Definition

A **commutative ring** is a set R together with two binary operations $+ : R \times R \to R$ ("addition") and $\cdot : R \times R \to R$ ("multiplication") such that

(a) $(R, +)$ is an Abelian group (we call the additive identity 0_R or just 0),

(b) multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$, and there exists a multiplicative identity 1_R: $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$, and

(c) for all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot b + a \cdot c$.

(d) $a \cdot b = b \cdot a$ for all $a, b \in R$.

Remark

We do not consider noncommutative rings in this course.

Definition

A ring R is a called an **integral domain**, or just a **domain** if it satisfies

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

An nonzero element a such that $ab = 0$ for some $b \neq 0$ is called a **zero divisor**. Thus a domain is a ring with no zero divisors.

Definition

An element $a \in R$ is called a **unit** or an **invertible element** if a has a multiplicative inverse: $b \in R$ with $ab = 1$.

Definition

A **field** is a ring where every nonzero element is a unit.

We have

$$\{\text{Fields}\} \subset \{\text{Integral domains}\} \subset \{\text{Rings}\}.$$

Simple examples

Example

The integers $\mathbb{Z}$ with its usual addition and multiplication is a ring. Also, $\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ the integers modulo n form a ring.

Definition

If R and S are rings then their Cartesian product $R \times S$ is a ring with operations defined componentwise:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2).$$

Note that $R \times S$ is never a domain because $(1, 0) \times (0, 1) = (0, 0)$.

Example

Let $\mathcal{C}[0, 1]$ be the set of continuous real functions defined on $[0, 1]$. For $f, g \in \mathcal{C}[0, 1]$ define $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$. This turns $\mathcal{C}[0, 1]$ into a ring. Is $\mathcal{C}[0, 1]$ an integral domain?

Polynomial rings

Let R be a ring.

- $R[x]$ is the set of all R-linear combinations of nonnegative powers of x, i.e., expressions of the form $a_0 + a_1 x + \cdots + a_d x^d$.
- Operations:

$$\left(\sum_i a_i x^i\right) + \left(\sum_j b_j x^j\right) = \sum_i (a_i + b_i) x^i$$

$$\left(\sum_i a_i x^i\right) \cdot \left(\sum_j b_j x^j\right) = \sum_d \sum_{k=0}^{d} (a_k \cdot b_{d-k}) x^d.$$

- Now define $R[x_1, \ldots, x_n]$, the polynomial ring in $x_1, \ldots, x_n$ with coefficients in R, inductively as $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$.
- If R is a domain, so is $R[x_1, \ldots, x_n]$ (exercise!).

Subrings

Definition

Let R be a ring. We say that $S \subseteq R$ is a **subring** of R if

(a) $(S, +)$ is a subgroup of $(R, +)$

(b) S is closed under multiplication, i.e. $a, b \in S \implies ab \in S$

(a) $1_R \in S$

In other words operations of R make S into a ring.

Example

We have subrings $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Example

If R is a ring, we have a chain of subrings

$$R \subset R[x_1] \subset R[x_1, x_2] \subset \dots.$$

Ideals

Definition

Let R be a ring. We say that $I \subseteq R$ is an **ideal** of R if

(a) $(I, +)$ is a subgroup of $(R, +)$

(b) I is closed under multiplication by R, i.e.
$a \in R, b \in I \implies ab \in I$.

0 and R are ideals of R. We refer to ideals $I \neq R$ as **proper ideals**.

Example

R is a field if and only if its only ideals are 0 and R.

Example

$n\mathbb{Z} \subset \mathbb{Z}$ is an ideal of $\mathbb{Z}$, $\mathbb{Z}$ is PID (principal ideal domain): every ideal of $\mathbb{Z}$ has this form.

Remark

Ideals are almost never subrings. The only ideal of R which is also a subring of R is R itself. Indeed if we have $1 \in I$, then for any $r \in R$ we have $r = r \cdot 1 \in I$ by definition of an ideal.

Construction of ideals

For every $a \in R$ we have a **principal ideal**

$$(a) = aR = \{ra : r \in R\} \subset R.$$

A useful trick: $a \in R$ is a unit if and only if $(a) = R$.

More generally, for $a_1, \ldots, a_n \in R$ we define **ideal generated by** $a_1, \ldots, a_n$ to be

$$(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n = \{r_1 a_1 + \cdots + r_n a_n,\ r_i \in R\}.$$

This is the smallest ideal which contains $a_1, \ldots, a_n$.

If $I_\lambda \subset R$, $\lambda \in \Lambda$, are ideals, then we can form

- The **intersection** $\bigcap_{\lambda \in \Lambda} I_\lambda \subset R$, which is the biggest ideal contained in all I_λ.
- The **sum** $\sum_{\lambda \in \Lambda} I_\lambda = \{r_1 + \cdots + r_n : r_i \in M_{\lambda_i}\} \subset R$, which is the smallest ideal which contains all I_λ.

Products and powers of ideals

Let $I, J \subset R$ be ideals. We define their **product** $I \cdot J$ to be the ideal generated by products $a \cdot b$, $a \in I$, $b \in J$. Thus we have

$$I \cdot J = \{a_1 b_1 + \cdots + a_n b_n, a_i \in I, b_j \in J\}.$$

Note that $IJ \subset I \cap J$.

For an ideal $I \subset R$ we define its **powers** $I^2 = I \cdot I, I^3 = I \cdot I \cdot I$ and so on.

Example

Let $R = k[x_1, \ldots, x_n]$, $I = (x_1, \ldots, x_n)$. What is I^m? Notice that $x_1^2 + x_2^2 \in I^2$ usually cannot be written as a product of two elements in I (unless $x^2 + 1 = 0$ has a solution in k).

Homomorphisms of rings

Definition

Let R and S be rings. A **homomorphism** from R to S is a map $\phi : R \to S$ which preserves the ring structure. In other words we require:

(a) ϕ is a homomorphism of additive groups $(R, +) \to (S, +)$

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

(b) $\phi(1_R) = 1_S$

A homomorphism is an **isomorphism** if it is a bijection (notation for isomorphic rings: $R \simeq S$).

Example

Let R, S be rings and let S be a subset of R. Then S is a subring of R if and only if the inclusion map $S \subseteq R$ is a homomorphism.

Exercise

For any ring R there exists a unique ring homomorphism $\mathbb{Z} \to R$.

Kernel and Image

Definition

Let R, S be rings and let $\phi : R \to S$ be a ring homomorphism. The **kernel** of ϕ, denoted $\ker(\phi)$, is $\{r \in R \mid \phi(r) = 0\}$ and the **image** of ϕ, denoted $\mathrm{Im}(\phi)$, is $\{\phi(r) \mid r \in R\}$.

Proposition

Let $\phi : R \to S$ be a ring homomorphism. Then

(a) *The the kernel of ϕ is an ideal* $\ker(\phi) \subset R$

(b) *The image of ϕ is a subring* $\mathrm{Im}(\phi) \subset S$

Proof is a straightforward exercise.

Note that $\phi : R \to S$ is injective if and only if $\ker(\phi) = 0$, because this is true for abelian groups.

Contraction and expansion of ideals

Proposition

Let $\phi : R \to S$ be a ring homomorphism and let J be an an ideal of S. Then $I = \phi^{-1}(J) = \{a \in R \,|\, \phi(a) \in J\}$ is an ideal of R.

The proof is a straightforward exercise. We sometimes refer to I as **contraction of J to R** and write $I = J^c$.

Example

Let $R \subset S$ be a subring, and $J \subset S$, then $J \cap R \subset R$ is an ideal.

Remark

In the notation of the Proposition if $I \subset R$ is an ideal, then $\phi(I)$ is usually not an ideal of S (think of an example!). We often consider $J = \phi(I)S \subset S$, the smallest ideal of S containing $\phi(I)$. We sometimes refer to $\phi(I)S$ as the **expansion of I to S**, and write $J = I^e$.

Quotients of rings

Ideals are used to form quotient rings. Let $I \subseteq R$ be an ideal. We consider the quotient abelian group R/I with multiplication

$$(r + I)(s + I) = rs + I,$$

and because I is an ideal we see that this is well-defined, i.e. independent of choices of representatives r, s of the equivalence classes. It is then easy to see that R/I together with this multiplication and identity element $1 + I$ forms a ring.

Proposition

The map $\phi : R \to R/I$ defined as $r \mapsto r + I$ is a surjective homomorphism with kernel $\ker(\phi) = I$.

This follows from the construction of R/I and its operations. We refer to ϕ as the quotient homomorphism.

Example

The quotient ring $\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ is the ring of integers modulo n.

Example

Let k be a field, consider the ideal $(x^n) \subset k[x]$. Consider the quotient ring $k[x]/(x^n)$. In this ring two polynomials $f(x)$ and $g(x)$ become equal if $f(x) - g(x) \in (x^n)$, that is if $f(x) - g(x)$ only has terms of degrees n and higher. In other words elements of the quotient ring are represented by McLaurin series expansions up to order $n-1$:

$$\overline{f(x)} = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}, \; a_i \in k$$

with usual operations and ignoring terms of higher order.

Quotients of rings

The statements about quotient groups often generalize easily to quotient rings. Proofs of the Theorems below are straightforward exercises.

Theorem (First Isomorphism Theorem)

Let $\phi : R \to S$ be an homomorphism. Then ϕ induces a isomorphism

$$\overline{\phi} : R/\ker\phi \to \operatorname{Im}\phi$$

given by $\overline{\phi}(r + \ker\phi) = \phi(r)$.

Theorem

Let R be a ring, $I \subseteq R$ an ideal and let $\phi : R \to R/I$ be the quotient map. There is a bijection:

$$\{\textit{Ideals } \overline{J} \subset R/I\} \leftrightarrow \{\textit{Intermediate ideals } I \subset J \subset R\}$$

given by $\overline{J} \subseteq R/I \mapsto \phi^{-1}(\overline{J})$ and $J \subseteq R \mapsto \phi(J) = J/I$.

Prime and maximal ideals

Let $I \subset R$ be a proper ideal (recall that this means $I \subsetneq R$).

Definition

(a) I is a **prime ideal** if whenever $ab \in I$ for some $a, b \in R$, then $a \in I$ or $b \in I$.

(b) I is a **maximal ideal** if I is maximal with respect to inclusion in the set of proper ideals, i.e. if there is no strictly larger proper ideal $I \subsetneq J \subsetneq R$.

Example

Let $R = \mathbb{Z}$. Then ideals $(p) \subset \mathbb{Z}$ are maximal and prime. The ideal $(0) \subset \mathbb{Z}$ is prime but not maximal.

Remark

Note that if $I \subset R$ is a prime ideal and if $r_1 r_2 \dots r_n \in I$, then $r_i \in I$ for some i (easy induction).

Maximal ideals are prime

Proposition

If $I \subset R$ is maximal, then I is prime.

Proof.

- Let $ab \in I$ and $a \notin I$. We need to show that $b \in I$.
- Consider $J = I + (a)$. We have $I \subsetneq J$.
- Since I is maximal, J can't be proper: $J = R$
- Thus $y + ax = 1$ for some $y \in I$, $a \in R$.
- Multiplying the equation by b we get $by + abx = b$, which implies $b \in I$.

Another perspective on maximal and prime ideals

Proposition

Let $I \subset R$ be a proper ideal.

(a) *$I \subset R$ is prime if and only if R/I is a domain.*

(b) *$I \subset R$ is maximal if and only if R/I is a field.*

This gives another proof why a maximal ideal must be prime.

Proof.

- (a): The condition for R/I to be a domain can be restated as $(a+I)(b+I) = 0+I \implies a+I = 0+I$ or $b+I = 0+I$. This is precisely the condition for I to be a prime ideal.
- (b): If R/I is a field, then the only proper ideal of R/I is $0+I$. Using the correspondence between ideals in the quotient ring and ideals $I \subset J \subset R$ we see that there is no proper ideal properly containing I, hence I is maximal. Conversely, if I is maximal ideal, then R/I has only two ideals: zero ideal and R/I. Such a ring is necessarily a field.

Example: prime and maximal ideals in $k[x_1, \ldots, x_n]$

- If f is an irreducible polynomial, then (f) is a prime ideal. This is because $k[x_1, \ldots, x_n]$ is a unique factorization domain: if $ab \in (f)$, so that $ab = fg$, then f divides a or b.
- Conversely, if $I = (f)$ is prime, then f is irreducible
- Ideals $(x_1, \ldots, x_j)$, $j \leq n$ are prime. Consider the quotient ring:

  $$k[x_1, \ldots, x_n]/(x_1, \ldots, x_j) \simeq k[x_{j+1}, \ldots, x_n].$$

  This is a domain, hence $(x_1, \ldots, x_j)$ are prime.
- The ideal $(x_1, \ldots, x_n)$ is maximal. Consider the quotient ring:

  $$k[x_1, \ldots, x_n]/(x_1, \ldots, x_n) \simeq k.$$

  This is a field, hence $(x_1, \ldots, x_n)$ is maximal.

Prime and maximal ideals of quotient rings

Proposition

Let $I \subset R$ be an ideal. In the bijection between ideals in R/I and intermediate ideals $I \subset J \subset R$ prime (resp. maximal) ideals correspond to prime (resp. maximal) ideals.

Proof.

- Let $\overline{J}$ be an ideal of R/I corresponding to an ideal $I \subset J \subset R$ This means $\phi^{-1}(\overline{J}) = J$ and $\phi(J) = J/I = \overline{J}$ for $\phi : R \to R/I$.
- Consider $S = (R/I)/\overline{J} = (R/I)/(J/I) \simeq R/J$ (third isomorphism theorem)
- Now $\overline{J}$ is prime (resp. maximal) iff S is a domain (resp. a field) iff J is prime (resp. maximal)

Contraction of prime ideals

Lemma

Let $\phi : R \to S$ be a ring homomorphism. If $P \subset S$ is a prime ideal, so is $\phi^{-1}(P) \subset R$.

The proof is easy from definitions.

Remark

Note that preimages of maximal ideals are usually not maximal. For instance, consider $\mathbb{Z} \subset \mathbb{Q}$. Then 0 is a maximal ideal of $\mathbb{Q}$ but its intersection with $\mathbb{Z}$, also 0 is not maximal in $\mathbb{Z}$.

Existence of maximal ideals

Theorem

Any proper ideal I in a ring R is contained in a maximal ideal.

Proof.

