mathfrak{p} = \bigcap_{i=1}^{n} \sqrt{(\mathfrak{q}_i : x)} = \mathfrak{p}_{i_1} \cap \mathfrak{p}_{i_2} \cap \cdots \cap \mathfrak{p}_{i_k},$$

where the set $\{i_1, \ldots, i_k\}$ is the set of i for which $x \notin \mathfrak{q}_i$. Using Lemma 1, then $\mathfrak{p} = \mathfrak{p}_{i_j}$ for some j.

We must also show that for every prime ideal $\mathfrak{p}_i$, we can find an $x \in A$ such that $\mathfrak{p}_i = \sqrt{(\mathfrak{a} : x)}$. Taking $x \in \mathfrak{q}_j$ for all $j \neq i$ but $x \notin \mathfrak{q}_i$ (which is possible since the decomposition is minimal), we get that $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_i$. □

Example. The ideal $(xy, y^2) \subset k[x, y]$ can be given minimal primary decompositions

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

The associated primes are $\sqrt{(x^2, xy, y^2)} = (x, y)$ and $\sqrt{(y)} = (y)$, and for each $n \geq 1$ we have that $\sqrt{(x^n, xy, y^2)} = (x, y)$.

Definition. The set of prime ideals associated with $\mathfrak{a}$ is partially ordered with respect to inclusion, i.e. $\mathfrak{p} \leq \mathfrak{p}'$ if $\mathfrak{p} \subseteq \mathfrak{p}'$.

The minimal elements of this set are called the **isolated** or **minimal** prime ideals associated with $\mathfrak{a}$, while the other ones are called **embedded**.

Example. In the decomposition $(y^2, xy) = (x^2, xy, y^2) \cap (y)$, the we have $(y) \subsetneq (x, y)$, so (y) is an isolated prime ideal, while (x, y) is embedded.

Proposition. *The isolated prime ideals of $\mathfrak{a}$ are exactly the prime ideals minimal over $\mathfrak{a}$, i.e. the prime ideals $\mathfrak{p}$ such that there is no prime ideal $\mathfrak{p}'$ with $\mathfrak{a} \subseteq \mathfrak{p}' \subsetneq \mathfrak{p}$.*

Proof. Let $\mathfrak{r}_1, \ldots, \mathfrak{r}_k$ be the prime ideals which are minimal over $\mathfrak{a}$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals associated with $\mathfrak{a}$, ordered in such a way that $\mathfrak{p}_i$ is isolated for $i = 1, \ldots, m$ and embedded for $i = m+1, \ldots, n$. The claim to be shown is

$$\{\mathfrak{r}_1, \ldots, \mathfrak{r}_k\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}.$$

We first show the inclusion $\subseteq$: Let $\mathfrak{p} = \mathfrak{r}_j \supseteq \mathfrak{a}$ be a minimal prime ideal containing $\mathfrak{a}$, and assume $\mathfrak{a} = \cap \mathfrak{q}_i$ is a minimal primary decomposition. We have

$$\mathfrak{a} \subseteq \mathfrak{p} \Rightarrow \sqrt{\mathfrak{a}} = \cap \sqrt{\mathfrak{q}_i} = \cap \mathfrak{p}_i \subseteq \mathfrak{p}.$$

This implies by the lemma above that for some i, $\mathfrak{p}_i \subseteq \mathfrak{p}$. But $\mathfrak{p}$ being minimal over $\mathfrak{a}$ then implies that $\mathfrak{p}_i = \mathfrak{p}$. Hence every prime ideal minimal over $\mathfrak{a}$ is an isolated prime ideal for $\mathfrak{a}$.

Now for the inclusion $\supseteq$, let $\mathfrak{p}_i$ be an isolated prime ideal of $\mathfrak{a}$. Assume for a contradiction that $\mathfrak{p}_i$ is not minimal over $\mathfrak{a}$, then there will be some minimal prime ideal $\mathfrak{p}'$ such that $\mathfrak{a} \subseteq \mathfrak{p}' \subsetneq \mathfrak{p}_i$ (this requires a Zorn's lemma argument). But by the above we know $\mathfrak{p}'$ is associated with $\mathfrak{a}$, so then $\mathfrak{p}_i$ is not isolated, giving a contradiction. □

Example. In our decompositions of $(y^2, xy) \subset k[x, y]$, we will always have two components, of which one is (y) and the other could be (x^2, xy, x^n) for any n. Our uniqueness statement from today says that at least $\sqrt{(y)} = (y)$ and $\sqrt{(x^2, xy, y^n)} = (x, y)$ will be the same for any primary decomposition.

Theorem. *Assume A admits a primary decomposition of (0), and let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be the associated prime ideals of (0). Then*

$$\{x \in A \mid x \text{ is a 0-divisor}\} = \bigcup_{i=1}^{n} \mathfrak{p}_i$$

Proof. Let

$$(0) = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

be a minimal primary decomposition, with $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.

Assume $y \notin \mathfrak{p}_i$ for any i, and that $xy = 0$. Then $\mathfrak{q}_i$ being primary implies that $x \in \mathfrak{q}_i$, and since this holds for all i, we have $x \in \cap \mathfrak{q}_i = (0)$, so $x = 0$. This means y is not a 0-divisor, proving the $\subseteq$ inclusion of the theorem.

For the inclusion $\supseteq$, assume $y \in \mathfrak{p}_i$ for some i. There is some $x \in A$ such that

$$\sqrt{\mathrm{Ann}(x)} = \sqrt{((0) : x)} = \mathfrak{p}_i.$$

This means there is some n such that $y^n \in \mathrm{Ann}(x)$, which means there is some n such that $y^n x = 0$. Taking n_0 to be the minimal such n, we have $y^{n_0-1}x \neq 0$, and $y(y^{n_0-1}x) = y^{n_0}x = 0$, which means y is a 0-divisor. □

Example. In the ring $A = k[x, y]/(xy, y^2)$, the ideal (0) has a primary decomposition

$$(0) = (\bar{x}^2, \bar{x}\bar{y}, \bar{y}^2) \cap (\bar{y}),$$

with $\bar{x}$ and $\bar{y}$ the images of x and y in A. The associated primes ideals of (0) are $(\bar{x}, \bar{y})$ and $(\bar{y})$, and so the set of 0-divisors in A is

$$(\bar{x}, \bar{y}) \cup (\bar{y}) = (\bar{x}, \bar{y}) \subset A.$$

Theorem (Uniqueness 2)**.** *Let $\mathfrak{a}$ be an ideal with primary decomposition*

$$\bigcap_{i=1}^{n} \mathfrak{q}_i,$$

with associated prime ideals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, and assume that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the minimal prime ideals.

Then for each i with $1 \leq i \leq m$, we have

$$\mathfrak{q}_i = \mathfrak{a}^{ec},$$

where extension and contraction are along the homomorphism $A \to A_{\mathfrak{p}_i}$.

In particular, these $\mathfrak{q}_i$ are the same in any minimal primary decomposition.

Example. In the case of (xy, y^2) and all its primary decompositions $(x^n, xy, y^2) \cap (y)$, the primary ideal (y) is uniquely determined by (xy, y^2).

Example. The ideal $(xy) = (x) \cap (y) \subset k[x, y]$ can have no other minimal primary decomposition, since both (x) and (y) are minimal over (xy).

Proof. The idea of the proof is the following simple lemma.

Lemma. *Let $\mathfrak{p} \subset A$ be a prime ideal, and assume that $\mathfrak{q}$ is a primary ideal. We consider the extension and contraction of ideals with respect to $A \to A_{\mathfrak{p}}$.*

- *If $\sqrt{\mathfrak{q}} \not\subseteq \mathfrak{p}$, then $\mathfrak{q}^e = (1)$, and $\mathfrak{q}^{ec} = (1)$.*
- *If $\sqrt{\mathfrak{q}} \subseteq \mathfrak{p}$, then $\mathfrak{q}^{ec} = \mathfrak{q}$.*

Now let $\mathfrak{p}_j$ be a minimal prime of $\mathfrak{a}$, and consider extension and contraction with respect to $A \to A_{\mathfrak{p}_j}$. Since $\mathfrak{p}_j$ is minimal, we have for all $i \neq j$ that $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i \not\subseteq \mathfrak{p}_j$, so $\mathfrak{q}_i^{ec} = (1)$, while $\mathfrak{q}_j^{ec} = \mathfrak{q}_j$.

Recall from the lecture on modules of fractions that localisation (the operation $\mathfrak{a} \mapsto \mathfrak{a}^e$) preserves finite intersections of ideals, as does contraction.

$$\mathfrak{a}^{ec} = \bigcap_{i=1}^{n} \mathfrak{q}_i{}^{ec} = (1) \cap (1) \cap \cdots \cap \mathfrak{q}_j \cap (1) \cap \cdots \cap (1).$$

□

Lecture 15 – Integral dependence

Recall that given a field extension $k \subseteq k'$, we say that an element $\alpha \in k'$ is **algebraic** over k if there is a some polynomial $f \in k[x]$ such that $f(\alpha) = 0$.

We now generalise this concept, but in a stronger form, to general rings.

Definition. Let $A \subseteq B$ be rings, and let $b \in B$. We say b is **integral** over A if we can find a polynomial

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in A,$$

such that $f(b) = 0$.

Remark. It is crucial in this definition that the coefficient of x^n is 1.

Example. Consider $\mathbb{Z} \subset \mathbb{Q}$. Then $b \in \mathbb{Q}$ is integral over $\mathbb{Z} \Leftrightarrow x \in \mathbb{Z}$.

$\Leftarrow$: If $b \in \mathbb{Z}$, then take $f = x - b$, so b is integral over $\mathbb{Z}$.

$\Rightarrow$: Let $b = p/q$, and assume that $\gcd(p, q) = 1$. If

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0,$$

then we get

$$p^n + c_{n-1}p^{n-1}q + \cdots + c_0 q^n = 0.$$

Since q divides all the other terms, q divides p^n, and since $\gcd(q, p) = 1$ this can only happen if $q = 1$. Hence $p/q \in \mathbb{Z}$.

Example. Let k be a field, and consider $k[x] \subseteq k(x)$. Then similarly $f \in k(x)$ is integral over $k[x]$ if and only if $f \in k[x]$. The proof is exactly the same as in the previous example: In $k[x]$ we have unique factorisation into irreducibles, so we can write $f = p/q$ with $p, q \in k[x]$ having no common factor, and the rest of the proof goes through.

Example. Given $A \subseteq B$, every element $a \in A$ is integral over A, by taking the polynomial $x - a$.

Definition. Given $A \subseteq B$ and $b \in B$, we let $A[b] \subseteq B$ be the smallest subring of B containing A and b. Explicitly

$$A[b] = \{\sum_{i=1}^{k} a_i b^i \mid a_i \in A\} \subseteq B.$$

More generally, given $b_1, \ldots, b_n \in B$, we let

$$A[b_1, \ldots, b_n] = \{\sum a_{i_1 \cdots i_n} b_1^{i_1} \cdots b_n^{i_n} \mid a_i \in A\} \subseteq B.$$

Theorem. *Let $A \subset B$, and let $b \in B$. The following are equivalent:*

1. *b is integral over A.*
2. *$A[b]$ is a finitely generated A-module.*
3. *There is a ring C with $A[b] \subseteq C \subseteq B$ such that C is a finitely generated A-module.*

Proof. (1) $\Rightarrow$ (2): The ring $A[b]$ is generated by the infinite set $1, b, b^2, \cdots$. If b is integral, we can write

$$b^k = -(a_{k-1}b^{k-1} + \cdots + a_0),$$

and therefore

$$b^{k+m} = (a_{k-1}b^{k+m-1} + \cdots + a_0 b^m)$$

So we can always express b^{k+m} in terms of b^i for $i < k+m$. This gives that $1, b, \ldots, b^{k-1}$ generate $A[b]$.