- Let $\mathcal{S}$ be the set of all proper ideals of R which contain a given ideal I. $\mathcal{S}$ is partially ordered set with respect to inclusion.
- To prove that $\mathcal{S}$ has a maximal element we invoke **Zorn's Lemma,** one of the equivalent forms of the Axiom of Choice
- Zorn's Lemma says that if in a nonempty partially ordered set $\mathcal{S}$ every totally ordered subset has an upper bound, then $\mathcal{S}$ has a maximal element.
- Given any totally ordered subset $\mathcal{A} \subseteq \mathcal{S}$ (i.e., for any $J, K \in \mathcal{A}$, $J \subseteq K$ or $K \subseteq J$) denote with $I_{\mathcal{A}}$ the union of all the ideals in $\mathcal{A}$. $I_{\mathcal{A}}$ is also a proper ideal.
- Hence $\mathcal{S}$ satisfies the conditions of Zorn's Lemma, and $\mathcal{S}$ has a maximal element, which is by definition a maximal ideal of R.

□

Local rings

Definition

A **local ring** R is a ring that has a unique maximal ideal m.

This terminology comes from the fact that in algebraic geometry maximal ideals correspond to closed points of an algebraic variety. Hence a local ring corresponds to a variety with one closed point.

Example

Any field k is a local ring as its unique maximal ideal is (0).

Example

The rings $\mathbb{Z}/(p^n)$, $k[x]/(x^2)$ are local rings, whereas $\mathbb{Z}$ and $k[x]$ are not local.

There is a procedure of making local rings from a given ring R, known as localization. We study localization later in this course.

The Nilradical and Jacobson radical

Definition

Let R be a ring. We define

(a) The **Nilradical** of R to be the intersection of all prime ideals in R:

$$\text{Nil}(R) = \bigcap_{P \subset R} P$$

(b) The **Jacobson radical** of R to be the intersection of all maximal ideals in R:

$$J(R) = \bigcap_{m \subset R} m$$

Both $\text{Nil}(R)$ and $J(R)$ are ideals of R (as they are intersections of ideals). Since every maximal ideal is prime, we have $Nil(R) \subset J(R)$.

Explicit characterization of Nil(R)

Theorem

We have $a \in \mathrm{Nil}(R)$ if and only if a is nilpotent, that is $a^n = 0$ for some $n \geq 1$.

Proof begins:

- Let us first prove that if a is nilpotent, then $a \in \mathrm{Nil}(R)$
- If $a^n = 0$, then for every prime ideal we have $a \in P$ (because $0 = a^n \in P$), so $a \in \mathrm{Nil}(R)$.

...

Proof ends:

- Now let us prove that if $a \in \mathrm{Nil}(R)$, then a is nilpotent
- Assume that $a^n \neq 0$ for all $n \geq 1$.
- Let $\mathcal{S} = \{I \subset R \mid I \text{ is an ideal and } a^n \notin I \text{ for all } n \geq 1\}$. Note that $\mathcal{S}$ is not empty because it contains the zero ideal.
- As in the proof of existence of maximal ideals, Zorn's Lemma implies that $\mathcal{S}$ contains a maximal element P. It suffices to check that P is prime.
- Assume $a, b \notin P$ but $ab \in P$. Then $P + (a), P + (b)$ properly contain P.
- Since P is maximal in $\mathcal{S}$, $P + (a)$ and $P + (b)$ don't belong to $\mathcal{S}$, so that we have $r^n \in P + (a)$, $r^m \in P + (b)$.
- Multiplying yields $r^{n+m} \in (P + (a))(P + (b)) = P + (ab) = P$, a contradiction!

□

Definition

A ring R is called **reduced** if $\mathrm{Nil}(R) = 0$, i.e. if the only nilpotent element in R is zero.

The radical

Definition

For an ideal $I \subset R$ we define the **radical of** I to be

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}.$$

Lemma

$\sqrt{I}$ is an ideal containing I.

Proof.

- The inclusion $I \subset \sqrt{I}$ is obvious. Let us show that $\sqrt{I}$ is an ideal.
- Let $a \in \sqrt{I}, b \in R$. Then $a^n \in I$ for some $n \geq 1$ and $(ra)^n \in I$, so that $ra \in \sqrt{I}$.
- Now let $a, b \in \sqrt{I}$ so that $a^n, b^n \in I$ (can take the larger of the two exponents). We have $(a+b)^{2n} = \sum_{i+j=2n} \binom{2n}{i} a^i b^j \in I$ since for each term $i \geq n$ or $j \geq n$.

Proposition

$\sqrt{I}$ is the intersection of all prime ideals which contain I.

Proof.

- We consider the quotient ring R/I and employ the bijection between ideals in R/I and intermediate ideals in R
- Under this bijection the nilradical $\sqrt{(\overline{0})} = \mathrm{Nil}(R/I)$ corresponds to $\sqrt{I}$: $\phi^{-1}(\mathrm{Nil}(R/I)) = \sqrt{I}$.
- We have

$$\sqrt{I} = \phi^{-1}\Big(\bigcap_{\overline{P}\subset R/I} \overline{P}\Big) = \bigcap_{\overline{P}\subset R/I} \phi^{-1}(\overline{P}) = \bigcap_{I\subset P\subset R} P.$$

□

Definition

An ideal $I \subset R$ is called a **radical ideal** if $\sqrt{I} = I$.

For instance, a prime ideal is radical.

Proposition

I is a radical ideal if and only if R/I is a reduced.

Proof.

- We use the bijection between ideals in R/I and intermediate ideals in R
- It gives us $I = \sqrt{I} \subset R \iff \overline{0} = \mathrm{Nil}(R/I) \subset R/I$
- Thus I is a radical ideal iff R/I is a reduced ring.

□

Example

Let $I = (x^2) \subset k[x]$. Then $\sqrt{I} = (x)$, so I is not a radical ideal. Also, $k[x]/I = k[x]/(x^2)$ has Nilradical $\mathrm{Nil}(k[x]/(x^2)) = (\overline{x})$, so $k[x]/(x^2)$ is not reduced.

Definition

Let R be a ring. An R-**module** (or a **module over** R) is an abelian group $(M, +)$ together with the map $R \times M \to M$ whose values for $r \in R$ and $m \in M$ are denoted with $(r, m) \mapsto r \cdot m$ (or just $(r, m) \mapsto rm$) which has the following properties:

(a) $1_R \cdot m = m$,

(b) $(rs) \cdot m = r \cdot (s \cdot m)$,

(c) $(r + s) \cdot m = r \cdot m + s \cdot m$,

(d) $r \cdot (m + n) = r \cdot m + r \cdot n$

for all $r, s \in R$ and $m, n \in M$.

We refer to the map $R \times M \to M$ as the action of R on M.

Examples

Example

Let k be a field; k-modules are precisely the k-vector spaces.

Example

A $\mathbb{Z}$-module is simply an abelian group. Indeed, if A is an abelian group then $\mathbb{Z}$ acts on M in an obvious way: $(n, a) \mapsto \underbrace{a + \cdots + a}_{n}$.

Example

The Abelian group with one element 0 is a module over any ring; we call this the zero module and denote it with 0.

Example

Any ring R is an R-module, and furthermore any ideal $I \subset R$ is an R-module.

Example

Let $I \subset R$ be an ideal. Then the quotient ring R/I is an R-module via the operation $r \cdot (s + I) = rs + I$.

Direct sums and products

Let R be a ring, let Λ be a set and let M_λ be an R-module for every $\lambda \in \Lambda$.

Definition

The **direct product** of $\{M_\lambda\}_{\lambda\in\Lambda}$, denoted $\prod_{\lambda\in\Lambda} M_\lambda$ consists of all sequences $(m_\lambda \in M_\lambda)_{\lambda\in\Lambda}$, with operations
$(m_\lambda)_{\lambda\in\Lambda} + (n_\lambda)_{\lambda\in\Lambda} = (m_\lambda + n_\lambda)_{\lambda\in\Lambda}$, $r(m_\lambda)_{\lambda\in\Lambda} = (rm_\lambda)_{\lambda\in\Lambda}$.

Definition

The **direct sum** $\bigoplus_{\lambda\in\Lambda} M_\lambda$ of $\{M_\lambda\}_{\lambda\in\Lambda}$ is the subset of $\prod_{\lambda\in\Lambda} M_\lambda$ consisting of sequences where all but finitely many m_λ are equal to zero. The operations in the direct sum are the same as in the direct product.

$\bigoplus_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$ if Λ is finite but not in general. For instance the infinite vector dimensional space k^∞ is ambiguous. It could either mean $\prod_{n\in\mathbb{N}} k$ (all sequences) or $\bigoplus_{n\in\mathbb{N}} k$ (sequences where only finitely many entries are nonzero).

Homomorphisms of R-modules

Definition

Let R be a ring and let M and N be R-modules. A map $\phi : M \to N$ is a **homomorphism of R-modules** if ϕ is a homomorphism of abelian groups which commutes with R-action. In other words we require:

(a) for all $m_1, m_2 \in M$, $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$,

(b) for all $r \in R$ and $m \in M$, $\phi(rm) = r\phi(m)$.

Definition

A homomorphism of R-modules $\phi : M \to N$ is a **isomorphism** of R-modules if it is injective and surjective.

Examples

Example

If k is a field, then k-module homomorphisms are linear maps between vector spaces.

Example

$\mathbb{Z}$-module homomorphisms are precisely homomorphisms of abelian groups.

Example

Let R be a ring and let $I \subseteq R$ be an ideal. The quotient map $R \to R/I$ is an R-module homomorphism.

Example

Let R be a ring and let M be a R-module. For any $r \in R$ the map $\mu_r : M \to M$ defined by $\mu_r(m) = rm$ for all $m \in M$ is an R-module homomorphism.

Submodules

Definition

Let R be a ring and let M be an R-module. A subset $N \subseteq M$ is an R-**submodule of** M if N is closed under addition and under the action of R.

Remark

If $N \subseteq M$ is a R-submodule of M, then the inclusion map is a homomorphism of R-modules.

Example

Submodules of k-vector spaces (considered as k-modules) are vector subspaces.

Example

Submodules of abelian groups (considered as $\mathbb{Z}$-modules) are subgroups.

Construction of submodules

Example

Let M be an R-module. Let Λ be a set and let $M_\lambda \subseteq M$ be an R-submodule for every $\lambda \in \Lambda$. Then $\cap_{\lambda\in\Lambda} M_\lambda$ (the intersection) and $\sum_{\lambda\in\Lambda} M_\lambda$ (consists of finite sums $m_1 + \cdots + m_k$) are submodules of M.

Example

Let R be a ring, let $I \subseteq R$ be an ideal and let M be an R-module. $IM = \{a_1 m_1 + \cdots + a_s m_s | s \geq 0,\ a_1, \ldots, a_s \in I,\ m_1, \ldots, m_s \in M\}$ is a submodule of M.

Proposition

Let R be a ring, let M and N be R-modules and let $\phi : M \to N$ be a homomorphism of R-modules. The **kernel** *of ϕ, denoted* $\ker\phi$*, defined as $\{m \in M \,|\, \phi(m) = 0\}$, is an R-submodule of M. The* **image** *of ϕ, denoted* $\mathrm{Im}\,\phi$*, is an R-submodule of N.*

Proof is an easy exercise.

Quotients of modules

Definition

Let R be a ring, let M be an R-module and let $N \subseteq M$ be a submodule. We define a new R module, the **quotient of M by N** as follows: as an Abelian group it is the quotient group of the Abelian group M by the (normal) subgroup N and for each $r \in R$ and each coset $m+N$ we define $r \cdot (m+N)$ to be the coset $rm+N$.

The map $\phi : M \to M/N$ given by $\phi(m) = m+N$ is a homomorphism of R-modules and we refer to it as the **quotient homomorphism**.

Example

This generalizes quotient vector spaces ($R = k$) and quotient abelian groups ($R = \mathbb{Z}$).

Example

If $I \subset R$ is an ideal, then the two possible ways of forming quotient R/I as R-module are the same! (Do you see what are the two ways?)

Submodules of the quotient module

Exercise

Recall the three isomorphism theorems for groups and generalize them to R-modules.

Proposition

Let R be a ring, let M be an R-module and let $N \subseteq M$ be a submodule. There is a bijection:

$$\{\textit{Submodules } \overline{K} \subset M/N\} \leftrightarrow \{\textit{Intermediate submodules } N \subset K \subset M\}$$

given by $\overline{K} \to \phi^{-1}(\overline{K})$ and $K \mapsto \phi(K)$ where $\phi : M \to M/N$ is the quotient homomorphism.

Proof is a straightforward exercise.

Exercise

Use the proposition to describe subgroups of $\mathbb{Z}/(12)$.

Free modules

Definition

An R-module M isomorphic to $\oplus_{\lambda\in\Lambda} R$ (for any set Λ) is called a **free module**. If Λ is finite, that is if M is isomorphic to R^n, then M is called a **finitely generated free module**.

Remark

The cardinality of Λ is called the rank of the free module $\oplus_{\lambda\in\Lambda} R$. It is not obvious that the rank is well-defined (e.g. think why $R^2 \simeq R^3$ is impossible).

Example

Every k-vector space has a basis (this is a form of Zorn's Lemma or Axiom of Choice), hence every k-module is free.

Example

Let $n \in \mathbb{N}$. Then $n\mathbb{Z} \subset \mathbb{Z}$ is a free $\mathbb{Z}$-module, but $\mathbb{Z}/(n)$ is not a free $\mathbb{Z}$-module.

Finitely generated modules

Definition

Let R be a ring, let M be an R-module and let $m_1, \ldots, m_n \in M$. The **submodule generated by** $m_1, \ldots, m_n$ is

$$\langle m_1, \ldots, m_n \rangle = Rm_1 + \cdots + Rm_n = \{r_1 m_1 + \cdots + r_n m_r,\ r_i \in R\}.$$

This is the smallest submodule of M which contains $m_1, \ldots, m_r$.

Definition

The R-module M is **finitely generated** if there exists a finite set of generators: $M = \langle m_1, \ldots, m_n \rangle$ for some $m_i \in M$.

Proposition

An R-module M is finitely generated if and only if M is quotient of a finitely generated free R-module.

The proof is a straightforward exercise.

Exact sequences

Definition

(a) Let L, M, N be R-modules and let $f : L \to M$ and $g : M \to N$ be homomorphisms of R-modules. We say that the sequence $L \xrightarrow{f} M \xrightarrow{g} N$ is **exact** if $\ker g = \operatorname{Im} f$.

(b) A **short exact sequence** is an exact sequence of the form $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$. Notice that this implies that f is injective and that g is surjective.

(c) A sequence of R-modules and homomorphisms

$$\ldots M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_i} \ldots$$

is a **long exact sequence** if, for all i for which f_i and f_{i-1} are in the sequence, $\ker f_i = \operatorname{Im} f_{i-1}$.

Example

Let R be a ring, let M be an R-module and let N be an R-submodule of M. We have an exact sequence

$$0 \to N \xrightarrow{i} M \xrightarrow{g} M/N \to 0$$

where i is the inclusion map and g is the quotient map.

Example

The sequence $0 \to L \xrightarrow{f} M$ is exact if and only if f is injective. The sequence $M \xrightarrow{g} N \to 0$ is exact if and only if g is surjective.

The Jacobson radical

Let R be a ring. Recall that the **Jacobson radical** $J(R)$ of R is the intersection of all its maximal ideals. For instance if R is a local ring with maximal ideal m, then $J(R) = m$.

Proposition

For any element $a \in J(R)$, $1 - a$ is a unit.

Proof.

- Let $a \in J$ and assume that $1 - a$ is not a unit
- Then $1 - a \in m$ for some maximal ideal $m \subset R$
- We also have $a \in J(R) \subset m$
- Now $1 = a + (1 - a) \in m$, contradiction!

Nakayama's Lemma

Nakayama's Lemma is one of the first nontrivial technical results in commutative algebra. We give several forms of the statement.

Theorem (Nakayama's Lemma, I)

Let R be a ring, let M be a finitely generated R-module and let $I \subset R$ be an ideal contained in the Jacobson radical $J(R)$. If $IM = M$ then $M = 0$.

Proof.

- Assume that $M \neq 0$ and let $m_1, \ldots, m_n$ $(n \geq 1)$ be a minimal set of generators of M.
- Since $M = IM$, we can write $m_n = a_1 m_1 + \cdots + a_n m_n$ with $a_i \in I$.
- Rewrite the equation as $(1 - a_1)m_n = a_1 m_1 + \cdots + a_{n-1} m_{n-1}$
- $1 - a_1$ is a unit (Lemma above) hence $m_n \in \langle m_1, \ldots, m_{n-1} \rangle$
- This contradicts to minimality of $m_1, \ldots, m_n$.

Corollary (Nakayama's Lemma, II)

Let R be a ring, let $I \subset R$ be an ideal contained in the Jacobson radical $J(R)$, let M be a finitely generated R-module and let $N \subseteq M$ be a submodule. If $M = N + IM$ then $M = N$.

Proof.

- We apply Nakayama's Lemma I to M/N
- We have $M/N = (N + IM)/N = I(M/N) \implies M/N = 0$
- Hence $M = N$.

□

We next specify how Nakayama's Lemma works for local rings. Let R be a local ring with maximal ideal m and let $k = R/m$ be the quotient field. Note that if M is an R-module, then M/mM is not only R-module, but also R/m-module (since m acts trivially), hence M/mM is actually a k-vector space.

Corollary (Nakayama's Lemma, III)

Let (R, m) be a local ring with quotient field $k = R/m$ and let M be a finitely generated R-module. Let $m_1, \ldots, m_n$. The following conditions are equivalent:

(a) *$m_1, \ldots, m_n$ generate M*

(b) *The images $\overline{m_1}, \ldots, \overline{m_n} \in M/mM$ generate M/mM as a k-vector space.*

Proof.

- $(a) \implies (b)$: If $m_1, \ldots, m_n$ generate M as R-module, then their images $\overline{m_1}, \ldots, \overline{m_n}$ generate M/mM as R/m-module, hence M/mM is finite dimensional k-vector space.
- $(b) \implies (a)$: Let $N = \langle m_1, \ldots m_n \rangle \subset M$. Since $\overline{m_1}, \ldots, \overline{m_n} \in M/mM$ generate M/mM we have $N + mM = M$
- Nakayama's Lemma II implies $N = M$, so that $m_1, \ldots, m_n$ generate M

Bilinear maps

Definition

Let M, N, K be R-modules. A map $f : M \times N \to K$ is called R-**bilinear** if f is an homomorphism of R-modules in both variables, that is if

$$f(rm_1 + m_2, n) = rf(m_1, n) + f(m_2, n)$$

for all $r \in R$, $m_1, m_2 \in M$, $n \in N$ and

$$f(m, rn_1 + n_2) = rf(m, n_1) + f(m, n_2)$$

for all $r \in R$, $n_1, n_2 \in N$, $m \in M$.

Example

Let $A = (a_{ij})$ be a symmetric $n \times n$ matrix with real coefficients. The map $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ given by $(\underline{x}, \underline{y}) \mapsto \sum_{i,j=1}^{n} a_{ij} x_i y_j$ is an $\mathbb{R}$-bilinear map. Note that in physics or applied mathematics one refers to A as a symmetric tensor.

Construction of $M \otimes_R N$

Let M, N be two R-modules. We define the following modules:

- $F(M, N)$ be the free R-module with basis given by symbols $m \otimes n$ for $m \in M$, $n \in N$:

$$F(M, N) = \bigoplus_{m \in M, n \in N} R \cdot m \otimes n.$$

  The R-module is very large, e.g. if M or N is uncountable as a set, then $F(M, N)$ has an uncountable basis.

- $B(M, N) \subset F(M, N)$ submodule generated by relations:

$$\begin{aligned} (m_1 + rm_2) \otimes n - m_1 \otimes n - rm_2 \otimes n, \\ m \otimes (n_1 + rn_2) - m \otimes n_1 - rm \otimes n_2. \end{aligned} \tag{1}$$

- The tensor product $M \otimes_R N$ is the R-module defined as a quotient $F(M, N)/B(M, N)$

Tensor product explained

Thus elements of $M \otimes_R N$ have the form $\sum_{i=1}^{k} m_i \otimes n_i$ for $m_i \in M$, $n_i \in N$, and there are relations $(m_1 + rm_2) \otimes n = m_1 \otimes n + rm_2 \otimes n$, $m \otimes (n_1 + rn_2) = m \otimes n_1 + rm \otimes n_2$.

For example

$$(2m) \otimes n = m \otimes n + m \otimes n = m \otimes (2n).$$

Elements of the kind $m \otimes n$ are called **decomposable tensors**. By construction decomposable tensors generate $M \otimes_R N$. In general there is no simple way to tell whether two elements of a tensor product are equal.

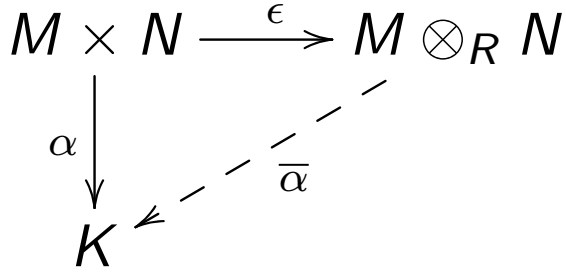
If the base ring R is fixed, we write $M \otimes N$ for $M \otimes_R N$.

Bilinear map ϵ and its universal property

We define $\epsilon : M \times N \to M \otimes N$ by $\epsilon(m, n) = m \otimes n$. Note that ϵ is bilinear by construction, because we quotiented out the relations $B(M, N)$. Now we prove the universal property of $(M \otimes N, \epsilon)$:

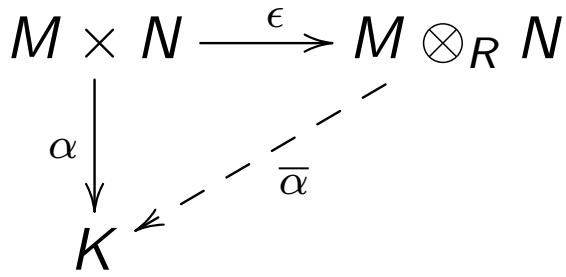
Theorem

For any R-bilinear map $\alpha : M \times N \to K$ there is a unique R-module homomorphism $\overline{\alpha} : M \otimes_R N$ satisfying $\overline{\alpha} \circ \epsilon = \alpha$:



In other words $M \otimes_R N$ is the smallest module which is a recipient of a bilinear map from $M \times N$. Using terminology from Category Theory tensor product is the initial object in the category of bilinear maps $M \times N \to K$.

Proof of the universal property



Proof.

- Uniqueness: we require $\overline{\alpha}(m \otimes n) = \overline{\alpha}(\epsilon(m, n)) = \alpha(m, n)$, hence values of $\overline{\alpha}$ on decomposable tensors are determined. Decomposable tensors generate $M \otimes N$, hence $\overline{\alpha}$ is unique (if exists).
- Existence: since $M \otimes N = F(M, N)/B(M, N)$ to define an R-module homomorphism $M \otimes N \to K$ we need to define a homomorphism $F(M, N) \to K$ which has $B(M, N)$ in its kernel
- We set $\overline{\alpha}(m \otimes n) = \alpha(m, n)$ and see that it defines an R-module homomorphism satisfying all the conditions.

□

Examples of tensor products

Lemma

If $m_1, \ldots, m_k$, $n_1, \ldots n_l$ generate R-modules M and N respectively, then $m_i \otimes n_j$ generate $M \otimes N$.

Proof.

Follows from the construction of $M \otimes N$: every tensor can be written as a combination of decomposable tensors, which in turn can be written as combinations of $m_i \otimes n_j$. □

Example

Let p, q be distinct primes. We have $\mathbb{Z}/(p) \otimes_{\mathbb{Z}} \mathbb{Z}/(q) = 0$. To see this, solve $px \equiv 1 \mod q$ and consider

$$\overline{1} \otimes \overline{1} = \overline{1} \otimes \overline{px} = \overline{p} \otimes \overline{x} = \overline{0} \otimes \overline{x} = 0,$$

and it follows that all tensors in $\mathbb{Z}/(p) \otimes \mathbb{Z}/(q)$ are zero.

Properties of tensor products

Proposition

If $R = k$, a field, and V and W are k-vector spaces with bases $V = \langle e_i \rangle_{i \in I}$, $W = \langle f_j \rangle_{j \in J}$, then $V \otimes_k W$ is a k-vector space with basis $e_i \otimes f_j$, $i \in I$, $j \in J$. In particular, we have

$$\dim_k(V \otimes W) = \dim_k(V) \cdot \dim_k(W)$$

in the case dimensions of V and W are finite.

Proposition

$$\begin{aligned} M \otimes_R N &\simeq N \otimes_R M \\ (M \oplus N) \otimes_R L &\simeq (M \otimes_R L) \oplus (N \otimes_R L) \\ (M \otimes_R N) \otimes_R L &\simeq M \otimes_R (N \otimes_R L) \\ R \otimes_R M &\simeq M \end{aligned}$$

Proofs rely on the universal property of the tensor products and are left to exercises.

Multiplicative sets

Definition

Let R be a ring. A subset $U \subset R$ is called a **multiplicative set** if

(a) $1 \in U$

(b) $a, b \in U \implies ab \in U$

Here are two main examples:

Example

Let $a \in R$ be a nonzero element. Then the set of powers $U = \{a^n\}_{n=0}^{\infty}$ is a multiplicative set.

Example

Let $P \subset R$ be a prime ideal. Then the complement $U = R \setminus P$ is a multiplicative set. Indeed, P is a proper ideal so $1 \notin P$ hence $1 \in U$ and $a, b \notin P \implies ab \notin P$.

Localization introduced

Given a multiplicative set $U \subset R$ we are going to define **localization of R with respect to U.** denoted $U^{-1}R$. By definition we put

$$U^{-1}R = R \times U/\sim,$$

where elements in $R \times U$ are written in the form $\frac{r}{u}$, $r \in R$, $u \in U$ and the equivalence relation $\sim$ is defined as

$$\frac{r}{u} \sim \frac{r'}{u'} \iff s(ru' - r'u) = 0 \text{ for some } s \in U.$$

Thus elements $\frac{r}{u}$ can be thought as "fractions".

Localization of rings

Theorem

Let $U \subset R$ be a multiplicative set.

(a) *The relation $\sim$ defined above is an equivalence relation.*

(b) *The operations*

$$\frac{r_1}{u_1} + \frac{r_2}{u_2} = \frac{r_1 u_2 + r_2 u_1}{u_1 u_2}$$
$$\frac{r_1}{u_1} \cdot \frac{r_2}{u_2} = \frac{r_1 r_2}{u_1 u_2}$$

on $U^{-1}R$ are well defined, and $U^{-1}R$ forms a ring with $0 = \frac{0}{1}$, $1 = \frac{1}{1}$.

Proof is a nice long exercise.

Example: field of fractions

Exercise

The set of non zero-divisors of R is a multiplicative set. Furthermore, R is an integral domain if and only if $R \setminus \{0\}$ is a multiplicative set.

Let R be a domain, and let $U = R \setminus \{0\}$. Let $F = U^{-1}R$. Then F is a field, because every nonzero element $\frac{r}{u}$ ($r \neq 0$, $u \neq 0$) has an inverse

$$\frac{r}{u} \cdot \frac{u}{r} = \frac{1}{1} = 1$$

The field F is called the **fraction field** of R.

Example

$\mathbb{Q}$ is the fraction field of $\mathbb{Z}$ and the fraction field of $k[x]$ is the field of rational functions in one variable:

$$k(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x], g(x) \neq 0 \right\}.$$

Universal property of localization

Theorem

Let R be a ring and let $U \subseteq R$ be a multiplicative set.

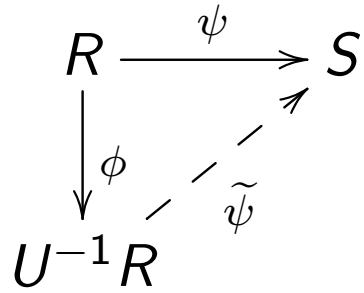
(a) *The map $\phi : R \to U^{-1}R$, $r \mapsto \frac{r}{1}$ is a ring homomorphism and $\phi(U)$ consists of units.*

(b) *For any ring homomorphism $\psi : R \to S$ satisfying the property that $\psi(U) \subset S$ consists of units, there exists a unique ring homomorphism $\widetilde{\psi} : U^{-1}R \to S$ such that $\psi = \widetilde{\psi} \circ \phi$*

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \downarrow{\scriptstyle \phi} & \nearrow{\scriptstyle \widetilde{\psi}} & \\ U^{-1}R & & \end{array} \qquad (1)$$

Thus, $U^{-1}R$ is the "smallest" way to extend R so that all elements of U are units.

Proof of the Universal Property



Proof.