(2) $\Rightarrow$ (3): Obvious, take $C = A[b]$.

(3) $\Rightarrow$ (1): We need the following

Lemma (Ch. 2, Lemma 2.4)**.** [7] *Let M be a finitely generated A-module, generated by k elements, and let $\phi\colon M \to M$ be a homomorphism. Then we can find $a_0, \cdots, a_{k-1} \in A$ such that*

$$\phi^k + a_{k-1}\phi^{k-1} + \cdots + a_0 = 0 \in \mathrm{Hom}_A(M, M).$$

where $\phi^i = \overbrace{\phi \circ \cdots \circ \phi}^{i}$.

Take now $M = C$, $\phi\colon C \to C$ given by $\phi(c) = bc$. The lemma ensures that we can find $a_i \in A$ such that

$$\phi^k + a_{k-1}\phi^{k-1} + \cdots + a_0 = 0 \in \mathrm{Hom}_A(C, C).$$

Inserting $1 \in C$ on both sides gives

$$b^k + a_{k-1}b^{k-1} + \cdots + a_0 = 0,$$

so b is integral over A. □

Example. Consider $\mathbb{Z} \subseteq \mathbb{Q}$ again, and take for instance $\frac{1}{2} \in \mathbb{Q}$. In this case $\frac{1}{2}$ is not integral over $\mathbb{Z}$, and equivalently the ring

$$\mathbb{Z}[1/2] = \mathbb{Z}_2 \subseteq \mathbb{Q}$$

is not a finite $\mathbb{Z}$-module.

Proposition. *Assume $b_1, b_2 \in B$ are integral over A. Then $A[b_1, b_2]$ is a finitely generated A-module.*

Proof. Consider the chain of rings

$$A \subseteq A[b_1] \subseteq A[b_1, b_2] \subseteq B$$

Then b_2 is integral over $A \Rightarrow b_2$ is integral over $A[b_1]$, so $A[b_1, b_2] = A[b_1][b_2]$ is a finitely generated $A[b_1]$-module. If it is generated by $c_1, \ldots, c_k$ and $A[b_1]$ is generated as an A-module by $d_1, \ldots, d_l$, one checks that $A[b_1, b_2]$ is generated as an A-module by $\{c_i d_j\}$:

$$\begin{aligned} x \in A[b_1, b_2] \Rightarrow x &= \sum_{i=1}^{k} f_i c_i, \qquad f_i \in A[b_i] \\ &= \sum_{i=1}^{k} \sum_{j=1}^{l} a_{ij} c_i d_j. \end{aligned}$$

[7] It is perhaps useful to think of this lemma as a version of the Cayley–Hamilton theorem. If A is an $(n \times n)$ matrix with coefficients in a field k, then recall its characteristic polynomial is given by

$$\det(xI_n - A) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x],$$

where for instance $a_{n-1} = -tr(A)$ and $a_0 = (-1)^n \det(A)$. The Cayley–Hamilton theorem says that we have an equality of $(n \times n)$-matrices

$$A^n + a_{n-1}A^{n-1} + \cdots + a_0 = 0.$$

□

Corollary. *Let $A \subseteq B$. The set of elements of B which are integral over A forms a subring of B.*

Proof. We must show that given $b_1, b_2 \in B$ integral over A, then also $b_1 \pm b_2$ and $b_1 b_2$ are integral over A. But b_1 and b_2 being integral over A implies $A[b_1, b_2]$ is a finitely generated A-module, and we have $b_1 \pm b_2, b_1 b_2 \in A[b_1, b_2]$. These then satisfy condition (3) of the theorem above, so are integral. □

Definition. Given $A \subseteq B$, we call the ring

$$C = \{b \in B \mid b \text{ integral over } A\}$$

the **integral closure** of A in B. If A is equal to its integral closure, we say it is **integrally closed** in B.

Proposition. *The integral closure C of A in B is itself integrally closed in B.*

Proof. Assume $b \in B$ is integral over C, then we can write

$$b^n + c_{n-1} b^{n-1} + \cdots + c_0 = 0, \qquad c_i \in C.$$

We have that b is integral over $A[c_0, \cdots, c_{n-1}]$, so $A[c_0, \cdots, c_{n-1}, b]$ is a finitely generated $A[c_0, \cdots, c_{n-1}]$-module. The ring $A[c_0, \cdots, c_{n-1}]$ is itself a finitely generated A-module, since the c_i are integral over A. Then $A[c_0, \cdots, c_{n-1}, b]$ is a finitely generated A-module. Therefore b is integral over A, so $b \in C$. □

Example. The ring $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Example. The integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is called the ring of **algebraic integers**, i.e. a complex number z is an algebraic integer if we can find integers $a_0, \cdots, a_{n-1}$ such that

$$z^n + a_{n-1} z^{n-1} + \cdots + a_0.$$

The most important special case is the following. Given an integral domain A, it is contained in its field of fractions K. We say A is **integrally closed** if it is integrally closed in K.

Example. The ring $\mathbb{Z}$, and more generally every unique factorisation domain, is integrally closed.

Example. The ring $\mathbb{Z}[\sqrt{5}]$ is *not* integrally closed (which means that it does not have unique factorisation). The fraction field

$$K = \{\frac{a + b\sqrt{5}}{c + d\sqrt{5}} \mid a, b, c, d \in \mathbb{Z}\} = \mathbb{Q}(\sqrt{5}) \subset \mathbb{R},$$

and in particular we have the golden ratio $\varphi = \frac{1+\sqrt{5}}{2} \in K$. But we have

$$\varphi^2 - \varphi - 1 = 0,$$

so φ is integral over $\mathbb{Z}$, hence over $\mathbb{Z}[\sqrt{5}]$. One checks that $\varphi \notin \mathbb{Z}[\sqrt{5}]$.

Example. Consider the ring $k[x^2, x^3] \subseteq k[x]$. Concretely, we have

$$k[x^2, x^3] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in k, a_1 = 0\}.$$

Let K be the fraction field of $k[x^2, x^3]$. We have an element $a = x^3/x^2 \in K$, and moreover

$$a^2 = x^4/x^2 = x^2/1,$$

so a is a zero of the polynomial $t^2 - x^2$. This shows that a is integral over $k[x^2, x^3]$. One can also check that $a \notin k[x^2, x^3]$, so $k[x^2, x^3]$ is not integrally closed.

(1) Let k be a field. Show that the inclusion homomorphism $\phi\colon k[x^2, x^3] \to k[x]$ extends to an isomorphism between the fraction fields of the two rings.
(2) With respect to the chain of rings $k[x^2, x^3] \subset k[x] \subset k(x)$ from the previous problem, show that $k[x]$ is the integral closure of $k[x^2, x^3]$ in $k(x)$.

Lecture 16 – More on integral dependence + chain conditions

Recall the notions of integral dependence and integral closure from last week. We round out the section on integral dependence with the claim that for an integral domain A, being integrally closed is a local property.

Theorem. *Let A be an integral domain. Then the following are equivalent:*

(1) *A is integrally closed.*
(2) *$A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p} \subset A$.*
(3) *$A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m} \subset A$.*

The proof goes via understanding how integrality behaves with respect to taking fraction rings more generally.

Proposition. *Let $A \subseteq B$ be rings, and let $C \subseteq B$ be the integral closure of A in B. Let $S \subseteq A$ be a multiplicatively closed subset. Then $S^{-1}C \subseteq S^{-1}B$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. Let $D \subseteq S^{-1}B$ be the integral closure of $S^{-1}A$ in $S^{-1}B$. We want $D = S^{-1}C$.

$D \subseteq S^{-1}C$: If $b/s \in D$, then b/s is integral over $S^{-1}A$, and so we can find $a_i \in A$, $s_i \in S$, such that

$$(b/s)^n + (a_{n-1}/s_{n-1})(b/s)^{n-1} + \cdots + \frac{a_0}{s_0} = 0.$$

Multiplying by $(ss_{n-1}\cdots s_0)^n$ gives us a relation

$$\frac{(bs_{n-1}\cdots s_0)^n + d_{n-1}(bs_{n-1}\cdots s_0)^{n-1} + \cdots + d_0 bs_{n-1}\cdots s_0}{1} = 0,$$

in $S^{-1}A$. This means that there is some $t \in S$ such that the relation

$$t((bs_{n-1}\cdots s_0)^n + d_{n-1}(bs_{n-1}\cdots s_0)^{n-1} + \cdots + d_0 bs_{n-1}\cdots s_0) = 0$$

holds in A. Multiplying by t^{n-1} we get that $bs_{n-1}\cdots s_0 t$ is integral over A, and so $bs_{n-1}\cdots s_0 t \in C$, which implies that $b/s \in S^{-1}C$.

$S^{-1}C \subseteq D$: Given $c \in C$ and $s \in S$, we have a relation

$$c^n + a_{n-1}c^{n-1} + \cdots + a_0 = 0 \qquad a_i \in A,$$

which implies that

$$\left(\frac{c}{s}\right)^n + sa_{n-1}\left(\frac{c}{s}\right)^{n-1} + \cdots + s^n a_0 = 0,$$

hence $\frac{c}{s}$ is integral over $S^{-1}A$. It follows that $S^{-1}C \subseteq D$. □

Corollary. *If A is an integral domain and C is the integral closure of A in the fraction field K, then for any prime ideal $\mathfrak{p} \subset A$, we have that $C_{\mathfrak{p}} \subset K$ is the integral closure of $A_{\mathfrak{p}}$ in K.*

Proof of theorem. Let K be the fraction field of A, and let C be the integral closure. If $A = C$, then also $A_{\mathfrak{p}} = C_{\mathfrak{p}}$, so we get (1) ⇒ (2).

(2) ⇒ (3) is obvious since maximal ideals are prime.

To get (3) ⇒ (1), we know that being surjective is a local property. The inclusion map $\phi\colon A \to C$ is an A-module homomorphism. By assumption (3), all $A_{\mathfrak{m}}$ are integrally closed, which means $\phi_{\mathfrak{m}}\colon A_{\mathfrak{m}} \to C_{\mathfrak{m}}$ is surjective. Since being surjective is a local property, it follows that ϕ is surjective, and hence A is integrally closed. □

Example. Recall that $k[x^2, x^3] \subset k[x]$ is an integral domain which is not integrally closed. The fraction field of A is identified with $k(x)$, so we have

$$k[x^2, x^3] \subset k[x] \subseteq k(x),$$

Now $x \in k(x) \setminus k[x^2, x^3]$ is integral over $k[x^2, x^3]$, since x is a zero of the polynomial

$$t^2 - x^2 \in k[x^2, x^3][t].$$

Since x is integral over $k[x^2, x^3]$, it is also integral over all the bigger rings $k[x^2, x^3]_{\mathfrak{p}} \subseteq k(x)$ for various primes $\mathfrak{p}$. Letting $\mathfrak{m} = (x^2, x^3)$, one can check that $x \notin k[x^2, x^3]_{\mathfrak{m}}$, and therefore $k[x^2, x^3]_{\mathfrak{m}}$ is not integrally closed.

Chain conditions

Our theory so far has mostly been developed for arbitrary rings. The motivation for the field of commutative algebra, both historically and in practice, is mostly drawn from number theory and algebraic geometry, where the rings which appear are "reasonably small". In order to develop the theory further, we now begin introducing these smallness conditions. The elegant formulation of these conditions is in terms of chains of subobjects.

Lemma. *Let $(S, \geq)$ be a partially ordered set. The following two conditions are equivalent:*

- *Every sequence $s_1 \leq s_2 \leq s_3 \leq \cdots$ stabilises, that is there is some N such that $s_i = s_N$ for all $i \geq N$.*
- *Every nonempty subset $T \subseteq S$ contains a maximal element of T.*

Recall an element $t \in T$ is maximal if there is no $t' \in T$ with $t' > t$.