- (a) is straightforward
- (b) Uniqueness: we require $\widetilde{\psi}(\phi(r)) = \psi(r)$, so that we know $\widetilde{\psi}(\frac{r}{1}) = \psi(r)$. This determines all values $\widetilde{\psi}\left(\frac{r}{u}\right)$ as $\frac{r}{u} = \frac{r}{1} \cdot \left(\frac{u}{1}\right)^{-1}$ so we must have $\widetilde{\psi}(\frac{r}{u}) = \psi(r)\psi(u)^{-1}$.
- (b) Existence: we set $\widetilde{\psi}(\frac{r}{u}) = \psi(r)\psi(u)^{-1} \in S$ and check that it is well-defined: if $\frac{r}{u} = \frac{r'}{u'}$, then $s(ru' - r'u) = 0$ for some $s \in U$, so that $\psi(s)(\psi(r)\psi(u') - \psi(r')\psi(u)) = 0$ which implies $\psi(r)\psi(u') = \psi(r')\psi(u)$, hence $\psi(r)\psi(u)^{-1} = \psi(r')\psi(u')^{-1}$.

□

Localization with respect to an element

Let $a \in R$ be a nonzero element and consider the multiplicative set

$$U = \{1, a, a^2, \dots\}.$$

The localization $U^{-1}R$ consists of fractions $\frac{r}{a^n}$, and the universal property says that $U^{-1}R$ is the smallest ring where a (and hence all its powers) is invertible. Thus we sometimes use the notation $U^{-1}R = R[a^{-1}]$.

If we'd like to invert several nonzero elements $a_1, \dots, a_n \in R$, then a useful trick is to consider $R[(a_1 \cdots a_n)^{-1}]$.

Localization with respect to the complement of a prime

Definition

Let $P \subset R$ be a prime ideal. The localization of R at P, denoted R_P, is the localization of R at the multiplicative set $U = R \setminus P$.

Example

In number theory we would sometimes want to work with a specific prime number rather than all primes at once, and for a prime $p \in \mathbb{Z}$ we may consider

$$\mathbb{Z}_{(p)} = \{\frac{n}{m},\ p \text{ does not divide } m\} \subset \mathbb{Q}.$$

Note that all primes $q \neq p$ become invertible in $\mathbb{Z}_{(p)}$.

This is the general phenomenon: R_P has only one maximal ideal.

Localization and local rings

Recall that a ring is local if it has a unique maximal ideal.

Proposition

Let $P \subset R$ be a prime ideal. The ring R_P is local with maximal ideal $PR_P = \{\frac{r}{u} \mid r \in P, u \notin P\}$, the expansion of P to R_P.

Proof.

- PR_P is a proper ideal: if $1 = \frac{1}{1} = \frac{r}{u} \in PR_P$, then $s(u - r) = 0$ for some $r \in P$, $s, u \notin U$ which leads to a contradiction
- Any element $\frac{s}{v} \in R_P \setminus PR_P$ is a unit (its inverse is $\frac{v}{s}$)
- Hence PR_P is a maximal ideal: every strictly bigger ideal is R_P

□

Ideals under localization

There is an analogy between quotient rings and localization. Let $U \subset R$ be a multiplicative set. Let us consider contraction and expansion of ideals under the localization map $\phi : R \to U^{-1}R$:

- Given a proper ideal $J \subset U^{-1}R$ we consider $I = \phi^{-1}(J) \subset R$, note that $I \cap U = \emptyset$ (otherwise if $u \in I$, then J contains a unit $\phi(u)$ and is not proper).
- Given an ideal $I \subset R$ we consider $U^{-1}I = \{\frac{r}{u} : r \in I, u \in U\}$.

This gives correspondence (but not a bijection):

$\{$Proper ideals of $U^{-1}R\} \leftrightarrow \{$Ideals of R which do not intersect $U\}$.

Theorem

(a) *Every ideal $J \subseteq U^{-1}R$ is expansion of its contraction, that is $J = U^{-1}(\phi^{-1}(J))$.*

(b) *For an ideal $I \subset R$ the contraction of its expansion is the so-called* **saturation of I with respect to U:**

$$\phi^{-1}(U^{-1}I) = \{r \in R : ru \in I \text{ for some } u \in U\} \supset I.$$

Proof.

- (a) By definition $\phi^{-1}(J) = \left\{r \in R : \frac{r}{1} \in J\right\}$.
- Now we have $\frac{r}{s} \in J \iff \frac{r}{1} \in J \iff r \in \phi^{-1}(J)$ This means that $J = U^{-1}(\phi^{-1}(J)$.
- (b) We have $\phi^{-1}(U^{-1}I) = \left\{r \in R : \frac{r}{1} = \frac{i}{u}, u \in U, i \in I\right\}$
- We rewrite the condition $\frac{r}{1} = \frac{i}{u}$ as $s(ru - i) = 0$, that is $ru' = i'$ for some $u' \in U$, $i' \in I$ and see that $\phi^{-1}(U^{-1}I)$ is the saturation of I with respect to U.

□

Definition

An ideal $I \subset R$ is called **saturated** with respect to multiplicative set U if I is equal to its saturation, i.e. if

$$sr \in I, s \in U \implies r \in I.$$

Note that prime ideal P is saturated with respect to U as soon as $U \cap P = \emptyset$.

Prime ideals under localization

Theorem

Expansion and contraction of ideals with respect to localization map $\phi : R \to U^{-1}R$ establish mutually inverse bijections:

$$\{\textit{Primes } Q \subset U^{-1}R\} \leftrightarrow \{\textit{Primes } P \subset R \textit{ such that } P \cap U = \emptyset\}.$$

Proof.

- We know that contraction of a prime ideal is prime.
- Let us show that for a prime $P \subset R$ such that $P \cap U = \emptyset$ its expansion $U^{-1}P \subset U^{-1}R$ is prime.
- Assume that $\frac{r_1}{u_1} \cdot \frac{r_2}{u_2} = \frac{r_1 r_2}{u_1 u_2} = \frac{p}{u_3} \in U^{-1}P$. This means $s(u_3 r_1 r_2 - p u_1 u_2) = 0$, hence $s u_3 r_1 r_2 \in P$, and so $r_1 r_2 \in P$, which implies $r_1 \in P$ or $r_2 \in P$. Therefore $U^{-1}P$ is prime.
- $U^{-1}\phi^{-1}(Q) = Q$ (this holds for all ideals $J \subset U^{-1}R$).
- $\phi^{-1}(U^{-1}P) = P$ (this holds for saturated ideals $I \subset R$, and prime ideals satisfying $U \cap P = \emptyset$ are saturated).

Prime ideals in R_P

We apply the theorem above to $U = R \setminus P_0$, for a prime ideal P_0:

Corollary

Expansion and contraction of ideals with respect to localization map $\phi : R \to R_{P_0}$ establish mutually inverse bijections:

$$\{\textit{Primes } Q \subset U^{-1}R\} \leftrightarrow \{\textit{Primes } P \subseteq P_0 \subset R\}.$$

Example

Prime ideals in the ring $\mathbb{Z}_{(p)}$ correspond to prime ideals in $\mathbb{Z}$ which are contained in (p). There are two such ideals: (0), (p), so that $\mathbb{Z}_{(p)}$ is a ring with two prime ideals: (0) and $(\frac{p}{1})$.

Localization of modules

Given a multiplicative set $U \subset R$ and an R-module M we construct an **localization of M with respect to U**:

$$U^{-1}M = M \times U/\sim,$$

where elements of $M \times U$ are written as fractions $\frac{m}{u}$, $m \in M$, $u \in U$ and the equivalence relation is

$$\frac{m}{u} \sim \frac{m'}{u'} \iff s(mu' - m'u) = 0 \text{ for some } s \in U.$$

Example

If $I \subset R$ is an R-module, then the expansion $U^{-1}I \subset U^{-1}R$ is the same as localization of I considered as an R-module. Indeed, in both case we consider the same set of pairs under the same equivalence relation.

Theorem

Let $U \subset R$ be a multiplicative set.

(a) *The relation $\sim$ defined above is an equivalence relation.*

(b) *The operations*

$$\frac{m_1}{u_1} + \frac{m_2}{u_2} = \frac{m_1 u_2 + m_2 u_1}{u_1 u_2}$$

$$\frac{r}{u_1} \cdot \frac{m}{u_2} = \frac{rm}{u_1 u_2}$$

on $U^{-1}M$ are well defined, and make $U^{-1}M$ into an $U^{-1}R$-module.

Proof is analogous to the Theorem about localization of rings: it is a nice long exercise.

Localization of modules as a functor

Theorem

Let $U \subset R$ be a multiplicative set.

(a) *Let $\phi : M \to N$ be a homomorphism of R-modules. The map $U^{-1}(\phi) : U^{-1}M \to U^{-1}N$*

$$U^{-1}(\phi)\left(\frac{m}{u}\right) = \frac{\phi(m)}{u}$$

is a well-defined homomorphism of $U^{-1}R$-modules.

(b) *Let $L \xrightarrow{f} M \xrightarrow{g} N$ be an exact sequence of R-modules. Then $U^{-1}L \xrightarrow{U^{-1}f} U^{-1}M \xrightarrow{U^{-1}g} U^{-1}N$ is an exact sequence of $U^{-1}R$-modules*

Let $R - mod$ denote the category of R-modules. Using the language of category theory, $U^{-1} : R - mod \to R - mod$ is an **exact functor**: it maps objects to objects, homomorphisms to homomorphisms and exact sequences to exact sequences.

Corollary

Let $U \subset R$ be a multiplicative set, and $N \subset M$ be R-modules. Then $U^{-1}N$ is a submodule of $U^{-1}M$ and we have an isomorphism of $U^{-1}R$-modules

$$U^{-1}M/U^{-1}N \simeq U^{-1}(M/N).$$

Proof.

- Consider the short exact sequence $0 \to N \to M \to M/N \to 0$.
- Since localization is exact, we get an exact sequence $0 \to U^{-1}N \to U^{-1}M \to U^{-1}M/N \to 0$ (note that localization of the zero module is obviously a zero module).
- This precisely means that $U^{-1}M/U^{-1}N \simeq U^{-1}M/N$.

□

Extension and restriction of scalars

If $f : R \to S$ is a ring homomorphism, we can define pullback and pushforward operations on modules as follows:

- If N is an S-module, we can consider it also as R-module via $r \cdot n := f(r)n$. One easily sees that all axioms are satisfied. N considered as R-module is called **restriction of scalars** of N. Restriction of scalars is a functor: if $N \to N'$ is a homomorphism of S-modules, then it is also a homomorphism of R-modules.
- If M is an R-module we consider the tensor product

$$S \otimes_R M,$$

with S-action given by $s' \cdot (s \otimes m) = ss' \otimes m$. One checks that the action is well-defined and gives an S-module structure to $S \otimes_R M$. $S \otimes_R M$ is called the **extension of scalars** of M. Extension of scalars is a functor: if $M \to M'$ is a homomorphism of R-modules, there is a corresponding homomorphism $S \otimes_R M \to S \otimes_R M'$ of S-modules.

Example

Example

Consider rings $\mathbb{R} \subset \mathbb{C}$. If W is a $\mathbb{C}$-vector space, then W considered as $\mathbb{R}$-vector is the restriction of scalars. If V is an $\mathbb{R}$-vector space, then its "complexification" $V \otimes_{\mathbb{R}} \mathbb{C}$ is the extension of scalars. Explicitly, if V has a basis $e_1, \ldots, e_n$ over $\mathbb{R}$, then $e_1 \otimes 1, \ldots, e_n \otimes 1$ is the basis of $\mathbb{C}$-vector space $V \otimes_{\mathbb{R}} \mathbb{C}$.

Example

Consider the quotient homomorphism $R \to R/I$. If M is an R-module, then the extension of scalars from R to R/I is

$$R/I \otimes_R M \simeq M/IM.$$

Indeed we can easily define mutually inverse homomorphisms between the two R/I-modules above (exercise!).

Localization of modules as extension of scalars

Theorem

Let $U \subset R$ be a multiplicative set and M be an R-module. Then we have an isomorphism of $U^{-1}R$-modules:

$$U^{-1}R \otimes_R M \simeq U^{-1}M.$$

given by $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$.

Proof.

- Since the map $(\frac{r}{s}, m) \mapsto \frac{rm}{s}$ is R-bilinear, the map given in the statement is a well-defined homomorphism of R-modules, and hence a homomorphism of $U^{-1}R$-modules as well
- We define the inverse homomorphism: $U^{-1}M \to U^{-1}R \otimes_R M$ via $\frac{m}{u} \mapsto \frac{1}{u} \otimes m$. This is well-defined: if $\frac{m}{u} = \frac{m'}{u'}$, then $s(mu' - m'u) = 0$, so that

$$\frac{1}{u} \otimes m = \frac{su'}{suu'} \otimes m = \frac{1}{suu'} \otimes su'm = \frac{1}{suu'} \otimes sum' = \frac{1}{u'} \otimes m'.$$

Tensor products are not exact

A big problem in commutative algebra is that extension of scalars (and more generally tensor products) are not exact. That is, if $R \to S$ is a ring homomorphism and $L \to M \to N$ an exact sequence of R-modules then the corresponding sequence $S \otimes_R L \to S \otimes_R M \to S \otimes_R N$ is not necessarily exact.

For instance, let $L = 0$, so that we have $0 \to M \to N$, i.e. $M \to N$ is an injective homomorphism. We then ask whether $S \otimes_R M \to S \otimes_R N$ is injective.

Example

Let $\mathbb{Z} \to \mathbb{Z}/(n)$ be the quotient homomorphism and let $f : \mathbb{Z} \to \mathbb{Z}$ be multiplication by n homomorphism $f(x) = nx$. f is clearly injective. Then $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(n) = \mathbb{Z}/(n)$ and we get a multiplication by n map

$$\mathbb{Z}/(n) \to \mathbb{Z}/(n)$$

which is also the zero-map, and it is not injective!

Flatness

Definition

A ring homomorphism $R \to S$ is called **flat** if for any exact sequence $L \to M \to N$ of R-modules the corresponding sequence of S-modules $S \otimes_R L \to S \otimes_R M \to S \otimes_R N$ is exact.

Proposition

The localization homomorphism $R \to U^{-1}R$ is flat.

Proof.

- Let $L \to M \to N$ be an exact sequence of R-modules
- Then $U^{-1}R \otimes_R M \simeq M$ and similarly for L, N
- Furthermore the exact sequence

$$U^{-1}R \otimes_R L \to U^{-1}R \otimes_R M \to U^{-1}R \otimes_R N$$

  is isomorphic to $U^{-1}L \to U^{-1}M \to U^{-1}N$.
- Since localization is exact the above sequence is exact.

Noetherian and Artinian modules

Let M be an R-module.

Definition

M is called **Noetherian** if every ascending chain of submodules stabilizes, i.e. if

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

is a chain of submodules of M, then there exists an integer N such that $M_n = M_N$ for all $N \geq n$.