Proof. (1) $\Rightarrow$ (2): Suppose $T \subseteq S$ contains no maximal element. This means that for every $t \in T$, we can choose an $f(t) \in T$ with $f(t) > t$. Take now the sequence

$$s_1 = t, s_2 = f(t), s_3 = f(f(t)), \cdots$$

which does not stabilise, so contradicts (1).

(2) $\Rightarrow$ (1): Given a sequence $s_1 \leq s_2 \leq \cdots$, let $T = \{s_i\}_{i=1}^{\infty}$. By (2) there is a maximal element, say s_N, and since $s_i \geq s_N$ for $i \geq N$, we have $s_i = s_N$ for $i \geq N$. □

Definition. Let A be a ring and let M be an A-module, and let S be the set of submodules of M.

- We say M is **Noetherian** if the set S, partially ordered by $M' \leq M''$ if $M' \subseteq M''$, satisfies either condition above.
- We say M is **Artinian** if the set S, partially ordered by $M' \leq M''$ if $M' \supseteq M''$, satisfies either condition above.

In concrete terms, M is Noetherian if it satisfies the **ascending chain condition**: Every sequence

$$M_1 \subseteq M_2 \subseteq M_3 \supseteq \cdots$$

of submodules stabilises, or equivalently, every set T of submodules has a maximal element.

The module M is Artinian if it satisfies the **descending chain condition**, every sequence of submodules

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$$

stabilises. Equivalently, every set T of submodules has a minimal element.

Definition. A ring A is called Noetherian (resp. Artinian) if it is Noetherian (resp. Artinian) as an A-module.

Example. The ring $\mathbb{Z}$ is Noetherian, but not Artinian. A submodule of $\mathbb{Z}$ is an ideal (n). An ascending chain looks like

$$(n_1) \subseteq (n_2) \subseteq (n_3) \subseteq \cdots .$$

The containment $(n_i) \subseteq (n_{i+1})$ implies that n_{i+1} divides n_i, so $n_{i+1} \leq n_i$. The sequence must then clearly stabilise.

The ring $\mathbb{Z}$ is not Artinian, since

$$(2) \supsetneq (4) \supsetneq (8) \supsetneq \cdots$$

does not stabilise.

Example. Let k be a field, and let M be a k-module (vector space). Then M is Noetherian if and only if M is Artinian if and only if M has finite dimension.

Example. The ring $C(\mathbb{R})$ of smooth functions on $\mathbb{R}$ is neither Artinian nor Noetherian, since

$$(1) \supsetneq (x) \supsetneq (x^2) \cdots ,$$

and

$$(\sin(x)) \subsetneq (\sin(x/2)) \subsetneq (\sin(x/4)) \subsetneq (\sin(x/8)) \subsetneq \cdots .$$

This example is mainly to show that the rings appearing outside of algebra typically satisfy none of the smallness conditions we want.

Proposition. *Let M be an A-module. Then M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. Assume that M is Noetherian, and let $M' \subseteq M$ be a submodule. Let

$$T = \{N \subseteq M' \mid M'' \text{ a finitely generated submodule of } M'\}.$$

By the Noetherian hypothesis, there is a maximal element $N_{max} \in T$. Assume for a contradiction that $N_{max} \neq M'$. Then there is an $m \in M' \setminus N_{max}$, so

$$N_{max} \subsetneq N = N_{max} + Am \subseteq M',$$

and N is still finitely generated, so $N \in T$. This contradicts the maximality of N_{max}, so we have our contradiciton, and $N_{max} = M'$, which means M' is finitely generated.

Assume that every submodule $M' \subseteq M$ is finitely generated. Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be a chain of submodules, and let

$$M' = \bigcup_{i=1}^{\infty} M_i \subseteq M.$$

Then M' is by assumption finitely generated, say by $m_1, \ldots, m_n$. We must then have $m_i \in M_{k_i}$ for certain k_i, and taking $k = \max(k_1, \ldots, k_n)$, we have $m_1, \ldots, m_n \in M_k$. But then $M_k = M'$, and the chain stabilises at M_k. $\square$

8. Lecture 17 – Chain conditions II

Theorem. *Let*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

be a short exact sequence of A-modules. Then

$$M \text{ Noetherian} \Leftrightarrow M' \text{ and } M'' \text{ Noetherian.}$$

and

$$M \text{ Artinian } \Leftrightarrow M' \text{ and } M'' \text{ Artinian.}$$

Proof. We only do the statement for te Noetherian condition, the Artinian case is exactly the same.

$\Rightarrow$: If

$$M_1' \subseteq M_2' \subseteq \cdots$$

is a chain of submodules of M', then

$$i(M_1') \subseteq i(M_2') \subseteq \cdots .$$

is a chain of submodules of M. Since M is Noetherian, the latter stabilises, so the first one must as well.

If

$$M_1' \subseteq M_2' \subseteq \cdots$$

is a chain of submodules of M'', then

$$p^{-1}(M_1') \subseteq p^{-1}(M_2') \subseteq \cdots .$$

is a chain of submodules of M. Since M is Noetherian, the latter stabilises, so the first one must as well.

$\Leftarrow$: If

$$M_1 \subseteq M_2 \subseteq \cdots$$

is a chain of submodules, then we get chains

$$i^{-1}(M_1) \subseteq i^{-1}(M_2) \subseteq \cdots$$

and

$$p(M_1) \subseteq p(M_2) \subseteq \cdots .$$

Both of these stabilise, so for some N we have that for all $i \geq N$, then

$$i^{-1}(M_i) = i^{-1}(M_{i+1})$$

and

$$p(M_i) = p(M_{i+1}).$$

Claim: It follows that $M_i = M_{i+1}$. It is not hard to prove this directly,[8] but for fun we can use the snake lemma on this:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & i^{-1}(M_i) & \xrightarrow{i} & M_i & \xrightarrow{p} & p(M_i) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & i^{-1}(M_{i+1}) & \xrightarrow{i} & M_{i+1} & \xrightarrow{p} & p(M_{i+1}) & \longrightarrow & 0. \end{array}$$

[8] If $m \in M_{i+1}$, then $p(m) \in p(M_{i+1}) = p(M_i)$, so there is some $m' \in M_{i+1}$ such that $p(m) = p(m')$. But then $p(m - m') = 0$, so there is some $m'' \in M'_{i+1}$ such that $i(m'') = m - m'$. Since $i^{-1}M_{i+1} = i^{-1}M_i$, we have that $m'' \in M_i'$, and therefore $m = m' + i(m'') \in M_i$.

The snake lemma gives an exact sequence

$$0 \to \ker f' \to \ker f \to \ker f'' \to \operatorname{cok} f' \to \operatorname{cok} f \to \operatorname{cok} f'' \to 0,$$

and since $\operatorname{cok} f' = \operatorname{cok} f'' = 0$, we get that $\operatorname{cok} f = 0$, so f is surjective. We've shown that the sequence M_i stabilises. □

Corollary. *If $M_1, \dots, M_n$ are Noetherian (resp. Artinian) A-modules, then so is*

$$\bigoplus_{i=1}^{n} M_i.$$

Proof. Inductively prove that $\oplus_{i=1}^{j} M_i$ is Noetherian, using the exact sequence

$$0 \to M_{j+1} \to \bigoplus_{i=1}^{j+1} M_i \to \bigoplus_{i=1}^{j} M_i \to 0.$$

□

Proposition. *Let A be a Noetherian (resp. Artinian) ring, and let M be a finitely generated A-module. Then M is Noetherian (resp. Artinian).*

Proof. A is Noetherian $\Rightarrow A^n$ is Noetherian. There is some surjective homomorphism $\phi\colon A^n \to M$, and the short exact sequence

$$0 \to \ker \phi \to A^n \to M \to 0$$

shows that M is Noetherian. □

Proposition. *Let A be a Noetherian (resp. Artinian) ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then A is Noetherian (resp. Artinian).*

Proof. The ring $A/\mathfrak{a}$ has structure as an $A/\mathfrak{a}$-module and an A-module. A set $M \subset A/\mathfrak{a}$ is an $A/\mathfrak{a}$-submodule if and only if it is an A-submodule, since

$$a(x + \mathfrak{a}) \in M \quad \forall a \in A, x + \mathfrak{a} \in M$$

is the same condition as

$$(a + \mathfrak{a})(x + \mathfrak{a}) \quad \forall a + \mathfrak{a} \in A/\mathfrak{a}, x + \mathfrak{a} \in M.$$

Since $A/\mathfrak{a}$ is a Noetherian A-module, it is then also a Noetherian $A/\mathfrak{a}$-module, i.e. Noetherian as a ring. □

Composition series

Definition. A module M is **simple** if it has no proper nontrivial submodules.

Example. If A is a ring with a maximal ideal $\mathfrak{m} \subset A$, then $A/\mathfrak{m}$ is a simple A-module: If $0 \subseteq M \subseteq A/\mathfrak{m}$ is a chain of modules, and $p\colon A \to A/\mathfrak{m}$ is the projection, then

$$p^{-1}(0) = \mathfrak{m} \subseteq p^{-1}(M) \subseteq p^{-1}(A/\mathfrak{m}) = A$$

is a chain of submodules (ideals) of A. Since $\mathfrak{m}$ is maximal, then either $p^{-1}(M) = \mathfrak{m}$ or $p^{-1}(M) = A$, which implies $M = 0$ or $M = A/\mathfrak{m}$.

Remark. One can show that every simple A-module is isomorphic to one of the form $A/\mathfrak{m}$.

Definition. A **composition series** of a module M is a finite chain

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \subsetneq M_{n-1} \supsetneq M_n = 0,$$

which is maximal, that is it cannot be extended to a longer chain by inserting

$$M_i \supsetneq M' \subsetneq M_{i+1}.$$

Equivalently, maximality means that M_i/M_{i+1} is simple for each i. The length of a composition series is n, the number of pieces M_i/M_{i+1} appearing.

Example. Let p be a prime, $k \geq 1$, and consider the $\mathbb{Z}$-module $\mathbb{Z}/(p^k)$. This has a composition series of length k, given by

$$\mathbb{Z}/(p^k) \supsetneq (p)/(p^k) \supsetneq (p^2)/(p^k) \supsetneq \cdots \supsetneq (p^k)/(p^k) = 0.$$

The quotients are $((p^i)/(p^k))/(p^{i+1})/(p^k) \cong (p^i)/(p^{i+1}) \cong \mathbb{Z}/p$, so are simple.

Example. Let p and q be primes, and consider the module $\mathbb{Z}/(pq)$. This has two compositions series

$$\mathbb{Z}/(pq) \supsetneq (p)/(pq) \supsetneq (pq)/(pq) = 0$$

and

$$\mathbb{Z}/(pq) \supsetneq (q)/(pq) \supsetneq (pq)/(pq) = 0$$

Proposition. *Let M be a module with a composition series of length n. Then every composition series has length n, and every chain*

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_k = 0$$

can be extended to a composition series by adding finitely many modules M' with $M_i \supsetneq M' \supsetneq M_{i+1}$.

Proof. Let $l(N)$ be the function on modules defined as the minimal length of a composition series of N ($+\infty$ if N has no composition series).

Lemma. *If $N \subsetneq M$, then $l(N) < l(M)$.*

Proof. Let

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_{l(M)} = 0$$

be a composition series of minimal length. We claim

$$N = M_0 \cap N \supseteq M_1 \cap N \supseteq \cdots \supseteq M_{l(M)} \cap N = 0$$

contains a composition series of N, in the sense that we can find

$$0 = j_0 < j_1 < \cdots < j_k \leq l(M)$$

such that

$$N = M_{j_0} \cap N \supsetneq M_{j_1} \cap N \supsetneq \cdots \supsetneq M_{j_k} \cap N = 0$$

is a composition series. For every i, we have a homomorphism

$$\phi\colon M_i \cap N \hookrightarrow M_i \to M_i/M_{i+1},$$

with

$$\ker \phi = M_{i+1} \cap N.$$

and with

$$\operatorname{im} \phi = M_i/M_{i+1} \text{ or } \operatorname{im} \phi = 0,$$

since M_i/M_{i+1} is simple. Hence

$$(M_i \cap N)/(M_{i+1} \cap N) = (M_i \cap N)/\ker\phi \cong \operatorname{im}\phi \begin{cases} M_i/M_{i+1}(\text{ Case 1}) \\ 0 \text{ Case 2.} \end{cases}$$

In Case 1, we have

$$N \cap M_i = N \cap M_{i+1}$$

and in Case 2,

$$(N \cap M_i)/(N \cap M_{i+1})$$

is simple. Taking the sequence

$$N \cap M_0 \supsetneq N \cap M_{j_1} \supsetneq N \cap M_{j_2} \supsetneq \cdots \supsetneq N \cap M_{j_k} = 0,$$

where $0 = j_0 < j_1 < \cdots < j_k \leq l(m)$ are the indices such that $N \cap M_{j_k} \neq N \cap M_{j_k - 1}$, we have produced a composition series of N of length $k \leq l(M)$, proving $l(N) \leq l(M)$.

Now as $N \subsetneq M$, we have

$$N = N \cap M_0 \neq M_0 = M,$$

while

$$0 = N \cap M_{l(M)} = M_{l(M)} = 0.$$

Let $i > 0$ be the smallest number such that $N \cap M_i = M_i$. Then we have

$$M_{i-1} \supsetneq N \cap M_{i-1} \supseteq N \cap M_i = M_i,$$

which shows that $N \cap M_{i-1} = N \cap M_i$, so i is not in the set $\{j_l\}_{l=1}^k$ Hence $k = l(N) < l(M)$. □

Now if M has a chain of length n, we have

$$l(M) = l(M_0) > l(M_1) > \cdots > l(M_n) = 0,$$

so $l(M) \geq n$. But by definition $l(M) \leq n$, so $l(M) = n$.

If

$$M = M_0 \supsetneq \cdots \supsetneq M_n = 0$$

is a chain of length $n < l(M)$, then by definition of $l(M)$ it cannot be a composition series, so we can extend it. □

Suggested problems

(1) Prove that every simple A-module is isomorphic $A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ in the following steps.
   (a) Show that if $M \neq 0$ is a simple A-module, then for every $m \in M \setminus \{0\}$, we have that
   $$\{am \mid a \in A\} = M.$$
   (b) Show that M is isomorphic to $A/\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq A$.
   (c) Show that the module $A/\mathfrak{a}$ is simple if and only if $\mathfrak{a}$ is maximal.

Lecture 18 – Finite length modules, Noetherian rings

Recall a **composition series** for a module M is a chain

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0,$$

such that every quotient M_i/M_{i+1} is **simple**, that is admits only 0 and M_i/M_{i+1} as submodules.

We stated and almost proved

Proposition. *If M admits a composition series of length n, then every composition series of M has length n, and every chain*

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_k = 0$$

satisfies

1. *$k \leq n$,*
2. *if $k < n$, then the chain can be extended to a composition series by adding modules.*

Definition. The **length** of a module M, denoted $l(M)$, is the length of any composition series of M, and ∞ if M admits no composition series.

Remark. Worth knowing, but not something we will prove or focus on, is the **Jordan–Hölder theorem**. This says that given two composition series M_i and M_i' of a module M, the isomorphism classes of modules appearing in $\{M_i/M_{i+1}\}_{i=1}^{l(M)}$ and $\{M_i'/M_{i+1}'\}_{i=1}^{l(M)}$ are the same. A given isomorphism class appears the same number of times in each of the two sets.

Example. Given distinct primes p and q, the two composition series for $\mathbb{Z}/(pq)$ are

$$\mathbb{Z}/(pq) \supsetneq (p)/(pq) \supsetneq 0$$

and

$$\mathbb{Z}/(pq) \supsetneq (q)/(pq) \supsetneq 0.$$

We have

$$(\mathbb{Z}/(pq))/((p)/(pq)) \cong \mathbb{Z}/p, \quad ((p)/(pq))/0 \cong \mathbb{Z}/q$$

and

$$(\mathbb{Z}/(pq))/((q)/(pq)) \cong \mathbb{Z}/q, \quad ((q)/(pq))/0 \cong \mathbb{Z}/p.$$

Proposition. *Let M be a module. Then M has finite length $\Leftrightarrow$ M is Noetherian and Artinian.*

Proof. $\Rightarrow$: Any increasing sequence has at most $l(M)$ distinct terms, similarly for a decreasing sequence.

$\Leftarrow$: Define a descending chain as follows: Let $M_0 = M$, and let M_1 be a maximal submodule of M not equal to M. This exists because M is Noetherian. Inductively define M_{i+1} as a maximal submodule of M_i among those not equal to M_i. The sequence $M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$ cannot be extended indefinitely, since M is Artinian, hence we eventually have $M_n = 0$. Then M_i defines a composition series for M. □

Proposition. *Given a short exact sequence of modules*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0,$$

we have $l(M) = l(M') + l(M'')$.

Proof. The case where one of $l(M), l(M')$ or $l(M'')$ is ∞ can be handled by the previous proposition and the fact that M is Noetherian (resp. Artinian) if and only if M' and M'' are.

Hence we can assume that M', M and M'' are all of finite length. Take a composition series M'_i for M' and M''_j for M''. These induce the following sequence of submodules of M:

$$\begin{aligned} M &= p^{-1}(M''_0) \supsetneq p^{-1}(M''_1) \supsetneq \cdots p^{-1}(M''_{l(M'')}) = p^{-1}(0) = i(M') \\ &= i(M'_0) \supsetneq i(M'_1) \supsetneq \cdots i(M'_{l(M')}) = 0. \end{aligned}$$

Since

$$p^{-1}(M''_i)/p^{-1}(M''_{i+1}) \cong M''_i/M''_{i+1}$$

and

$$i(M'_i)/i(M'_{i+1}) \cong M'_i/M'_{i+1}$$

this gives a composition series of length $l(M') + l(M'')$ for M. □

Noetherian rings

Recall a ring A is Noetherian if either of the following equivalent conditions hold

(1) Every ascending chain of ideals stabilises.
(2) Every set of ideals has a maximal element.
(3) Every set of ideals is finitely generated.

We have shown that the class of Noetherian rings is closed under quotients, i.e. if A is Noetherian and $\mathfrak{a} \subseteq A$ is an ideal, then so is $A/\mathfrak{a}$.

Proposition. *Let A be a ring, and let $S \subseteq A$ be a multiplicative closed subset. The if A is Noetherian, so is $S^{-1}A$.*

Proof. Every ideal in $S^{-1}A$ is of the form $\mathfrak{a}^e$, where $\mathfrak{a} \subseteq A$ is an ideal and extension is along $A \to S^{-1}A$. Since A is Noetherian, we can write $\mathfrak{a} = (a_1, \ldots, a_n)$, and then $\mathfrak{a}^e = (a_1/1, \cdots, a_n/1)$. Hence every ideal of $S^{-1}A$ is finitely generated. □

Theorem (Hilbert's basis theorem)**.** *Let A be a Noetherian ring. Then $A[x]$ is Noetherian.*

Proof. For any ideal $\mathfrak{a} \subseteq A[x]$, define

$$\mathfrak{a}_n = \{a_n \in A \mid a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathfrak{a}\}.$$

In words, $\mathfrak{a}_n$ is the set of leading terms of degree n polynomials in $\mathfrak{a}$.

Easy claim 1: $\mathfrak{a}_n \subseteq A$ is an ideal.

Easy claim 2: $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ for every n.

Since A is Noetherian, there is an N such that $\mathfrak{a}_n = \mathfrak{a}_\infty$, for all $n \geq N$, i.e. we have

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_N = \mathfrak{a}_{N+1} \subseteq \cdots .$$

Now for each $i = 0, \ldots, N$, we can find a finite set of generators $a_{i,j} \in A$ for $\mathfrak{a}_i$, so that e.g.

$$(a_{i,1}, \ldots, a_{i,k_i}) = \mathfrak{a}_i$$

For each i, j, the fact that $a_{i,j} \in \mathfrak{a}_i$ means there is an $f_{i,j} \in \mathfrak{a}$ such that

$$f_{i,j} = a_{i,j}x^i + \text{lower order terms.}$$

Main claim: We have $\mathfrak{a} = (f_{i,j})_{i,j}$. Let $g \in \mathfrak{a}$, we need to show $g \in (f_{i,j})_{i,j}$. Arguing by induction on $\deg g$, starting from $\deg g = -\infty$ where $g = 0$. There are two cases:

- $\deg g < N$: Writing
$$g = a_i x^i + \text{lower order terms},$$
we have $a_i \in \mathfrak{a}_i$. We can then write
$$a_i = \sum_{j=1}^{k_i} c_i a_{i,j}, \qquad c_i \in A.$$
Considering
$$g' = g - \sum_{j=1}^{k_i} c_i f_{i,j} = (a_i - \sum c_i a_{i,j}) x^i + \text{ lower order terms},$$
we have $\deg g' < \deg g$, and clearly $g' \in \mathfrak{a}$. By induction on degree $g' \in (f_{i,j})$, so $g \in (f_{i,j})$.
- If $\deg g \geq N$, take instead
$$g' = g - \sum_{j=1}^{r_N} c_i f_{N,j} x^{\deg g - N},$$
and conclude similarly.

□

Example. Consider the case of a field k. Then for any ideal $\mathfrak{a} \subseteq k[x]$, we have $\mathfrak{a}_i = (0)$ or $\mathfrak{a}_i = (1)$. We thus get
$$0 = \mathfrak{a}_0 = \mathfrak{a}_1 = \cdots = \mathfrak{a}_{N-1} \subsetneq \mathfrak{a}_N = (1) = \mathfrak{a}_{N+1} = \cdots .$$
In this case the proof above says: Take a generator $a_{N,1}$ $\mathfrak{a}_N$. Choose an $f_{N,1} \in \mathfrak{a}_N$ such that
$$f_{N,1} = a_{N,1} x^N + \text{ lower order terms}.$$
Then $\mathfrak{a} = (f_{N,1})$.

Corollary. *If A is a Noetherian ring, then so is $A[x_1, \ldots, x_n]$.*

Proof. A Noetherian $\Rightarrow$ $A[x_1]$ Noetherian $\Rightarrow$ $A[x_1, x_2] \cong A[x_1][x_2]$ Noetherian and so on. □

Corollary. *If A is Noetherian and B is an A-algebra of finite type, then B is Noetherian.*

Proof. B is of finite type if it is isormorphic (as A-algebra) to $A[x_1, \ldots, x_n]/\mathfrak{a}$. Now A Noetherian $\Rightarrow$ $A[x_1, \ldots, x_n]$ Noetherian $\Rightarrow$ $A[x_1, \ldots, x_n]/\mathfrak{a}$ Noetherian. □

9. Lecture 19 – Hilbert's nullstellensatz and primary decomposition in Noetherian rings

Recall that a field extension $k \subseteq k'$ is finite if k' is a finite-dimensional k-vector space.

Proposition (Zariski's lemma)**.** *Let k be a field, and let A be a finitely generated k-algebra. If A is a field, then A is a finite field extension of k.*

Remark. Clearly, if A is a finite field extension of k, then it is finitely generated as a k-algebra, since then A has a k-basis $a_1, \ldots, a_n$ which generates A as a module over k. These must therefore also generate A as a k-algebra.