Definition

M is called **Artinian** if every descending chain of submodules stabilizes, i.e. if

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$

is a chain of submodules of M, then there exists an integer N such that $M_n = M_N$ for all $N \geq n$.

An equivalent characterization

Let M be an R-module.

Proposition

M is Noetherian (resp. Artinian) if and only if any nonempty collection $\mathcal{S}$ of submodules of M has a maximal (resp. minimal) element with respect to inclusion.

Proof.

- We proof the Noetherian statement, the Artinian case is exactly the same
- Assume that every nonempty collection of submodules has a maximal element. Take an ascending chain $M_1 \subset M_2 \subset \dots$ and let $\mathcal{S} = \{M_n\}_{n \geq 1}$. Then $\mathcal{S}$ has a maximal element $M_N \in \mathcal{S}$. M_N is maximal $\implies$ $M_n = M_N$ for all $n \geq N$.
- Assume that M is Noetherian and let $\mathcal{S}$ be a nonempty set of submodules of M. If M does not have a maximal element, we can construct an infinite strictly ascending chain of submodules which contradicts to M being Noetherian.

Example: vector spaces

Let V be a vector space over a field k.

- Then V is Noetherian if and only if V has finite dimension. Indeed, if we have an infinite ascending chain

$$V_1 \subset V_2 \subset \dots$$

of subspaces, then $\dim(V_n)$ is an increasing sequence. If $\dim(V)$ is finite, this chain must stabilize. Conversely, if $\dim(V)$ is infinite, there is a strictly ascending chain of subspaces.

- Similarly V is Artinian if and only if V has finite dimension. Indeed same argument with dimensions of chains as above shows that finite dimensional vector spaces are Artinian. Conversely, if V is infinite dimensional, we can construct a sequence of linearly independent linear functions $f_i : V \to k$, and let $V_n = \ker(f_1) \cap \dots \cap \ker(f_n)$ to be the infinite strictly descending chain.

Theorem

Let $0 \to N \to M \to L \to 0$ *be an exact sequence of* R*-modules. Then* M *is Noetherian (resp. Artinian) if and only if both* N *and* L *are Noetherian (resp. Artinian). In particular submodules and quotient modules of Noetherian (resp. Artinian) modules are Noetherian (resp. Artinian).*

Proof begins:

- As usual we only do Noetherian case
- If M is Noetherian, then N and L are Noetherian too, because submodules of N are also submodules of M so chains in N stabilize, and submodules of L correspond to submodules of M which contain N, so chains in L stabilize too
- Now assume that N and L are Noetherian
- Take an ascending chain $M_n \subset M$, and let $N_n = M_n \cap N \subset N$

...

Proof ends:

- N is Noetherian, hence N_n stabilize for large n, so let's just assume $M_n \cap N = N_0$ for all n (otherwise replace the chain by its tail)
- Now consider the quotients $M_n/N_0 = M_n/(M_n \cap N)$
- We use 2nd isomorphism theorem (which I haven't stated but it the same as for abelian groups):

$$M_n/(M_n \cap N) \simeq (M_n + N)/N = \overline{M_n}.$$

- Now the chain $\overline{M_n} \subset M/N = L$ stabilizes since L is Noetherian
- This implies: $M_n/N_0 = M_{n+1}/N_0$ (think this through, that's a bit subtle!)
- Hence M_n stabilizes

□

Corollary

Finite direct sums of Noetherian (resp. Artinian) modules are Noetherian (resp. Artinian).

Proof.

Let M and N be R-modules. There is a short exact sequence

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

and using the Theorem above, $M \oplus N$ is Noetherian (resp. Artinian) as soon as both M and N are Noetherian (resp. Artinian). □

Example

We've seen earlier that finite dimensional vector spaces are Noetherian and Artinian as k-modules directly. We can deduce this fact from the Corollary as follows. We start with $V \simeq k^n$, $n = \dim(V)$. Now k is both Noetherian and Artinian as k-module: indeed the only submodules of k are 0 and k. Now the Corollary tells us that $V \simeq k^n$ is also Noetherian and Artinian k-module.

So far properties of Noetherian and Artinian modules have been pretty much parallel. The next Theorem breaks the symmetry.

Theorem

An R-module M is Noetherian if and only every submodule is finitely generated. In particular, Noetherian modules are finitely generated.

Proof.

- Let M be Noetherian, and let $N \subset M$ be a submodule. Construct a chain of submodules of M as follows: take $n_1 \in N$, and let $N_1 = Rn_1 \subseteq N$ Now take $n_2 \in N \setminus N_1$ and let $N_2 = Rn_1 + Rn_2 \subseteq N$, and so on. This chain must stabilize which shows that N is finitely generated.
- Conversely, assume that every submodule of M is finitely generated and let M_n be an infinite ascending chain. Take $N = \cup_{n \geq 1} M_n$, this is a submodule of M. Now N must be finitely generated: $N = \langle m_1, \ldots, m_k \rangle$, and all the generators belong to some M_n, hence the chain stabilizes: $N = M_n$.

Noetherian and Artinian rings

Definition

We call a ring R **Noetherian** (resp. **Artinian**) if R is a Noetherian (resp. Artinian) module over itself.

That is, we require respective chains of ideals in R to stabilize.

Example

A field is a Noetherian and Artinian ring since there are only two ideals, hence no infinite chains.

Corollary

R is Noetherian if and only if every ideal $I \subset R$ is finitely generated.

This follows from the Theorem above since submodules of R are precisely its ideals.

Noetherian rings are quite common: the Noetherian property simply says that R is "not too large".

Example

Any PID, such as $\mathbb{Z}$ or $k[x]$ is Noetherian, because in a PID all ideals are principal hence finitely generated.

Example

We'll soon see that $k[x_1, \ldots, x_n]$ is Noetherian (this is so-called Hilbert's Basis Theorem).

Example

The polynomial ring $k[x_1, x_2, \ldots]$ in infinitely many variables is not Noetherian. Indeed its maximal ideal $(x_1, x_2, \ldots)$ is not finitely generated, as every generator involves only finitely many variables.

Artinian rings are quite rare and they are "quite small". As soon as we define dimension of a ring we will see that Artinian rings are zero-dimensional.

Example

$\mathbb{Z}$ is not Artinian. This is because we have infinite descending chains of ideals: $\mathbb{Z} \supset (p) \supset (p^2) \supset (p^3) \supset \dots$

Example

Any finite ring, such as $\mathbb{Z}/(n)$ is Artinian (and Noetherian too). Indeed ideals are finite subsets, hence chains must stabilize.

Example

$R = k[x]/(x^n)$ is Artinian (and Noetherian too). Ideals of R correspond to ideals of $k[x]$ which contain (x^n). Every ideal in $k[x]$ is principal: $I = (f(x))$ and we require $f(x)$ to divide x^n. That is *all* ideals in R are among

$$(0) \subset (\overline{x^{n-1}}) \subset \cdots \subset (\overline{x}) \subset R,$$

and there are no infinite chains.

Finitely generated modules over Noetherian and Artinian rings

Theorem

If R is a Noetherian (resp. Artinian) ring, then any finitely generated R-module is Noetherian (resp. Artinian).

Proof.

- We do the Noetherian case, the Artinian case being parallel
- For any $n \geq 1$, finitely generated free module R^n is a direct sum of Noetherian modules, hence R^n is Noetherian
- Any finitely generated module M is a quotient R^n
- Therefore M is Noetherian

□

Quotients of Noetherian and Artinian rings

Theorem

If R is Noetherian (resp. Artinian) ring, and $I \subset R$ is an ideal, then any finitely generated R/I is Noetherian (resp. Artinian) ring.

Proof.

- We do Noetherian case.
- R/I is a quotient R-module of R, hence R/I is an Noetherian R-module
- However R-modules of R/I coincide with its ideals, hence R/I is Noetherian an R/I-module too

□

Hilbert's Basis Theorem

Theorem (Hilbert's Basis Theorem)

If R is a Noetherian ring, so is $R[x]$.

Proof begins:

- Let $I \subseteq R[x]$ be an ideal. We show that I is finitely generated.
- Any element $f \in R[x]$ has the form $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_n \neq 0$; denote by $\mathrm{lc}(f) = a_n$ the leading coefficient of f.
- $\mathrm{lc}(I) = \{\mathrm{lc}(f) : f \in I\}$ is an ideal (easy to see)
- R is Noetherian, hence ideals are finitely generated: $\mathrm{lc}(I) = (a_1, \ldots, a_n) \subset R$, and take $f_i \in I$ with $\mathrm{lc}(f_i) = a_i$ for $i = 1 \ldots n$.
- Let $K = (f_1, \ldots, f_n) \subset R[x]$.
- Let $D = \max\{\deg(f_i) \,|\, 1 \leq i \leq n\}$ and let $I^{<D}$ be the R-submodule of I consisting of polynomials of degree $\leq D-1$.

...

Proof ends:

- We have $K, I^{<D} \subset I$. Let us show that $I = K + I^{<D}$ (as R-modules).
- Take $f \in I$ and do induction on $\deg(f)$.
- If $\deg(f) < D$, then $f \in I^{<D}$ and we are done
- Otherwise, the top coefficient $\mathrm{lc}(f)$ is an R-linear combination of $a_1, \ldots, a_n$: $\mathrm{lc}(f) = r_1 a_1 + \cdots + r_n a_n$.
- Thus we may get rid of the top coefficient:

$$f = (r_1 f_1 x^{\deg(f)-\deg(f_1)} + \cdots + r_n f_n x^{\deg(f)-\deg(f_1)}) + g$$

  where $\deg(g) < \deg(f)$, and we proceed by induction as the first term is in K. We have shown that $I = K + I^{<D}$.
- $I^{<D}$ is a submodule of Noetherian R-module $R \oplus Rx \oplus \cdots \oplus Rx^{D-1}$, hence $I^{<D}$ is finitely generated R-module, so let $I^{<D} = Rg_1 + \cdots + Rg_m$
- Now $I = K + I^{<D} = (f_1, \ldots, f_n, g_1, \ldots, g_m)$ and we are done.

□

Corollary

$R = k[x_1, \ldots, x_n]$ is a Noetherian ring, and any quotient ring of R is also Noetherian.

Proof.

- k is Noetherian, hence $k[x_1, \ldots, x_n]$ is Noetherian by induction using Hilbert's Basis Theorem
- Quotient rings of Noetherian rings are Noetherian.

Irreducible ideals

Throughout this chapter R will denote a Noetherian ring. We try to generalize factorization of integers into prime powers to a statement about decomposing ideals into intersections of so-called primary ideals.

Definition

We call an ideal $I \subset R$ **irreducible** if it cannot be written as $I_1 \cap I_2$ where I_1 and I_2 are proper ideals of R which strictly contain I.

Proposition

Every proper ideal $I \subset R$ can be presented as an intersection of finitely many irreducible ideals.

Proof.

- Assume the proposition is false, i.e, the set $\mathcal{S}$ of ideals which can not be written as an intersection of irreducibles is nonempty
- Since R is Noetherian we can take a maximal element $J \in \mathcal{S}$
- J is not irreducible $\implies$ $J = K \cap L$ for ideals $J \subsetneq K$ and $J \subsetneq L$
- J maximal in $\mathcal{S}$ $\implies$ $K, L \notin \mathcal{S}$ $\implies$ $K = K_1 \cap \cdots \cap K_s$ and $L = L_1 \cap \cdots \cap L_t$
- Now $J = K \cap L = K_1 \cap \cdots \cap K_s \cap L_1 \cap \cdots \cap L_t$, a contradiction!

$\square$

Definition

We call a proper ideal $I \subset R$ **primary** if the zero-divisors of R/I are nilpotent, or equivalently

$$ab \in I \implies a \in I \text{ or } b^n \in I \text{ for some } n \geq 1.$$

Proposition

If $I \subset R$ is a primary ideal then $\sqrt{I}$ is a prime ideal

Proof.

- Let $ab \in \sqrt{I}$
- This means $a^n b^n \in I$ for some $n \geq 1$.
- I is primary $\implies a^n \in I$ or $(b^n)^m = b^{mn} \in I$ for some $m \geq 1$
- Therefore $a \in \sqrt{I}$ or $b \in \sqrt{I}$.

□

If $\sqrt{I}$ is a prime ideal, is I primary? (See problem sheet.)

Definition

We call an ideal $I \subset R$ P-**primary** if it is primary and $\sqrt{I} = P$.

Proposition

Let $q_1, \ldots, q_s$ be P-primary ideals of a commutative ring R. Then $q_1 \cap \cdots \cap q_s$ is P primary.

Proof.

- Taking radicals commutes with finite intersections: $\sqrt{q_1 \cap \cdots \cap q_s} = \sqrt{q_1} \cap \cdots \cap \sqrt{q_s} = P$
- Let $ab \in q_1 \cap \cdots \cap q_s$ and $b \notin q_1 \cap \cdots \cap q_s$
- Pick $1 \leq j \leq s$ such that $b \notin q_j$
- q_j primary, $ab \in q_j$, $b \notin q_j \implies a \in \sqrt{q_j} = \sqrt{q_1 \cap \cdots \cap q_s}$

Primary decomposition: statement

Definition

- Primary decomposition of an ideal $I \subset R$ is a decomposition $I = \cap_{i=1}^{n} q_i$ where q_i are primary ideals.
- If in addition all radicals $\sqrt{q_i}$ are distinct and $q_i \not\supset \cap_{j \neq i} q_j$, then such a decomposition is called minimal.

Theorem

Any ideal $I \subset R$ admits a primary decomposition. If $I = \cap_{i=1}^{n} q_i$ is a minimal primary decomposition, then the set of primes $\{\sqrt{q_1}, \ldots, \sqrt{q_n}\}$ does not depend on the decomposition.

The radicals $\sqrt{q_i}$ of a minimal primary decomposition are called primes associated to I, and their collection is denoted by $\operatorname{ass} I$.

Colon ideals

The proof of the the Theorem about primary decomposition will occupy the rest of this chapter. As one of the tools we will use colon ideals $(I : J)$. Recall the following exercise from the first problem sheet:

For any subsets $I, J \subseteq R$ we define $(I : J) = \{a \in R \mid aJ \subseteq I\}$. Show that

(a) if I is an ideal, so is $(I : J)$,

(b) if $I, J_1, \ldots, J_s \subseteq R$ are ideals then
$(I : J_1 + \cdots + J_s) = (I : J_1) \cap \cdots \cap (I : J_s)$,

(c) for any $I_1, \ldots, I_s \subseteq R$,
$(I_1 \cap \cdots \cap I_s : J) = (I_1 : J) \cap \cdots \cap (I_s : J)$,

Proposition

If $I \subset R$ is irreducible, then I is primary.