Example. The field extension $k \subset k(x)$ is not finite, so the lemma says in this case that $k(x)$ is not a finitely generated k-algebra.

Corollary (Weak nullstellensatz)**.** *Let $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ be a maximal ideal. Then $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension of k.*

If k is algebraically closed, then $k[x_1, \ldots, x_n]/\mathfrak{m} \cong k$, and $\mathfrak{m}$ has the form

$$\mathfrak{m} = (x - a_1, x - a_2, \ldots, x - a_n)$$

for some $a_1, \ldots, a_n \in k$.

Proof. The ring $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a field, so Zariski's lemma applies.

If k is algebraically closed, then it has no non-trivial finite field extension, so we must get $k[x_1, \ldots, x_n]/\mathfrak{m} \cong k$. The homomorphism

$$\phi \colon k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/\mathfrak{m} \to k$$

has

$$(x_1 - \phi(x_1), \ldots, x_n - \phi(x_n)) \subseteq \ker \phi = \mathfrak{m}.$$

It's easy to see that the ideal on the left hand side is maximal, so we have an equality. □

Proof of Zariski's lemma, cheap version. Assume that k is uncountable, (e.g. $k = \mathbb{C}, \mathbb{R}$, not $k = \mathbb{Q}, \overline{\mathbb{Q}}$). Let A be a k-algebra generated by $a_1, \ldots, a_n \in A$, and assume that A is a field.

We claim that each of the a_i are algebraic. If a_i is not algebraic over k, so that $f(a_i) \neq 0$ for all $0 \neq f \in k[x]$, we have an inclusion of fields

$$k \subseteq k(x) \overset{x \mapsto a_i}{\to} A.$$

Now A is generated as a k-module by the elements $a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}$, of which there are countably many, so that A has countable dimension as a k-module.

Claim: The dimension of $k(x)$ as a k-module is greater than or equal to the cardinality of k.

Proof. For each $\alpha \in k$, we have an element $(x - \alpha)^{-1} \in k(x)$. These are all linearly independent. Suppose we have a linear relation

$$\sum_{i=1}^{n} \beta_i (x - \alpha_i)^{-1} = 0$$

between some of them with α_i distinct. Multiplying by $f\prod_{i=1}^n(x-\alpha_i)$ gives a relation between polynomials

$$0 = \sum_{i=1}^n \beta_i \frac{f}{(x-\alpha_i)} \in k[x].$$

Evaluating this polynomial in α_i proves $0 = \beta_i$, so the elements $(x-\alpha_i)^{-1}$ are linearly independent. □

Now since $k(x) \cong k(a_i) \subseteq A$, we have a relation between the dimensions

$$|k| \leq \dim k(x) = \dim k(a_i) \leq \dim A = |\mathbb{Z}|,$$

contradicting our assumption that k was uncountable. □

Primary decompositions in Noetherian rings

Theorem (Lasker–Noether theorem)**.** *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ admits a primary decomposition, i.e. we can write*

$$\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$$

with $\mathfrak{q}_i$ primary ideals.

We prove this in two steps. We say an ideal is **irreducible** if it cannot be written as a finite intersection of strictly bigger ideals. The first step is

Lemma. *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then we can write $\mathfrak{a}$ as a finite intersection of irreducible ideals.*

Proof. Assume there is an ideal which is not an intersection of finitely many irreducible ideals. Since A is Noetherian we can take a maximal such ideal, call it $\mathfrak{a}$. The ideal $\mathfrak{a}$ is not itself irreducible, hence we can write $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{a} \subsetneq \mathfrak{b}, \mathfrak{c}$. But now since $\mathfrak{a}$ is maximal, we can write $\mathfrak{b}$ and $\mathfrak{c}$ as finite intersections of irreducible ideals, so the same holds for $\mathfrak{a}$, a contradiction. □

Lemma. *Let A be a Noetherian ring, and let $\mathfrak{a}$ be irreducible. Then $\mathfrak{a}$ is primary.*

Proof. Passing to $A/\mathfrak{a}$, we may assume that $\mathfrak{a} = (0)$, and we want to show that (0) is primary.

We will assume that (0) is not primary, and then show that it is not irreducible. Since (0) is not primary, there exist $x, y \in A$ such that $xy = 0$, but $x \neq 0$ and y is not nilpotent. Consider then the sequence of ideals in A given by

$$\mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^2) \subseteq \cdots .$$

Since A is Noetherian, this stabilises, so there is an N such that for $n \geq N$, we have $\mathrm{Ann}(y^n) = \mathrm{Ann}(y^N)$. Consider now the ideals (y^N) and $\mathrm{Ann}(y^N)$. Since y is not nilpotent, we have $(y^N) \neq (0)$. And since $x \in \mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^N)$, we have $\mathrm{Ann}(y^N) \neq (0)$.

Main claim: $(y^N) \cap \mathrm{Ann}(y^N) = (0)$, which contradicts (0) being irreducible. *Proof of claim:* An element in the intersection has the form ay^N for some $a \in A$. It further satisfies

$$ay^N y^N = ay^{2N} = 0.$$

But then $a \in \mathrm{Ann}(y^{2N}) = \mathrm{Ann}(y^N)$, so $ay^N = 0$. □

Corollary. *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal.*

- *There is a primary decomposition of* $\mathfrak{a}$.
- *The set of prime ideals of the form* $\sqrt{(\mathfrak{a} : x)}$ *with* $x \in A$ *is finite, and contains all the minimal prime ideals containing* $\mathfrak{a}$.
- *If* $\mathfrak{a} = \sqrt{\mathfrak{a}}$, *then*
$$\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{p}_i,$$
where $\mathfrak{p}_i$ *are the minimal prime ideals containing* $\mathfrak{a}$.
- *The set of 0-divisors in* A *is the union of the (finitely many) minimal prime ideals in* A.

Suggested problems

(1) Let k be a field, let $f \in k[x]$ be such that $f = \prod_{i=1}^{n} g_i$, where the g_i are irreducible. Prove that $k[x]/(f)$ has finite length n.

(2) (*) Let $\mathfrak{a} \subseteq \mathbb{Z}[x]$ be an ideal, and let $0 \neq f \in \mathfrak{a}$ have minimal degree. Examine the proof of the Hilbert basis theorem and use this to prove that if coefficient of the leading term of f is $n = p_1^{e_1} \cdots p_k^{e_k}$, then $\mathfrak{a}$ is generated by at most $\sum_{i=1}^{k} e_i$ elements.

(3) (*) Here is a less constructive proof of the Hilbert basis theorem.
   (a) Let A be a ring, let $\mathfrak{a} \subseteq A[x]$ be an ideal, and let $\mathfrak{a}_i \subseteq A$ be as in the proof of the Hilbert basis theorem. Prove that if $\mathfrak{a} \subseteq \mathfrak{a}'$ and $\mathfrak{a}_i = \mathfrak{a}'_i$ for all i, then $\mathfrak{a} = \mathfrak{a}'$.
   (b) Let $(S, \geq)$ be a partially ordered set satisfying the ascending chain condition, and let $\{s_{i,j}\}_{i,j \geq 0}$ be such that $s_{i,j} \leq s_{i+1,j}$ and $s_{i,j} \leq s_{i,j+1}$ for all $i, j \geq 0$. Prove that there is a J such that $s_{i,j} = s_{i,j+1}$ for all $i \geq 0$ and all $j \geq J$.
   (c) Combine the previous two points and show that if A is a Noeterian ring, then every increasing chain of ideals $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots$ in $A[x]$ must stabilise.

Lecture 20 – Artinian rings

Recall a ring A is **Artinian** if every sequence of ideals

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$$

of A stabilises.

Example. Let k be a field, and let A be a k-algebra which is finite-dimensional as a k-module. Then A is both Artinian and Noetherian as a k-module, since every chain of k-submodules has at most $\dim_k A$ distinct k-modules.

Moreover, since every chain of ideals

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$$

is a chain of A-submodules of A, these are also k-submodules of A, so A is Artinian and Noetherian as a ring.

Take for instance $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$. Then $A = k[x]/(f)$ has a basis as a k-module given by

$$1 + (f), x + (f), \cdots, x^{n-1} + (f),$$

so $\dim_k A = n$, and A is Artinian and Noetherian.

Example. Let $A = k[x, y]/(x^m, y^n)$. Then A has a k-basis given by $x^i y^j + (x^m, y^n)$, with $0 \leq i \leq m, 0 \leq j \leq n$, and so A is Artinian and Noetherian.

Example. For any $n \geq 1$, the ring $\mathbb{Z}/n$ is Artinian and Noetherian.

Lemma. *Let A be an Artinian ring. Then A has finitely many maximal ideals.*

Proof. Suppose not, then we can find an infinite sequence $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ of distinct maximal ideals. The descending sequence

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \cdots$$

must stabilise, so for some N we must have

$$\bigcap_{i=1}^{N} \mathfrak{m}_i = \bigcap_{i=1}^{N+1} \mathfrak{m}_i,$$

which means

$$\mathfrak{m}_{N+1} \supseteq \bigcap_{i=1}^{N} \mathfrak{m}_i.$$

But this implies $\mathfrak{m}_i \subseteq \mathfrak{m}_{N+1}$, which is impossible since these are maximal and distinct. □

Lemma. *In an Artinian ring, every prime ideal is maximal.*

Proof. If A is Artinian and $\mathfrak{p} \subset A$ is prime, then also $A/\mathfrak{p}$ is Artinian, and moreover an integral domain. For any $x \in A/\mathfrak{p}$, we have a descending chain

$$1 \supseteq (x) \supseteq (x^2) \cdots,$$

which must stabilise, so $(x^N) = (x^{N+1})$ for some N. This implies $x^N = yx^{N+1}$, and since $A/\mathfrak{p}$ is an integral domain, we can cancel to get $xy = 1$. Hence x is a unit, and since this holds for all x, $A/\mathfrak{p}$ is a field, so $\mathfrak{p}$ is maximal. □

Definition. Let A be a ring. Its **dimension** (or **Krull dimension**) is the maximum length n of a chain of prime ideals in A

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n.$$

Example. A field k has one prime ideal, so $\dim k = 0$.

Example. In $\mathbb{Z}$, the chains of maximal length look like $(p) \supsetneq (0)$, so $\dim \mathbb{Z} = 1$.

Similarly $\dim k[x] = 1$, since a maximal length chain looks like $(f) \supsetneq (0)$ with f irreducible.

Example. We have shown that every Artinian ring has dimension 0.

Proposition. *Every Artinian ring is Noetherian.*

Proof. We don't prove this; the main steps are as follows.

(1) Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n \subset A$ be the maximal ideals of A. For some $e \geq 0$, we have
$$\mathfrak{m}_1^e \cdots \mathfrak{m}_n^e = (0).$$
(2) In the chain
$$A \supseteq \mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{m}_1^e \supseteq \mathfrak{m}_1^e \mathfrak{m}_2 \cdots \supseteq \mathfrak{m}_1^e \mathfrak{m}_2^e \cdots \mathfrak{m}_n^e = (0),$$
the quotients
$$\mathfrak{m}_1^{i_1} \cdots \mathfrak{m}_n^{i_n} / \mathfrak{m}_1^{i_1} \cdots \mathfrak{m}_j^{i_j+1} \cdots \mathfrak{m}_n^{i_n}$$
are all Artinian A-modules, since A is Artinian.
(3) The quotients are Artinian A-modules, hence Artinian $A/\mathfrak{m}_j$-modules, hence finite dimensional $A/\mathfrak{m}_j$-modules, hence Noetherian $A/\mathfrak{m}_j$-modules, hence Noetherian A-modules.
(4) A is a Noetherian A-module, i.e. Noetherian as a ring.

□

Proposition. *If A is Noetherian and every prime ideal is maximal, then A is Artinian.*

Proof. We assume for a contradiction that A is not Artinian, and consider the set of ideals $\mathfrak{a} \subset A$ such that $A/\mathfrak{a}$ is not Artinian. Since A is Noetherian, we can take a maximal ideal $\mathfrak{a}$ in this set, and obtain $B = A/\mathfrak{a}$, with the property that

- B is Noetherian, but not Artinian.
- Every prime ideal of B is maximal
- If $(0) \neq \mathfrak{b} \subseteq B$ is an ideal, then $B/\mathfrak{b}$ is Artinian.

Claim: B is an integral domain.

Proof. If $xy = 0$ in B with $x, y \neq 0$, then we get a short exact sequence of B-modules

$$0 \to B/\operatorname{Ann}(x) \xrightarrow{\cdot x} B \to B/(x) \to 0.$$

The outer two modules are Artinian, by our assumptions, and so B must be, which is a contradiction. □

Now since B is an integral domain and every prime ideal is maximal, it follows that B is a field, which contradicts our assumption that B is not Artinian. □

Summing up, we have shown

Theorem. *Let A be a ring. Then A is Artinian if and only if it is Noetherian and of dimension 0.*

Proposition. *Every Artinian ring A is isomorphic to a product of Artinian local rings.*

More precisely, if $e \geq 1$ is such that $\mathfrak{m}_1^e \cdots \mathfrak{m}_n^e = 0$, then

$$A \cong \prod_{i=1}^{n} A/\mathfrak{m}_i^e.$$

Proof. The ideal $\mathfrak{m}_i^e$ is not contained in $\mathfrak{m}_j$ for $j \neq i$. It follows that $\mathfrak{m}_i^e + \mathfrak{m}_j^e = (1)$ when $j \neq i$, and that $A/\mathfrak{m}_i^e$ is local.

By the Chinese remainder theorem, the natural homomorphism

$$\phi\colon A \to \prod_{i=1}^{n} A/\mathfrak{m}_i^e,$$

is surjective, and $\ker \phi = \mathfrak{m}_1^e \cdots \mathfrak{m}_n^e = (0)$, so it is an isomorphism. □

Theorem. *Every Artinian ring is isomorphic to a product of Artinian local rings.*

Corollary. *A finite type k-algebra A is Artinian if and only if it is a finite k-algebra (i.e. finite-dimensional as a k-module).*

Proof. We have seen the implication $\Leftarrow$.

Since A is Artinian, it is also Noetherian, and we therefore have a composition series

$$A = \mathfrak{a}_0 \supsetneq \mathfrak{a}_1 \supsetneq \cdots \supsetneq \mathfrak{a}_n = 0,$$

where each quotient $\mathfrak{a}_i/\mathfrak{a}_{i+1}$ is a simple A-module. We know that simple A-modules are isomorphic $A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. By the Nullstellensatz, a module of the form $A/\mathfrak{m}$ has finite dimension as a k-module. The short exact sequences

$$0 \to \mathfrak{a}_{i+1} \to \mathfrak{a}_i \to \mathfrak{a}_i/\mathfrak{a}_{i+1} \to 0$$

together with additivity of dimension show that

$$\dim_k A = \sum_{i=0}^{n-1} \dim_k \mathfrak{a}_i/\mathfrak{a}_{i+1},$$

and in particular is finite. □

Lecture 21 – Discrete valuation rings

Recall from last time the notion of **dimension** of a ring A, the maximal length of any chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

Proposition. *An integral domain A has dimension 1 if and only it is not a field, and every non-zero prime ideal is maximal.*

Proof. If A has dimension 1, there must be a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$$

of prime ideals, which implies that A is not a field. Assume for a contradiction that there is a prime ideal $\mathfrak{p} \neq (0)$ which is not maximal. Then we can find a maximal $\mathfrak{m}$ containing $\mathfrak{p}$, and so find the chain

$$(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m},$$

contradicting $\dim A = 1$.

Conversely, if A is not a field, there is a maximal ideal $\mathfrak{m} \neq (0)$, and so we have at least one chain

$$(0) \subsetneq \mathfrak{m}.$$

On the other hand, there can be no chain

$$(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m},$$

so $\dim A = 1$. □

Proposition. *Let A be a Noetherian integral domain of dimension 1. Then every ideal $\mathfrak{a}$ can be written as a product of primary ideals.*

Proof. If $\mathfrak{a} = (0)$, then $\mathfrak{a}$ is prime and so primary.

Otherwise, the Lasker–Noether theorem asserts that we can write

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n,$$

where the $\mathfrak{q}_i$ are primary and have distinct radicals $\sqrt{\mathfrak{q}_i}$. These are all maximal, and we have that

$$\sqrt{\mathfrak{q}_i + \mathfrak{q}_j} \supseteq \sqrt{\mathfrak{q}_i} + \sqrt{\mathfrak{q}_j} = (1),$$

hence $1 \in \mathfrak{q}_i + \mathfrak{q}_j$, and these are pairwise coprime. Thus we can replace the intersection by a product and find

$$\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_n.$$

□

Discrete valuation rings

Definition. Let K be a field. A **discrete valuation** on K is a surjective function $v\colon K \setminus \{0\} \to \mathbb{Z} \cup \{\infty\}$ satisfying three properties

(1) For all $x, y \in K$, we have $v(xy) = v(x) + v(y)$.
(2) For all $x, y \in K$, we have $v(x + y) \geq \min(v(x), v(y))$.
(3) $v(x) = \infty \Leftrightarrow x = 0$.

Example. The field $\mathbb{Q}$ admits an valuation v_p, defined as follows. Every rational number x admits a prime factorisation $x = p^a p_1^{e_1} \cdots p_n^{e_n}$, where the primes $p, p_1, \cdots p_n$ are distinct and $a, e_1, \cdots, e_n \in \mathbb{Z}$. We define $v_p(x) = a$.

E.g. $v_2(2) = 1$, $v_2(3/2) = -1$.

Example. Let k be a field. The field $k(x)$ admits a valuation defined by the "order of vanishing at 0". Every element of $k(x)$ can be written as $x^n \frac{f}{g}$, where f and g are polynomials such that $f(0), g(0) \neq 0$, and $n \in \mathbb{Z}$. We define $v(x^n \frac{f}{g}) = n$.

Definition. Let A be an integral domain, with fraction field K. We say that A is a **discrete valuation ring** (or DVR), if there exists some valuation v on K such that for $x \in K$ we have

$$x \in A \Leftrightarrow v(x) \geq 0.$$

Remark. If v is a valuation on a field K, then the set $\{x \in K \mid v(x) \geq 0\}$ is easily seen to be a subring of K. In other words, every field equipped with a valuation contains a DVR determined by the valuation.

Example. For the valuation v_p on $\mathbb{Q}$, the associated discrete valuation ring consists of fractions of the form $p^a \frac{m}{n}$ where $a \geq 0$ and p divides neither m nor n. Equivalently, setting $m' = p^a m$, we see that it consists of all fractions m'/n such that p does not divide n, which is precisely the ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$.

Example. For the valuation $v(x^n f/g) = n$, the associated DVR is $k[x]_{(x)} \subset k(x)$.

Example. Let k be a field, and let $k((x))$ be the ring of formal Laurent series, i.e. whose elements are formal sums

$$\sum_{i \geq n} a_i x^i,$$

where $n \in \mathbb{Z}$ (so finitely many terms $a_i x^i$ with $i < 0$ are allowed). One can check that this is a field. Setting $v(f) = i$, where i is the smallest integer such that $a_i \neq 0$, we get a discrete valuation on $k((x))$, with associated DVR the ring of formal power series $k[[x]] \subset k((x))$.

Discrete valuation rings have excellent properties.

Theorem. *Let A be a discrete valuation ring with fraction field K and discrete valuation v. Then*

(1) *The ring A is local, with maximal ideal*

$$\mathfrak{m} = \{x \in A \mid v(x) > 0\}.$$

(2) *For any element $x \in A$ such that $v(x) = 1$, we have $\mathfrak{m} = (x)$.*
(3) *With x as in the previous point, every ideal in A is either (0) or equal to (x^k) for some $k \geq 0$.*
(4) *A has dimension 1.*
(5) *A is integrally closed.*

Proof. (1) Let $x \in A$, and consider $x^{-1} \in K$. The element x is a unit in A if and only if $x^{-1} \in A$, which is if and only if $v(x^{-1}) = -v(x) \geq 0$. But we know that $v(x) \geq 0$, so x is a unit if and only if $v(x) = 0$. Thus the set of non-units is precisely the set described in the proposition, which it's easy to see is an ideal.

(2) If $x, y \in A$ and $v(y) \geq v(x)$, then $v(xy^{-1}) \geq 0$, so $xy^{-1} \in A$, which means that $y \in (x)$. Since a discrete valuation is by definition surjective, there exists at least one such x. In particular, $\mathfrak{m} = (x)$ for any element $x \in A$ with $v(x) = 1$.

(3) Let $\mathfrak{a}$ be an ideal, and let $x \in \mathfrak{a}$ be such that $v(x)$ is minimal. Then for any $y \in \mathfrak{a}$, we have $v(y) \geq v(x)$, so as above we find $y \in (x)$. Thus $\mathfrak{a} \subseteq (x)$. Since obviously $(x) \subseteq \mathfrak{a}$, we have $\mathfrak{a} = (x)$.

(4) By the previous two points, we have that the ideals of A are $(1), (x), (x^2), \cdots$ and (0). It is easy to see that (x) and (0) are the only prime ideals of A, so A has dimension 1.

(5) Let $x \in K$, and assume that x is integral over A. We must show that $x \in A$.
Since x is integral over A, we can find a relation.

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \qquad a_i \in A$$

so

$$x^n = -a_{n-1}x^{n-1} - \cdots - a_0.$$

If $v(x) = d$, we then get

$$\begin{aligned} v(x^n) = nv(x) = nd &= v(-a_{n-1}x^{n-1} - \cdots - a_0) \\ &\geq \min_i(v(-a_i x^i)) \end{aligned}$$

Thus there exists an $i \leq n-1$ such that

$$nd = v(x^d) \geq v(-a_i x^i) = v(-a_i) + v(x^i) \geq id,$$

This gives $(n-i)d \geq 0$, and so $d \geq 0$. Hence $x \in A$.

□

In fact, most of these properties characterise DVRs (among Noetherian local domains of dimension 1).

Proposition. *Let A be a Noetherian, local integral domain of dimension 1. The following are equivalent:*

(1) *A is a DVR.*
(2) *A is integrally closed.*
(3) *$\mathfrak{m}$ is principal.*
(4) *$\mathfrak{m}/\mathfrak{m}^2$ is a 1-dimensional $A/\mathfrak{m}$-module.*
(5) *Every non-zero ideal of A is a power of $\mathfrak{m}$.*
(6) *There exists an $x \in A$ such that every ideal in A is of the form (x^k).*

Proof. We have already seen that (1) implies all the other conditions.

Let us just do a few of the easier other implications.

(4) $\Rightarrow$ (3): If $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional, there is some $x \in \mathfrak{m}$ such that $x + \mathfrak{m}^2$ generates $\mathfrak{m}/\mathfrak{m}^2$. But $\mathfrak{m}$ is finitely generated, since A is Noetherian, and then Nakayama's lemma says that x generates $\mathfrak{m}$.

(3) $\Rightarrow$ (6): There is an x such that $\mathfrak{m} = (x)$, so that every non-unit in A is of the form ax for some $a \in A$. Assume for a contradiction that $\mathfrak{a}$ is an ideal which is not of the form (x^k), and let it be maximal among ideals with this property (there is such a maximal one since A is Noetherian). We have

$$\mathfrak{a} = (y_1, \ldots, y_n) = (a_1 x, \cdots, a_n x) = (a_1, \cdots, a_n)(x).$$

Now $\mathfrak{a} = (a_1, \ldots, a_n)(x) \subseteq (a_1, \ldots, a_n)$. If $\mathfrak{a} = (a_1, \ldots, a_n)$, we have $\mathfrak{a} = (x)\mathfrak{a}$, which by Nakayama's lemma implies $\mathfrak{a} = (0)$.