Corollary

Any ideal admits a primary decomposition.

Proof.

- Already seen: any ideal is a finite intersection of irreducible ideals, hence the Corollary follows from the Proposition
- Take $I \subset R$ an irreducible ideal and suppose that $ab \in I$ for some $a \in R \setminus I$ and $b \in R$. Let's check that $b^n \in I$ for some n.
- Consider the ascending chain of ideals $\{(I : b^n)\}_{n=1}^{\infty}$;
- R Noetherian, so we can find $N \geq 1$ such that

$$(I : b^n) = (I : b^N) \text{ for all } n \geq N$$

- Let $K = I + Ra$ and $L = I + Rb^N$ and notice that K is a proper ideal which strictly contains I.
- We have $I \subseteq K \cap L$. Let's show that $I = K \cap L$.

Proof continues.

- Pick $f \in K \cap L$ and write it as

$$f = i + ra = j + sb^N$$

  for $i, j \in I$ and $r, s \in R$.
- Multiply the equation by b to obtain

$$fb = bi + rab \implies fb \in I$$
$$fb = bj + sb^{N+1} \implies s \in (I : b^{N+1})$$

- Hence $s \in (I : b^N) = (I : b^{N+1})$.
- Now $f = j + sb^N \in I$.
- This shows $I = K \cap L$.
- I irreducible, $I \neq K \implies I = L = I + Rb^N \implies b^N \in I$.

A simple example

Let $R = \mathbb{Z}$. R is a PID: every ideal is principal, and we have

$$(n) \text{ is a prime ideal } \iff n = \pm p, \ p \text{ prime}$$
$$(n) \text{ is a primary ideal } \iff n = \pm p^k, \ p \text{ prime}, k \geq 1$$

Intersections of ideals are computed as $(n) \cap (m) = (lcm(n, m))$ and we see that if $n = \pm p_1^{k_1} \cdots p_r^{k_r}$, then

$$(n) = (p_1^{k_1}) \cap \cdots \cap (p_r^{k_r})$$

is a minimal primary decomposition. Primary decomposition is unique in $R = \mathbb{Z}$.

Furthermore we have (n) is irreducible $\iff$ (n) is primary.

An interesting example

Let $R = k[x, y]$, $I = (xy, y^2) \subset R$.

We have two primary decompositions

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

Note that the radicals in the primary decompositions above coincide (as the Theorem on primary decomposition says), and we have

$$\operatorname{ass} I = \{(x, y), (y)\}.$$

Remark

As we have seen primary components of an ideal are not well-defined. However one can show that primary components corresponding to minimal primes in $\operatorname{ass} I$ are well-defined.

Lemma

Let $P \subset R$ be a prime ideal, and $I_i \subset R$ a finite set of ideals. If $P \supset \cap_{i=1}^{n} I_i$, then $P \supset I_i$ for some i. In particular if $P = \cap_{i=1}^{n} I_i$, then $P = I_i$ for some i.

Proof.

- Assume $P \not\supset I_i$ for every i. Take $a_i \in I_i \backslash P$
- Consider $a = a_1 \cdots a_n \in P$, but none of the a_i belong to P, a contradiction!

□

Lemma

Let q be a primary ideal in a commutative ring R. For any $a \in R$,

$$\sqrt{(q : a)} = \begin{cases} R & \text{if } a \in q \\ \sqrt{q} & \text{if } a \notin q \end{cases}$$

Proof.

Immediate from definition. □

Proposition

Let $I = q_1 \cap \cdots \cap q_s$ be a minimal primary decomposition of I. Then the set $\{\sqrt{q_1}, \ldots, \sqrt{q_s}\}$ coincides with the set of prime ideals among $\sqrt{(I : a)}$, $a \in R$.

Proof.

We rely on the two Lemmas above. We start with a computation:

$$\begin{aligned}\sqrt{(I : a)} &= \sqrt{(q_1 \cap \cdots \cap q_s : a)} = \\ &= \sqrt{(q_1 : a)} \cap \ldots \sqrt{(q_s : a)} = \\ &= \cap_{q_j \not\ni a} \sqrt{q_j}.\end{aligned}$$

Now the prime ideals among the latter intersections are only the $\sqrt{q_j}$'s (because prime ideals are irreducible by the Lemma above). □

Proof of the Theorem about primary decomposition is now complete: we showed that ideals admit irreducible, hence primary decompositions, and that the set of associated primes is well-defined.

Example

Let $I \subset R$ be a radical ideal, i.e. $\sqrt{I} = I$. Let

$$I = q_1 \cap \cdots \cap q_s$$

be its minimal primary decomposition. Then

$$I = \sqrt{I} = \sqrt{q_1} \cap \cdots \cap \sqrt{q_s} = p_1 \cap \cdots \cap p_s$$

is a prime decomposition. Here $\{p_1, \ldots, p_s\} = \operatorname{ass} I$.

Proposition

The set D of zero-divisors of R is the union of all ideals $P \in \operatorname{ass} 0$.

Proof.

- By definition we have $D = \cup_{a \neq 0} \sqrt{(0 : a)}$.
- Let $0 = q_1 \cap \cdots \cap q_n$ with $\sqrt{q_i} = P_i$ so that $\operatorname{ass} 0 = \{P_1, \ldots, P_n\}$.
- We know that every P_i has the form $\sqrt{(0 : a)}$, hence $\cup_{i=1}^{n} P_i \subset D$.
- We've seen that for $a \neq 0$, we have

$$\sqrt{(0 : a)} = \bigcap_{q_j \not\supset a} P_j \subset \bigcup_{i=1}^{n} P_i.$$

- Hence $D = \cup_{i=1}^{n} P_i$.

Definition

Let $I \subset R$ be an ideal. A prime ideal $P \subset R$ is a **minimal ideal of** I if $P \supseteq I$ and there is no prime ideal Q such that $I \subset Q \subsetneq P$.

Proposition

Any prime ideal P which contains I also contains an associated prime of I. In particular the set of minimal prime ideals of I coincides with the set of minimal ideals in $\operatorname{ass} I$.

Proof.

- Let $I \subset P$, P prime
- Then $\sqrt{I} = \cap_{Q \in \operatorname{ass} I} Q \subset P$
- Hence (by one of the Lemmas above) $Q \subset P$, for some $Q \in \operatorname{ass} I$.
- So if P is minimal prime of I then $Q = P$.

Example

Let $R = k[x, y]/(xy, y^2)$, i.e. R has a k-basis

$$1, y, x, x^2, x^3, \ldots,$$

and relations $xy = y^2 = 0$. We describe primary decomposition of the ideal 0 of R and illustrate all previous statements in this case. Prime ideals in R are $P_1 = (x, y)$ and $P_2 = (y)$. In fact P_1 and P_2 are ideals associated to 0 and the primary decomposition is

$$0 = (y) \cap (x, y)^2 = (y) \cap (x^2).$$

Among these primes P_1, P_2 the minimal prime is $P_2 = (y)$ and the maximal prime is $P_1 = (x, y)$. Note that $Nil(0) = \sqrt{0} = (y)$ and the set of zero-divisors D of R is the union

$$D = (y) \cup (x, y) = (x, y).$$

The height on an ideal

Definition

Let R be a commutative ring.

(a) The **height** of a prime ideal $P \subset R$, denoted $\operatorname{ht} P$, is the length h of the longest chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h = P.$$

If there are arbitrarily long such chains we set $\operatorname{ht} P = \infty$.

(b) The **height** of an ideal $I \subset R$, denoted $\operatorname{ht} I$, is defined to be the infimum over all prime ideals $P \supseteq I$ of $\operatorname{ht} P$.

(c) The (Krull) **dimension** of a ring R is the supremum of the lengths of chains of primes. Notation: $\dim(R)$.

Remark

We will see that in Noetherian rings heights of ideals are finite. However, Noetherian rings may have infinite dimension.

Example

If (R, m) is a local ring, then $\dim(R) = \operatorname{ht} m$ since every chain of primes can be extended to a chain finishing with m.

Example

If k is a field, then $\dim k = 0$, since the only prime ideal is (0) and its height is zero.

Example

In $R = \mathbb{Z}$ maximal chains of prime ideals have the form $0 \subset (p)$, so that $\dim(\mathbb{Z}) = 1$.

Exercise

Verify that $\dim k[x] = 1$ and that $\dim k[x]/(x^2) = 0$.

Example

It is easy to see that $\dim k[x_1, \ldots, x_n] \geq n$. Much work will be require to prove the equality here.

Maximal ideals in R can have different heights

We'll see later on that in a polynomial ring $k[x_1, \ldots, x_n]$ all maximal ideals have same height n. We now give an example of a domain R with maximal ideals m_1, m_2 such that $\mathrm{ht}(m_1) \neq \mathrm{ht}(m_2)$.

- Let $R = \mathbb{Z}_{(p)}[x]$, the polynomial ring over $\mathbb{Z}$ localized at (p)
- Let $m_1 = (p, x)$. We have $R/(p, x) = \mathbb{Z}_{(p)}/(p) = \mathbb{Z}/(p)$, a field, hence m_1 is maximal
- For the height of m_1, consider the chain $0 \subset (x) \subset (p, x)$, hence $\mathrm{ht}(m_1) \geq 2$ (in fact it is equal to two by the Krull's Principal Ideal Theorem which we prove later in this chapter)
- Let $m_2 = (px - 1)$. We have $R/(px - 1) = \mathbb{Z}_{(p)}[1/p] = \mathbb{Q}$, a field, hence m_2 is maximal
- $px - 1$ is irreducible, $\mathrm{ht}(m_2) = 1$.

Artinian rings

We now study rings of dimension 0. We will prove that any Artinian ring is zero-dimensional.

Lemma

An Artinian domain is a field.

Proof.

- Take a nonzero element $a \in R$, and consider a chain of ideals $(a) \supset (a^2) \supset \dots$ This chain stabilizes: $(a^n) = (a^{n+1})$
- Hence $a^n = ba^{n+1} \implies 1 = ab$ (R is a domain), and a is invertible. Thus R is a field!

□

Proposition

An Artinian ring R has finitely many prime ideals and all prime ideals are maximal. In particular $\dim(R) = 0$.

Proof.

- Let $P \subset R$ be a prime ideal and consider the ring $D = R/P$
- D is an Artinian domain, therefore D is a field (previous Lemma)
- Therefore P is maximal
- Assume $P_1, P_2, \ldots$ is an infinite sequence of distinct primes
- Then $P_1 \cap \cdots \cap P_n \cap P_{n+1} = P_1 \cap \cdots \cap P_n$ for some $n \geq 1$ (since R Artinian),
- That is $P_{n+1} \supseteq P_1 \cap \cdots \cap P_n \implies P_{n+1} \supseteq P_j$ for some j (Lemma from last week), a contradiction!

□

Exercise

Is any ring of dimension zero Artinian (Noetherian)?

Theorem

Let (R, m) be a Noetherian local ring. The following conditions are equivalent:

(a) *R is Artinian*

(b) *m is the only prime ideal of R*

(c) *m is nilpotent, i.e. $m^n = 0$ for some $n \geq 1$*

Remark

In fact if R is Artinian, then it is automatically Noetherian but we don't prove this fact.

Proof.

- We use notation $k = R/m$
- $(a) \implies (b)$: follows since every prime ideal in Artinian ring is maximal
- $(b) \implies (c)$: since m is the only prime ideal, we have $\mathrm{Nil}(R) = m$, so that every element of m is nilpotent, and since R is Noetherian so that m is finitely generated, (c) follows
- $(c) \implies (a)$: consider the chain of R-modules:

$$R \supset m \supset m^2 \supset \cdots \supset m^n = 0$$

The factors m^i/m^{i+1} are finitely generated R/m-modules, hence finite dimensional k-vector spaces and so they are Artinian R-modules. By induction we get that R is an Artinian R-module, hence an Artinian ring.

Krull's Principal Ideal Theorem

Our aim is to describe height of ideals generated by n elements. We start with principal ideals.

Theorem (Krull's Principal Ideal Theorem)

The height of a minimal prime of a principal ideal in a Noetherian ring R is at most one.

Remark

If R is a domain, then the only prime ideal of height 0 is the zero ideal.

Example: ideals of height one in polynomial rings

Let $R = k[x_1, \ldots, x_n]$. Let us show that prime ideals of height 1 in R are precisely principal ideals $P = (f)$ where f is an nonconstant irreducible polynomial.

- Let $f \in R$ be a nonconstant irreducible polynomial. Then (f) has height one by the principal ideal theorem (it can not have height zero because $f \neq 0$).
- Conversely, let $P \subset R$ be a prime ideal of height one. Take any element $f \in P$. Because P is prime we may assume that f is irreducible. Then $0 \subset (f) \subseteq P$, so that $P = (f)$ because P has height one.

For the proof of Krull's Principal Ideal Theorem we use ideas from primary decomposition. Recall one of the exercises from Week 5: if P is a prime ideal, then the so-called n'th symbolic power of P

$$P^{(n)} = \{r \in R : sr \in P^n \text{ for some } s \notin P\}$$

is a P-primary ideal and in fact $P^{(n)} \supset P^n$ is the P-primary component of P^n. Finally we'll use that $P^{(n)}$ is the contraction of the ideal $P^n R_P$ under localization $R \to R_P$.

Proof begins:

- Let P be a minimal prime ideal containing an element $f \in R$
- We may assume that P is the unique maximal ideal of R (otherwise replace R by localization R_P)
- We need to show that $\operatorname{ht} P \leq 1$. So take a prime $Q \subsetneq P$.
- Consider the descending chain $Q^{(n)} \supset Q^{(n+1)}$. Our aim is to show that this chain stabilizes.

...

Proof ends:

- The ring $\overline{R} = R/(x)$ is Artinian. This is because the unique maximal ideal $\overline{P} \subset \overline{R}$ is also minimal.
- Hence the chain $Q^{(n)} + (x)$ stabilizes.
- In particular $Q^{(n)} \subset Q^{(n+1)} + (x)$: for every $f \in Q^{(n)}$, we have $f = g + ax$, $g \in Q^{(n+1)}$. Since $x \notin \sqrt{Q^{(n)}} = Q$ and $Q^{(n)}$ is P-primary we deduce that $a \in Q^{(n)}$.
- Therefore $Q^{(n)} = Q^{(n+1)} + Q^{(n)}(x)$.
- By Nakayama's Lemma, we have $Q^{(n)} = Q^{(n+1)}$.
- This means that in the localization R_Q we have $Q_Q^n = Q_Q^{n+1}$
- Again by Nakayama's Lemma we have $Q_Q^n = 0$.
- This implies that R_Q is Artinian hence $\operatorname{ht} Q = \dim R_Q = 0$
- Q was an arbitrary prime contained in P, so $\operatorname{ht} P \leq 1$.

□

Corollary (Krull's Height Theorem)

Let R be a Noetherian ring R and let I be an ideal generated by n elements. Then $\operatorname{ht} I \leq n$.

Proof begins:

- Let P be a minimal prime containing $I = (f_1, \ldots, f_n)$.
- May assume P to be the unique maximal ideal of R (otherwise replace R with R_P).
- The proof goes by induction on n
- Let $Q \subsetneq P$ be a prime ideal maximal among the primes strictly contained in P.
- Let us show that we can choose generators $f_1, \ldots, f_n$ in such a way that $Q = (f_2, \ldots, f_n)$.
- We may assume $f_1 \notin Q$ (otherwise relabel the generators).

...

Proof ends:

- So we work with ideals $Q \subset Q + (f_1) \subset P$
- Consider the quotient ring $\overline{R} = R/(Q + (f_1))$
- $\overline{R}$ is Artinian because its unique maximal ideal $\overline{P}$ is also minimal (no primes between Q and P), hence $\overline{P}$ nilpotent
- In other words P is nilpotent modulo $Q + (f_1)$
- This means: $f_j^n = a_i f_1 + g_j$, $j = 2 \ldots n$ with $g_j \in Q$
- Now replace generators $f_2, \ldots, f_n$ with $g_2, \ldots, g_n$
- We have $P = (f_1, \ldots, f_n)$ and $Q = (f_2, \ldots, f_n)$.
- By the induction hypothesis ht $Q \leq n - 1$, hence ht $P \leq n$

□

Corollary

In Noetherian rings ideals have finite height.

Example

Let $R = k[x_1, \ldots, x_n]$, then Krull's Principal Ideal Theorem says that $\mathrm{ht}(x_1, \ldots, x_n) \leq n$. However we have a chain

$$(0) \subset (x_1) \subset \cdots \subset (x_1, \ldots, x_n),$$

so in fact $\mathrm{ht}(x_1, \ldots, x_n) = n$.

We are not yet ready to show that $\dim R = n$.

Converse of the Principal Ideal Theorem

It is a subtle problem to check if a given ideal of height n is generated by n elements, even if R is a polynomial ring. The best we have in general is:

Theorem

Any prime ideal $P \subset R$ of height n is minimal over an ideal generated by n elements.

Proof begins:

- We do induction on $1 \leq r \leq n$ to prove that there exist elements $f_1, \ldots, f_r \in P$ which generate an ideal of height r
- Assume $f_1, \ldots, f_r \in P$ with $\mathrm{ht}(f_1, \ldots, f_r) = r$, and let $P_1, \ldots, P_k$ be the minimal primes of $(f_1, \ldots, f_r)$ that have height r.

...

Proof ends:

- Choose $f_{r+1} \in P \setminus \cup_{i=1}^{k} P_i$ (this is possible by so-called prime avoidance since $P \not\subset P_i$, see Problem Sheet Week 1).
- Now $f_1, \ldots, f_{r+1}$ generate an ideal not contained in any of the P_i, hence its height is strictly bigger than r, so by the Principal Ideal Theorem we have $\mathrm{ht}(f_1, \ldots, f_{r+1}) = r + 1$
- Thus eventually we construct an ideal $(f_1, \ldots, f_n)$ of height n. Since $(f_1, \ldots, f_n) \subset P$ and both ideals have height n, P must be minimal over $(f_1, \ldots, f_n)$.

$\square$

Algebras

Definition

Let R be a ring. An R-**algebra** is a ring S together with a ring homomorphism

$$\phi : R \to S.$$

An R-algebra S has a structure of an R-module given by

$$r \cdot s := \phi(r)s.$$

In fact S is an R-algebra if S is both a ring and an R-module, such these structures are compatible (do you see what I mean?).

Example

- For any subring $R \subset S$, S is an R-algebra (in this case we will sometimes refer to S as an **extension** of R).
- The polynomial ring $R[x_1, \ldots, x_n]$ is an R-algebra
- Any ring S is a $\mathbb{Z}$-algebra (in a unique way!).

Definition

An R-**subalgebra** of S is a subring which is closed under R-multiplication.

Definition

Let R be a ring and let S, T be R-algebras. A homomorphism of R algebras $\phi : S \to T$ is a homomorphism of rings for which $\phi(rs) = r\phi(s)$ for all $r \in R$ and $s \in S$.

Example

$k[x] \subset k[x, y]$ is a k-subalgebra, and the map

$$\begin{aligned} k[x, y] &\to k[x] \\ x &\mapsto x \\ y &\mapsto 0 \end{aligned}$$

is a homomorphism of k-algebras.

Let S be an R-algebra, and let $a_1, \ldots, a_n \in S$. Then we may consider the **subalgebra generated by** $a_1, \ldots, a_n$. This is smallest subalgebra $S' \subset S$ which contains the elements a_i. We use the notation

$$S' = R[a_1, \ldots, a_n] \subset S.$$

Explicitly S' consists of polynomial expressions which involve coefficients from R and variables $a_1, \ldots, a_n$. Note that this notation is potentially confusing: we do not mean that S' is a polynomial ring over R (see examples below).

Remark

Note that we also can consider R-submodule of S generated by $a_1, \ldots, a_n$:

$$Ra_1 + \cdots + Ra_n \subset S$$

and it is strictly smaller that the subalgebra generated by these elements, as for submodule we don't allow to multiply the generators a_i with each other.

Examples of subalgebras

Example

The k-subalgebra of $k[x, y]$ generated by x is $k[x]$.

Example

The k-subalgebra of $k[x]$ generated by x^2 is $k[x^2]$, i.e. the set of polynomials in x with only even degree monomials.

Example

The k-subalgebra of $k[x]$ generated by x^2, x^3 is $k[x^2, x^3]$. Its elements are k-linear combinations of powers x^{2i+3j}, $i, j \geq 0$. In fact any $n \geq 2$ can be written as $n = 2i + 3j$, so we only exclude first power x, hence $k[x^2, x^3]$ consists of

$$f(x) = a_0 + a_2x^2 + a_3x^3 + \dots$$

Note that $k[x^2, x^3]$ is not a polynomial ring over k, that is the k-algebra $k[x^2, x^3]$ is not isomorphic to any polynomial algebra $k[x_1, \dots, x_n]$.

Finitely generated and finite algebras

Definition

Let R be a ring and let S be an R-algebra.

1. We call S a **finitely generated** R-algebra if there exist $s_1, \ldots, s_n \in S$ such that $S = R[s_1, \ldots, s_n]$.
2. We call S is **finite** R-algebra if it is a finitely generated R-module, that is there exist elements $s_1, \ldots, s_n \in S$ such that $S = Rs_1 + \cdots + Rs_n$.

Remark

- If S is finite R-algebra, it is also finitely generated.
- Finitely generated R-algebras are usually not finite, a typical example being the polynomial ring $S = k[x]$ over k.
- If a homomorphism $\pi : R \to S$ is surjective (so that $S \simeq R/I$), then S is finite (and so also finitely generated) R-algebra. Indeed we can even take the empty set of generators.

Recall that a module is finitely generated if and only if it is a quotient of a free finitely generated module. Here is an analogous statement for algebras.

Proposition

Let S be an R-algebra. Then S is a finitely generated R-algebra if and only if there exist $n \geq 0$ and a surjective homomorphism of R-algebras

$$\phi : R[x_1, \ldots, x_n] \to S.$$

Proof.

- If $\phi : R[x_1, \ldots, x_n] \to S$ is a surjective homomorphism, then S is generated as an algebra by $\phi(x_1), \ldots, \phi(x_n)$. So S is finitely generated.
- Conversely, let $s_1, \ldots, s_n$ be generators of S as R-algebra
- Define a map $\phi : R[x_1, \ldots, x_n] \to S$ using $x_i \mapsto s_i$.
- Explicitly, if $f \in R[x_1, \ldots, x_n]$, then $\phi(f) = f(s_1, \ldots, s_n)$.
- This map is a surjective homomorphism of R-algebras.

Finiteness is transitive

If you ever studied Galois Theory you will know that if L/k, M/L are finite field extensions, then M/k is also a finite field extension. Same holds for rings in general, with the same proof!

Proposition

Let S be an R algebra and T be an S algebra. If S is finite over R and T is finite over S then T is finite over R.

Proof.

- So we have our homomorphisms $R \xrightarrow{f} S \xrightarrow{g} T$
- Let $s_1, \ldots, s_n$ be a set of generators of S over R
- Let $t_1, \ldots, t_m$ be a set of generators of T over S
- Consider the set $f(s_i)t_j \in S$ for $i = 1, \ldots, n$, $j = 1, \ldots, m$.
- Take any $t \in T$ and write it as $t = \sum_{j=1}^{m} g(v_j)t_j$, $v_j \in S$
- Now write each $v_j = \sum_{i=1}^{n} f(u_{ij})s_i$, $u_{ij} \in R$ so that we obtain $t = \sum_{i,j} g(f(u_{ij}))f(s_i)t_j$
- Thus every element in T is an R-linear combination of $f(s_i)t_j$.

Integral elements

Definition

Let $i : R \to S$ be an R-algebra (for instance $R \subset S$ is a subring). We say that an element $s \in S$ is **integral over** R if there exists a monic polynomial $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in R[X]$ such that $f(s) = 0$, i.e. we require

$$s^d + i(a_{d-1})s^{d-1} + \cdots + i(a_1)s + i(a_0) = 0 \in S.$$

Example

$\sqrt{2} \in \mathbb{Q}$ is integral over $\mathbb{Z}$ as it satisfies $X^2 - 2 = 0$, and $\frac{2}{3} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$ (exercise!).

Example

If $\pi : R \to S$ is surjective, then every element $s \in S$ is integral: if $s = \pi(r)$, then s is a root of $f(X) = X - r \in R[X]$ as $f(s) = s - \pi(r) = 0$.

Including integral elements gives a finite algebra

Lemma

If $s_1, \ldots, s_n \in S$ are integral elements of an R-algebra, then $R[s_1, \ldots, s_n]$ is finite over R.

Proof.

- We do induction on n. Let $n = 1$. As an R-module, $R[s]$ is generated by all powers $1, s, s^2, \ldots$ However since s is integral over R, $s^{N+1} \in R + Rs + \cdots + Rs^N$ for some N, and thus for $m \geq n$, $s^m \in R + Rs + \cdots + Rs^N$. We have shown that $R[s] = R + \cdots + Rs^N$.
- Induction step: consider the chain of homomorphisms

$$R \to R[s_1, \ldots, s_k] \to R[s_1, \ldots, s_k, s_{k+1}].$$

By induction hypothesis, both homomorphisms represent finite algebras. By transitivity of finiteness, $R \to R[s_1, \ldots, s_{k+1}]$ is a finite algebra.

Integral extensions

Theorem

Let $R \subset S$ be rings. The following condition are equivalent:

(a) *S is finite over R.*

(b) *There exist integral elements $s_1, \ldots, s_n \in S$ which generate S as an R-algebra.*

(c) *S is a finitely generated R-algebra and every element in S is integral over R.*

If the equivalent conditions of the Theorem are satisfied, the extension $R \subset S$ is called an **integral extension**, or we say that S **is integral over** R.

More generally, if $i : R \to S$ is an algebra, then we say that S is integral over R if S is integral over subalgebra $i(R) \subset S$. For instance, if $\pi : R \to S$ is surjective, then S is integral over R by trivial reasons (see Example above).

Proof

- (c) $\Rightarrow$ (b): trivial
- (b) $\Rightarrow$ (a): we've proved this earlier
- (a) $\Rightarrow$ (c). Pick a set of generators $\{s_1, \ldots, s_n\}$ for S as an R-module. Clearly $s_1, \ldots, s_n$ generate S as an R-algebra. Let us add one generator if necessary and assume that $s_1 = 1$.
- We need to show that every element $s \in S$ is integral over R.
- For each $1 \leq i \leq n$ we can write $ss_i = a_{i1}s_1 + \cdots + a_{in}s_n$.
- In other words, if we write v for the vector $(s_1, \ldots, s_n)$ and A for the matrix (a_{ij}) we have $Av = sv$, or $(A - sI)v = 0$, where I is the identity $n \times n$ matrix.
- Now we use adjoint matrices which make sense for commutative rings in the same way as they are defined for fields. We have $\det(A - sI)I = \mathrm{adj}(A - sI)(A - sI)$, so $\det(A - sI)v = 0$, and looking at the first coordinate of this vector we get $\det(A - sI)s_1 = \det(A - sI) = 0$, and this is the desired equation for s with coefficients in R: for $p(x) = \det(A - xI) = \pm x^n + \cdots \in R[x]$, we have $p(s) = 0$.

Prime ideals in Integral Extensions

Recall that for any ring extension $R \subset S$ and a prime ideal $Q \subset S$, the intersection $Q \cap R$ is a prime ideal in R. One of the useful features of integral extensions $R \subset S$ is a correspondence between prime ideals in R and S. We will see that for integral extensions $\dim(R) = \dim(S)$.

Example

In Algebraic Number Theory one considers integral extensions such as $\mathbb{Z} \subset S = \mathbb{Z}[\sqrt{2}]$ and describes prime ideals $Q \subset S$ over prime ideals $(p) \subset \mathbb{Z}$, that is satisfying $Q \cap \mathbb{Z} = (p)$. For example, $7 = (3+\sqrt{2})(3-\sqrt{2})$ leads to $Q_1 = (3-\sqrt{2})S$, $Q_2 = (3+\sqrt{2})S$ being primes over (7). To see this, consider the norm map $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$, defined by $N(a+b\sqrt{2}) = a^2 - 2b^2$. We have

$$n \in Q_1 \cap \mathbb{Z} \implies N(3-\sqrt{2}) \mid n^2 \implies n \in (7).$$

and similarly for Q_2.

Theorem (Going up Theorem)

Let $R \subset S$ be an integral extension.

(a) *For any prime $P \subset R$ there exists a prime $Q \subset S$ with $P = Q \cap R$.*

(b) *If $Q \subseteq Q' \subset S$ are primes with $Q \cap R = Q' \cap R$, then $Q = Q'$.*

(c) *For any chain of primes $P_0 \subset \cdots \subset P_n$ of R and prime $Q_0 \subset S$ such that $Q_0 \cap R = P_0$ there exist primes $Q_0 \subset Q_1 \subset \cdots \subset Q_n$ in S with $P_i = Q_i \cap R$.*

Proof of going up (a).