Otherwise $\mathfrak{a} \subsetneq (a_1, \ldots, a_n)$, which by the maximality property of $\mathfrak{a}$ implies that $(a_1, \ldots, a_n) = (x^k)$ for some k. But then $\mathfrak{a} = (x)(x^k) = (x^{k+1})$, contradicting the defining property of $\mathfrak{a}$.

(6) $\Rightarrow$ (1): For every $y \neq 0$, we have $\sqrt{(y)} = \mathfrak{m} = (x)$. It then follows that $y \in (x^k)$ for some k, and we take a minimal such. Then define $v(y) = k$, and extend this multiplicatively to the fraction field of A. $\square$

Example. Consider the domain $A = k[x^2, x^3] \subset k[x]$, and consider the maximal ideal $\mathfrak{m} = (x^2, x^3) \subset A$. Then $\mathfrak{m}^2 = (x^4, x^5, x^6)$, and we find that $\mathfrak{m}/\mathfrak{m}^2$ is spanned by $x^2 + \mathfrak{m}^2, x^3 + \mathfrak{m}^2$, so is 2-dimensional as a k-module.

The ring $A_\mathfrak{m}$ has local ideal $\mathfrak{m}_\mathfrak{m}$, and the quotient is given by

$$\mathfrak{m}_\mathfrak{m}/(\mathfrak{m}_\mathfrak{m})^2 = (\mathfrak{m}/\mathfrak{m}^2)_\mathfrak{m} \cong \mathfrak{m}/\mathfrak{m}^2,$$

so is 2-dimensional as an $A/\mathfrak{m}$-module.

It follows that $A_\mathfrak{m}$ is not a DVR.

Suggested problems

(1) Let A be a ring such that every ideal is principal. Prove that $\dim A \leq 1$.
(2) Let v be a discrete valuation on a field K. Prove that if $x, y \in K$ are such that $v(x) < v(y)$, then $v(x+y) = v(x)$.
(3) Let v be a discrete valuation on a field K. Prove that if $x \in K$ is such that $x^n = 1$ for some $n \geq 1$, then $v(x) = 0$.
(4) Let A be an integral domain. Let $v\colon A \to \mathbb{Z} \cup \{\infty\}$ be a function such that
$$v(x) = \infty \Leftrightarrow x = 0.$$
and such that for all $x, y \in A$ we have
$$v(xy) = v(x) + v(y)$$
and
$$v(x) + v(y) \geq \min(v(x), v(y)).$$
Assume further that the elements $\{v(x) \mid x \in A\} \subset \mathbb{Z}$ generate $\mathbb{Z}$ as a group. Prove that v can be extended uniquely to give a discrete valuation on the fraction field of A.
(5) Let k be a field. Prove that there is a unique discrete valuation v on $k(x)$ such that
$$v(f) = -n$$
if $f \in k[x]$ is a polynomial of degree n. Describe the associated discrete valuation ring and find a generator of its maximal ideal.
(6) Let k be a field. Prove that there exists a discrete valuation v on $k(x, y)$ such that
$$v(\sum a_{i,j} x^i y^j) = n,$$
where $n = \min\{i + j \mid a_{i,j} \neq 0\}$. Describe the associated discrete valuation ring and find a generator of its maximal ideal.

Definition. A **graded ring** is a ring A together with subgroups $A_i \subseteq A$ for each $i \geq 0$ such that

$$A = \bigoplus_{i=0}^{\infty} A_i,$$

and such that for every $i, j \geq 0$, we have

$$a \in A_i, b \in A_j \Rightarrow ab \in A_{i+j}.$$

Remark. The condition that $A = \bigoplus_{i=0}^{\infty} A_i$ is equivalent to requiring that for every $a \in A$, we can write

$$a = \sum_{i=0}^{\infty} a_i \qquad a_i \in A_i$$

in a unique way (with only finitely many $a_i \neq 0$).

Example. For any ring A, the ring $A[x]$ is graded, by setting

$$A[x]_i = \{ax^i \mid a \in A\} \subset A[x]$$

More generally, the ring $A[x_1, \ldots, x_n]$ is graded by setting

$$f \in A[x_1, \ldots, x_n]_i$$

if and only if f is a sum of terms of the form $ax^{i_1} \cdots x_n^{i_n}$ with $\sum i_k = i$.

Definition. If A is a graded ring and $a \in A_i$, we say that a is **homogeneous of degree** i.

Remark. A given ring A may be considered as a graded ring in different ways, e.g. for $k[x, y]$, we can for instance define a grading by saying $x^i y^j$ is homogeneous of degree $i + j$, or we can say it is homogeneous of degree i.

Remark. Since $A_0 A_0 \subseteq A_0$ and more generally $A_0 A_i \subseteq A_i$ for every i, we have that $A_0 \subseteq A$ is a subring, so A is an A_0-algebra, and every A_i is naturally an A_0-module.

Example. If $f \in A$ is a homogeneous element, then $B = A/(f)$ is also a graded ring, with graded pieces

$$B_i = A_i/(f) \cap A_i.$$

It is an easy exercise to check that this defines a valid grading of B, but note that it is necessary that f is homogeneous.

More generally, if $f_1, \ldots, f_n \in A$ are homogeneous, the ring $A/(f_1, \ldots, f_n)$ inherits a grading from A.

Assumption: We will for the rest of these lectures assume of our graded ring A that $A_0 = k$ is a field, and that A is generated as a k-algebra by homogeneous elements $x_1, \ldots, x_n$ of degree 1. In particular, this implies that we have

$$A \cong k[x_1, \ldots, x_n]/\mathfrak{a},$$

for some ideal $\mathfrak{a} = (f_1, \ldots, f_k)$, where $f_i \in k[x_1, \ldots, x_n]$ are homogeneous elements. The grading of elements in A is inherited from that in $k[x_1, \ldots, x_n]$, i.e. in A we have that

$$ax_1^{i_1} \cdots x_n^{i_n} + \mathfrak{a}$$

is homogeneous of degree $\sum i_k$.

Definition. Let A be a graded ring as above. The **Hilbert function of** A is the function $H_A\colon \mathbb{N} \to \mathbb{N}$ given by $H_A(i) = \dim_k(A_i)$.

Example. Consider $k[x]$. We have $k[x]_n = \{ax^n \mid a \in k\}$ for all n, so $H_{k[x]}(n) = 1$ for all n.

Example. For $k[x_1, \ldots, x_n]$, we have that a basis for $k[x_1, \ldots, x_n]_d$ as a k-module is given by elements

$$x_1^{i_1} \cdots x_n^{i_n}$$

with $i_1 + \cdots + i_n = n$. One can compute the number of such to be

$$\binom{n+d-1}{n-1} = \frac{(n+d-1)(n+d-2)\cdots(d)}{(n-1)!},$$

which gives $H_{k[x_1,\ldots,x_n]}(d) = \binom{n+d-1}{n-1} = \frac{d^{n-1}}{(n-1)!} +$ lower order terms in d.

Example. Let $f \in k[x_1, \ldots, x_n]_i$, and let $A = k[x_1, \ldots, x_n]/(f)$. We have a short exact sequence

$$0 \to k[x_1, \ldots, x_n] \xrightarrow{\cdot f} k[x_1, \ldots, x_n] \to A \to 0,$$

which gives short exact sequences

$$0 \to k[x_1, \ldots, x_n]_{d-i} \xrightarrow{\cdot f} k[x_1, \ldots, x_n]_d \to A_d \to 0,$$

and so

$$\dim A_d = \dim k[x_1, \ldots, x_n]_d - \dim k[x_1, \ldots, x_n]_{d-i}.$$

In particular

$$H_A(d) = \begin{cases} \binom{n+d-1}{n-1} \text{ if } d < i \\ \binom{n+d}{n} - \binom{n+d-i-1}{n-1} \text{ if } d \geq i. \end{cases}$$

Note in particular that for $d \geq i$, we have $H_A(d)$ is a polynomial in d, of the form

$$\frac{id^{n-1}}{(n-2)!} + \text{ lower order terms}$$

Proposition. *Let A be a graded ring as above. There exists a rational polynomial g and an integer N such that, for $n \geq N$, we have $H_A(n) = f(n)$.*

Lemma. *Let $F\colon \mathbb{N} \to \mathbb{N}$ be a function. Assume that there is an $N \geq 0$ and a rational polynomial g such that*

$$F(n+1) - F(n) = g(n)$$

for all $n \geq N$. Then there exists a polynomial f, with $\deg f = \deg g + 1$, such that $F(n) = f(n)$ for all $n \geq N$.

Proof. Let V_d be the space of degree d rational polynomials. We have a $\mathbb{Q}$-linear map $\phi\colon V_d \to V_{d-1}$ given by $f(x) \mapsto f(x+1) - f(x)$. The kernel of ϕ is the set of constant polynomials, and since $\dim V_d = \dim V_{d-1} + 1$, the map ϕ is surjective. We can therefore find an $f \in V_d$ such that $\phi(f) = g$, and by adjusting the constant term of f, we can ensure that $f(N) = F(N)$. By induction on n, starting from N, we then find that $f(n) = F(n)$ for all $n \geq N$. $\square$

Proof of proposition. The proof is by induction on the number of generators of A as a k-algebra. Assume A is generated by elements $x_1, \ldots, x_n$, homogeneous of degree 1. If x_1 is not a 0-divisor, we have a short exact sequence

$$0 \to A \xrightarrow{\cdot x_1} A \to A/(x_1) \to 0,$$

which gives, for each i, a short exact sequence

$$0 \to A_i \xrightarrow{\cdot x_1} A_{i+1} \to (A/(x_1))_{i+1} \to 0.$$

We thus have

$$H_A(i+1) = H_A(i) + H_{A/(x_1)}(i+1)$$

or equivalently

$$H_A(i+1) - H_A(i) = H_{A/(x_1)}(i+1).$$

Since $A/(x_1)$ is generated by the elements $x_2, \cdots, x_n$, the induction hypothesis shows that $H_{A/(x_1)}$ is eventually a polynomial, and our lemma shows that the same is then true of H_A.

If x_1 *is* a 0-divisor, the short exact sequence

$$0 \to A/\operatorname{Ann}(x_1) \xrightarrow{\cdot x_1} A \to A/(x_1) \to 0$$

let's us reduce the claim from A to $A/(x_1)$ (handled by induction) and $A/\operatorname{Ann}(x_1)$ (where x_1 is not a 0-divisor, so handled above). □

Definition. We call the polynomial which computes the Hilbert function for large integers the **Hilbert polynomial**.

Lecture 23 – The associated graded ring of a local ring, and the dimension theorem

Definition. Let A be a ring, and let $\mathfrak{a} \subseteq A$ be an ideal. We define the graded ring $G_{\mathfrak{a}}(A)$ as the group

$$A/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \mathfrak{a}^2/\mathfrak{a}^3 \oplus \cdots .$$

We have

(1) A grading given by $G_{\mathfrak{a}}(A)_i = \mathfrak{a}^i/\mathfrak{a}^{i+1}$.
(2) Given homogeneous elements $x + \mathfrak{a}^i \in G_{\mathfrak{a}}(A)_i$ and $y + \mathfrak{a}^j \in G_{\mathfrak{a}}(A)_j$, their product is
$$(x + \mathfrak{a}^i)(y + \mathfrak{a}^j) = xy + \mathfrak{a}^{i+j-1} \in G_{\mathfrak{a}}(A)_{i+j}.$$
(3) Given general elements $x = \sum_i x_i, y = \sum_j y_j \in G_{\mathfrak{a}}(A)$, with x_i and y_j, homogeneous, we have
$$xy = \sum_{i,j} x_i y_j.$$

Definition. Let A be a local ring, and let $\mathfrak{m} \subset A$ be the maximal ideal. Define the **associated graded ring** of A by

$$G(A) = G_{\mathfrak{m}}(A) = \bigoplus_{i=0}^{\infty} \mathfrak{m}^i/\mathfrak{m}^{i+1},$$

with the above graded ring structure.

Remark. Note that $G(A)_0 = A/\mathfrak{m}$ is a field, which we will denote by k.

Assume that A is Noetherian. Then $\mathfrak{m}$ is finitely generated, say $\mathfrak{m} = (y_1, \ldots, y_n)$. Let $x_i = y_i + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$. Every element of $G(A)_1$ can be written as

$$\sum_{i=1}^{n} a_i y_i + \mathfrak{m}^2 = \sum_{i=1}^{n} (a_i + \mathfrak{m})(y_i + \mathfrak{m}) = \sum_{i+1}^{n} (a_i + \mathfrak{m}) x_i,$$

so in other words the x_i generate $G(A)_1$ as a k-module.

More generally, for $j \geq 1$, the ideal $\mathfrak{m}^j$ is generated by elements $y_1^{e_1} \cdots y_n^{e_n}$, with $\sum e_i = j$. It follows that $G(A)_j$ is generated as a k-module by elements $x_1^{e_1} \cdots x_n^{e_n}$ with $\sum e_i = j$.

Finally this implies that $G(A)$ is generated as a k-module by the elements $x_1^{e_1} \cdots x_n^{e_n}$, where $e_i \geq 0$. This is the same as saying that $G(A)$ is generated as a k-algebra by the x_i.

In other words, the ring $G(A)$ satisfies our good assumptions from last lecture, namely that $G(A)_0$ is a field and that $G(A)$ is generated by finitely many elements $x_1, \ldots, x_n \in G(A)_1$, so our definitions and results about the Hilbert polynomial apply to $G(A)$.

Example. If A is a field, then $\mathfrak{m} = 0$, so $\mathfrak{m}^k/\mathfrak{m}^{k+1} = 0$ for $k \geq 1$. We thus get $G(k) = G(k)_0 = k$.

Example. Let A be a DVR, e.g. $A = \mathbb{Z}_{(p)}$ or $A = k[x]_{(x)}$. Then there exists an $x \in \mathfrak{m}$ such that $\mathfrak{m}^i = (x^i)$ for all k. We also have that

$$\mathfrak{m}^i = (x^i) \supsetneq (x^{i+1}) = \mathfrak{m}^{i+1}.$$

Thus we have an isomorphism of k-modules

$$G(A) = A/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \cdots \cong k \oplus k \oplus k \cdots,$$

We define a k-algebra homomorphism

$$\phi\colon k[y] \to G(A)$$

by setting $\phi(y) = x + \mathfrak{m}^2 \in G(A)_1$, which implies more generally that

$$\phi(\sum a_i t^i) = \sum (a_i x^i + (x)^{i+1}).$$

Since $G(A)$ is generated as a k-algebra by $x + \mathfrak{m}^2$, this map is surjective.

We thus have $G(A) \cong k[y]/\ker\phi = k[y]/(f)$ for some $f \in k[y]$. But if $f \neq 0$, we have $\dim_k k[y]/(f) = \deg f$, and $\dim_k G(A) = \infty$, so in fact $f = 0$, and $G(A) \cong k[y]$.

Example. The ring $\mathbb{Z}/(p^k)$ is local, with maximal ideal (p). The associated graded ring is

$$\mathbb{Z}/(p) \oplus (p)/(p^2) \oplus (p^2)/(p^3) \oplus \cdots \oplus (p^{k-1})/(p^k).$$

Each group $(p^i)/(p^{i+1})$ is isomorphic to $\mathbb{Z}/p$ via $a \mapsto ap^i + (p^{i+1})$, so we get

$$G(A) \cong \mathbb{Z}/(p) \oplus \mathbb{Z}/(p) \oplus \cdots \oplus \mathbb{Z}/(p).$$

A similar computation to the previous example shows $G(A) \cong (\mathbb{Z}/p)[y]/(y^{k+1})$.

Example. If A is a graded ring with our assumptions, then $\mathfrak{m} = \bigoplus_{i \geq 1} A_i$ is a maximal ideal, with $A/\mathfrak{m} = A_0$. We get a local ring $A_\mathfrak{m}$, and we have $G(A_\mathfrak{m}) \cong A$. The isomorphism from A to $G(A_\mathfrak{m})$ sends $x \in A_i$ to $x/1 + \mathfrak{m}^{i+1} \in G(A_\mathfrak{m})_i$.

Proposition. *Let A be a Noetherian local ring. There is an $N \geq 0$ and a rational polynomial χ_A such that if $n \geq N$, we have*

$$l(A/\mathfrak{m}^n) = \chi_A(n).$$

Proof. Using the short exact sequences

$$0 \to \mathfrak{m}^{i+1} \to \mathfrak{m}^i \to A/\mathfrak{m}^i \to 0,$$

and the additivity of the length function, we find that

$$l(A/\mathfrak{m}^i) - l(A/\mathfrak{m}^{i-1}) = l(\mathfrak{m}^{i-1}/\mathfrak{m}^i).$$

Now

$$l(\mathfrak{m}^{i-1}/\mathfrak{m}^i) = \dim_k(\mathfrak{m}^{i-1}/\mathfrak{m}^i) = H_{G(A)}(i-1),$$

which is a polynomial for sufficiently large i. Hence by our difference lemma from last lecture, the function $i \mapsto l(A/\mathfrak{m}^i)$ is a polynomial for large i (of degree one greater than $H_{G(A)}(i)$). □

Definition. For a Noetherian local ring A, the above polynomial χ is called the **characteristic polynomial**, or the **Hilbert–Samuel polynomial**.

Example. If A is an Artinian local ring, then $\mathfrak{m}^n = 0$ for some sufficiently large n. This implies that the characteristic polynomial is constant, equal to $l(A)$.

Example. If A is a DVR, then $\chi_A(n) = n$.

Theorem (The dimension theorem)**.** *Let A be a Noetherian local ring. Then A has finite dimension, and the following three numbers are equal:*

(1) $\dim A$
(2) $\deg \chi_\mathfrak{m}(A)(n)$.

(3) *The minimal number of generators for an $\mathfrak{m}$-primary ideal $\mathfrak{q}$.*

Remark. Let $\mathfrak{q} = (x_1, \ldots, x_n) \subset A$. Then $\mathfrak{q}$ is $\mathfrak{m}$-primary if and only if either of the following hold:

- $\sqrt{\mathfrak{q}} = \mathfrak{m}$
- $\mathfrak{q}$ is contained in no other primes than $\mathfrak{m}$
- $A/\mathfrak{q}$ is of dimension 0.

Thus the integer in point 3 is the minimal n such that we can find $x_1, \ldots, x_n \in \mathfrak{m}$ with $\dim A/(x_1, \ldots, x_n) = 0$.

Corollary. *Let A be a Noetherian local ring. Then* $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Proof. Let $N = \dim_k \mathfrak{m}/\mathfrak{m}^2$, and let $x_1 + \mathfrak{m}^2, \ldots, x_N + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$ be a basis for $\mathfrak{m}/\mathfrak{m}^2$. Then by Nakayama's lemma, we have $\mathfrak{m} = (x_1, \ldots, x_N)$, so (3) = (1) implies $\dim A \leq N$. □

Corollary. *Let k be a field. Then* $\dim k[x_1, \ldots, x_n] = n$.

Proof. We'll assume k is algebraically closed for simplicity. We have $\dim k[x_1, \ldots, x_n] = \max \dim k[x_1, \ldots, x_n]_{\mathfrak{m}}$, where the maximum is taken over all maximal ideals $\mathfrak{m}$. By the Nullstellensatz, we know that $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ with $a_i \in k$, and so

$$\mathfrak{m}_{\mathfrak{m}} = ((x_1 - a_1)/1, \cdots, (x_n - a_n)/1) \subset k[x_1, \ldots, x_n]_{\mathfrak{m}}.$$

Hence $\dim k[x_1, \ldots, x_n]_{\mathfrak{m}} \leq n$ by the previous corollary. But $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n) \subsetneq k[x_1, \ldots, x_n]$ is a chain of prime ideals, so also $\dim k[x_1, \ldots, x_n] \geq n$. □

Corollary (Krull's principal ideal theorem)**.** *Let A be a Noetherian ring, let $x \in A$, and let $\mathfrak{p} \subset A$ be a prime ideal which is minimal among those containing x. Then* $\dim A_{\mathfrak{p}} \leq 1$.

Proof. We have that $A_{\mathfrak{p}}$ is Noetherian and local, and moreover there is no prime ideal containing $(x/1)$ besides the maximal ideal $\mathfrak{p}_{\mathfrak{p}}$. Thus $(x/1)$ generates a $\mathfrak{p}_{\mathfrak{p}}$-primary ideal, so $\dim A_{\mathfrak{p}} \leq 1$. □

Corollary. *Let A be a Noetherian local ring, and let $x \in \mathfrak{m}$ be a non-zero-divisor. Then* $\dim A/(x) = \dim A - 1$.

Proof. We estimate $\dim A/(x)$ in two ways. First, a maximal chain of prime ideals in $A/(x)$ corresponds (by contraction along $A \to A/(x)$) to a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_{\dim A/(x)} = \mathfrak{m},$$

where $x \in \mathfrak{p}_0$, and $\mathfrak{p}_0$ is minimal among prime ideals containing x. Since x is not a 0-divisor, it is not contained in any minimal prime ideal of A, so $\mathfrak{p}_0$ is not minimal. Hence there exists a prime ideal $\mathfrak{p} \subsetneq \mathfrak{p}_0$, which implies $\dim A \geq \dim A/(x) + 1$.

On the other hand, by Krull's principal ideal theorem, since $\dim A_{\mathfrak{p}_0} \leq 1$, there can not be a longer chain of prime ideals contained in $\mathfrak{p}_0$, so $\dim A \leq \dim A/(x) + 1$. □

Example. Let $B = k[x^2, x^3]$, let $\mathfrak{m} = (x^2, x^3)$ and let $A = B_{\mathfrak{m}}$, with maximal ideal $\mathfrak{m}_{\mathfrak{m}}$. Then

$$\mathfrak{m}_{\mathfrak{m}}^i/\mathfrak{m}_{\mathfrak{m}}^{i+1} \cong \mathfrak{m}^i/\mathfrak{m}^{i+1} \cong (x^{2i}, x^{2i+1})/(x^{2i+2}, x^{2i+3}) \cong k^2$$

as k-modules. It follows that $\dim G(A)_i = 2$ for $i \geq 1$ and $\dim G(A)_0 = 1$, and so $\chi_A(i) = 2i + 1$.

Suggested problems

(1) Let A be a graded ring and let $f \in A_d$. Prove that $B = A/(f)$ becomes a graded ring by setting $B_i = A_i/((f) \cap A_i)$.

(2) Let A be a graded ring such that A_0 is a field, which is generated as an A_0-algebra by finitely many elements $x_1, \ldots, x_n \in A_1$. Prove that $\mathfrak{m} = \oplus_{d \geq 1} A_d$ is a maximal ideal of A, and that

$$\mathfrak{m} = (x_1, \ldots, x_n).$$

(3) With the notation from the previous problem, show that for each $k \geq 0$, we have

$$\mathfrak{m} = \bigoplus_{d \geq k} A_d.$$

(4) With notation from the previous two problems, show that we have an isomorphism of graded rings

$$A \cong G(A_{\mathfrak{m}}).$$