- Consider $U = R \setminus P$, and replace R and S by localizations $R_P = U^{-1}R$ and $U^{-1}S$ respectively. Then $R_P \to U^{-1}S$ is injective (localization is exact!) and integral, because every element in $U^{-1}S$ has the form $\frac{s}{u} = s \cdot \frac{1}{u}$ with $s \in S$ integral and $\frac{1}{u} \in R_P$ is unit, so $\frac{s}{u}$ is integral.
- Thus we may assume that R is local with maximal ideal P
- Now any prime ideal $Q \subset S$ which contains PS will satisfy $Q \cap R = P$ because $Q \cap R \supset P$ and P is maximal.
- Thus we only need to show that PS is a proper ideal, that is $PS \neq S$.
- We use Nakayama's Lemma applied to finitely generated R-module S (S is a integral over R, hence it is a finitely generated R-module): $PS = S \implies S = 0$, which is impossible

Proof of going up (b).

- We may replace R and S with R/P and S/Q. Indeed note $R/P \to S/Q$ is still injective, so that we have a ring extension $R/P \subset S/Q$ and it is obviously integral. We thus may assume that R, S are domains and that $P = 0$, $Q = 0$ and $0 \subseteq Q' \subset S$.
- Let us show that $Q' \cap R = 0$ is impossible unless $Q' = 0$
- Take an element $s \in Q'$ and write its equation as $s^d + r_{d-1}s^{d-1} + \cdots + r_0 = 0$.
- We may assume $r_0 \neq 0$, otherwise divide the equation by s (we are in a domain!)
- Hence we may rewrite the equation $r_0 = s \cdot (\dots) \in Q' \cap R = 0$, a contradiction!

Proof of going up (c).

- Using induction on n we can reduce to the case $n = 1$.
- S/Q_0 is integral extension of R/P_0
- Going Up (a) shows that there exists a prime Q_1/Q_0 of S/Q_0 lying over P_1/P_0.

□

Dimensions of integral extensions

Corollary

If $R \subseteq S$ is an integral extension, $\dim(R) = \dim(S)$.

Proof.

- Any chain of primes $Q_0 \subsetneq \cdots \subsetneq Q_d$ in S gives a chain of primes $Q_0 \cap R \subsetneq \cdots \subsetneq Q_d \cap R$. Inclusions are strict by Going Up Theorem (b), hence R has a chain of length equal to $\dim(S)$, so that $\dim(R) \geq \dim(S)$.
- Conversely, by Going Up Theorem (c) any strictly ascending chain of primes $P_0 \subsetneq \cdots \subsetneq P_d$ in R can be lifted to a strictly ascending chain of primes in S of the same length, hence S has chains of length equal to $\dim(R)$, so $\dim(S) \geq \dim(R)$

□

For example, we have

- $\dim k[x]/(x^2) = \dim k = 0$
- $\dim \mathbb{Z}[\sqrt{2}] = \dim \mathbb{Z} = 1$

From now on we work with k algebras. Note that if $k \to R$ is a ring homomorphism, then it is automatically injective (because k has no proper ideals other than 0): so we may assume that we have a subring $k = k \cdot 1 \subset R$.

Definition

Let R be a k-algebra. We call $u_1, \ldots, u_n \in R$ **algebraically independent over** k if for all non-zero $f \in k[x_1, \ldots, x_n]$, $f(u_1, \ldots, u_n) \neq 0$.

In other words $u_1, \ldots, u_n \in R$ are algebraically independent if the k-algebra they generate is isomorphic to the polynomials: $k[u_1, \ldots, u_n] \simeq k[x_1, \ldots, x_n]$.

For instance elements $x, y \in k[x, y]$ are algebraically independent, but elements $x^2, x^3 \in k[x]$ are not algebraically independent.

Noether Normalization

Theorem (Noether's Normalization Theorem)

Let R be a finitely generated algebra over a field k. There exist elements $u_1, \ldots, u_d \in R$ which are algebraically independent over k and such that R is finite over $k[u_1, \ldots, u_d]$.

Example

Consider the following (artificial) example: $R = \mathbb{Q}[\pi, \sqrt{2}]$, the $\mathbb{Q}$-subalgebra of $\mathbb{C}$ generated by π and $\sqrt{2}$. Then R is finitely generated over $\mathbb{Q}$ and Noether Normalization presents in the chain

$$\mathbb{Q} \subset \mathbb{Q}[\pi] \subset \mathbb{Q}[\pi, \sqrt{2}]$$

with the first step a polynomial extension (note: $\pi \in \mathbb{C}$ is transcendental), followed by an integral extension.

Proof of the Noether Normalization

- Since R is finitely generated it has the form $R = k[s_1, \ldots, s_n]$.
- If $s_1, \ldots, s_n$ are algebraically independent, we are done. Therefore assume that

$$F(s_1, \ldots, s_n) = 0$$

  is an algebraic dependence.
- If F has the form

$$F(x_1, \ldots, x_n) = a_d x_n^d + a_{d-1} x_n^{d-1} + \cdots + a_1 x_n + a_0$$

  where $a_i \in k[x_1, \ldots, x_{n-1}]$ and $a_d \in k \backslash \{0\}$, then s_n is integral over $k[s_1, \ldots, s_{n-1}]$, and we may proceed by induction using transitivity of finiteness.
- However by the next Lemma we always can find coordinates in which F has the form as above.

Lemma

Let $R = k[x_1, \ldots, x_n]$ for some field k, and let $f \in R$. There exists an isomorphism of k-algebras $\phi : R \to R$ for which $\phi(f)$ has the form:

$$\phi(f) = a_d x_n^d + a_{d-1} x_n^{d-1} + \cdots + a_1 x_n + a_0$$

with $a_i \in k[x_1, \ldots, x_{n-1}]$ and $a_d \in k \backslash \{0\}$.

Proof begins:

- Pick $B \in \mathbb{N}$, a large integer (we later specify exactly how large B must be). Let $\phi : R \to R$ be the isomorphism of k-algebras defined by $\phi(x_n) = x_n$ and $\phi(x_i) = x_i + x_n^{B^i}$ for all $1 \leq i \leq n-1$.
- Pick any term $t = \lambda x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n}$ in f; we have $\phi(t) = \lambda(x_1 + x_n^B)^{\alpha_1}(x_2 + x_n^{B^2})^{\alpha_2} \ldots (x_{n-1} + x_n^{B^{n-1}})^{\alpha_{n-1}} x_n^{\alpha_n}$ and its expansion has a unique term of maximal degree in x_n: $\lambda x_n^{\alpha_n + \alpha_1 B + \alpha_2 B^2 + \cdots + \alpha_{n-1} B^{n-1}}$.

...

Proof ends:

- Different terms in f will produce different terms of maximal degree in x_n in $\phi(f)$, because if $B > \alpha_j$ for all $1 \leq j \leq n$ so $\alpha_n + \alpha_1 B + \alpha_2 B^2 + \cdots + \alpha_{n-1} B^{n-1}$ is a base-B expansion.
- The leading term of $\phi(f)$ will be one of the terms above (namely the unique term with maximal $\alpha_n + \alpha_1 B + \alpha_2 B^2 + \cdots + \alpha_{n-1} B^{n-1}$), and we are done!

$\square$

Remark

While proving Noether's Normalization we proved a bit more: if R is a k-algebra generated by $s_1, \ldots, s_n$, then either these are algebraically independent or R is finite over a polynomial ring with $< n$ variables.

Theorem (Finally!)

$\dim(k[x_1, \ldots, x_n]) = n$

Proof.

- Let $R = k[x_1, \ldots, x_n]$. We know that $\mathrm{ht}(x_1, \ldots, x_n) = n$, so we only need to show that $\dim(R) \leq n$. We use induction on n. For $n = 0$ (and $n = 1$) the statement is clear.
- Take a prime $P_1 \subset k[x_1, \ldots, x_n]$ of height one. Let $\overline{R} = R/P_1$. By the Remark above, $\overline{R}$ is finite extension of a polynomial ring $k[x_1, \ldots, x_j]$ with $j < n$, so $\dim(\overline{R}) \leq n - 1$.
- This implies that any chain of primes in R containing P_1 has length bounded by n, and so $\dim(k[x_1, \ldots, x_n]) \leq n$.

Since dimension is preserved under integral extensions we get:

Corollary

In the setup of the Noether Normalization, $\dim(R) = d$*, that is dimension of a finitely generated* k*-algebra* R *equals the maximal number of algebraically independent elements in* R*.*

Example

Let $R = k[x, y]/(y^2 - x^3 - x)$. Then R is integral over $k[x]$, as the generator y satisfies the monic equation $y^2 - (x^3 + x) = 0$ over $k[x]$. In particular, $\dim(R) = \dim(k[x]) = 1$. The geometric intuition behind this example: R is the ring of functions on the elliptic curve $y^2 = x^3 + x$, and projecting the curve onto the x-axis is a (ramified) covering map of degree 2. We go back to this interpretation in the chapter on Algebraic Sets.

The basic correspondence between k-algebras and algebraic sets starts with Hilbert's Nullstellensatz. The correspondence simplifies over algebraically closed fields.

Algebraically closed fields

Definition

A field k is algebraically closed if every polynomial in $k[X]$ has a root in k. (This implies that every polynomial in $k[X]$ factors into a product of linear factors.)

Example

Fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{Z}/p\mathbb{Z}$ (prime p) are not algebraically closed. The Fundamental Theorem of Algebra states that $\mathbb{C}$ is algebraically closed.

Proposition

Let k be an algebraically closed field and let $k \subset L$ be a field extension. If L is finite over k then $k = L$.

Proof.

By assumption, any $a \in L$ is integral over k, say $f(a) = 0$ for $f \in k[X]$. But all roots of f are in k, hence $a \in k$. $\square$

Maximal ideals of $k[x_1, \ldots, x_n]$

For any $a_1, \ldots, a_n \in k$,

$$m_a := (x_1 - a_1, \ldots, x_n - a_n) \subset k[x_1, \ldots, x_n]$$

is a maximal ideal (because the k-algebra homomorphism $k[x_1, \ldots, x_n] \to k$ sending x_i to a_i is surjective, and m_a is its kernel). We shall see that when k is algebraically closed, all maximal ideals of $k[x_1, \ldots, x_n]$ have this form. This statement is one of the forms of the **Hilbert Nullstellensatz** (German: Hilbert's theorem about zeros).

If $n = 1$, so that $R = k[x]$, the statement is easy. All maximal ideals have the form $I = (f)$ with f irreducible. If k is algebraically closed, f must be a linear polynomial, so $I = (x - a)$.

For $n \geq 2$ Hilbert Nullstellensatz is a highly nontrivial statement for which several proofs exist. Our proof relies on the so-called Zariski Lemma, which in turn is based on integral extensions and Noether Normalization.

Theorem (Zariski's Lemma)

Let $k \subset L$ be a field extension such that L is a finitely generated k-algebra. Then L finite over k, i.e. L is a finite field extension of k. In particular, if k is algebraically closed, then $L = k$.

Proof.

- Apply Noether's Normalization Theorem to find algebraically independent $x_1, \ldots, x_d \in R$ such that R is finite over $A = k[x_1, \ldots, x_d] \subseteq R$.
- But R is a field, so the next lemma implies that $A = k[x_1, \ldots, x_d]$ must be a field too which holds only if $d = 0$. Thus R is finite over k.

□

Lemma

Let $R \subset S$ be an integral extension. Then R is a field if and only if S is a field.

For the proof of the Lemma, see Problem Sheet for this week.

Theorem (Hilbert's Nullstellensatz, first form)

Let k be an algebraically closed field. All maximal ideals in $R = k[x_1, \ldots, x_n]$ have the form $m = (x_1 - a_1, \ldots, x_n - a_n)$ for $(a_1, \ldots, a_n) \in k^n$.

Proof.

- The composition of $k \subset R \to R/m$ is a ring homomorphism whose kernel is either k or 0. But $1 \in k$ is not in the kernel so $k \subseteq R/m$. Let $L = R/m$ (this is a field).
- L is a finitely generated k algebra, because R is. Zariski's Lemma implies that $k \subset L$ is a finite extension, hence $L = k$ because k is algebraically closed.
- Now we see elements of k represent all equivalence classes modulo m so that for all $1 \leq i \leq n$ we can find $a_i \in k$ such that $x_i - a_i \in m$ and so $m_a = (x_1 - a_1, \ldots, x_n - a_n) \subseteq m$.
- Both ideals are maximal, so $m_a = m$.

Algebraic sets

k is a field.

Definition

For any $S \subseteq k[x_1, \ldots, x_n]$ we define

$$V(S) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}.$$

An **algebraic subset** of k^n is the set of the form $V(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$.

Example

(a) $V(x_1^2 + x_2^2 - 1) \subseteq \mathbb{R}^2$ is a circle with center at the origin and radius 1.

(b) $V(x_1 x_2 x_3) \subseteq \mathbb{R}^3$ is the union of the planes $x_1 = 0$, $x_2 = 0$, $x_3 = 0$.

(c) The algebraic subsets of k are its finite subsets and the whole of $k = V(0)$.

Proposition

Let $R = k[x_1, \ldots, x_n]$, let $S \subseteq R$ be any subset and let $I = \langle S \rangle$ be the ideal generated by I. Then $V(S) = V(I)$.

Proof.

- Since $S \subseteq I$, $V(S) \supseteq V(I)$.
- To show the opposite inclusion, pick any $f \in I = \langle S \rangle$, and write it as

$$f = r_1 s_1 + \cdots + r_k s_k$$

where $r_1, \ldots, r_k \in R$ and $s_1, \ldots, s_k \in S$ and pick any $a \in V(S)$. Now $f(a) = r_1(a)s_1(a) + \cdots + r_k(a)s_k(a) = 0$ and we deduce that $a \in V(I)$.

□

Thus when considering algebraic sets we may restrict ourselves to $V(I)$, $I \subset R$ ideal. Furthermore since finitely generated k-algebras are Noetherian, the ideal I is finitely generated: $I = (f_1, \ldots, f_k)$, hence $V(I) = V(f_1, \ldots, f_k) = V(f_1) \cap \ldots V(f_k)$.

Proposition

Write $R = k[x_1, \ldots, x_n]$.

(a) *For any ideals* $I, J \subseteq R$, $I \subseteq J \Rightarrow V(I) \supseteq V(J)$.

(b) $V(R) = \emptyset$ *and* $V(0) = k^n$.

(c) *For any ideals* $I, J \subseteq R$, $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

(d) *For any set of ideals* $\{I_\lambda\}_{\lambda \in \Lambda}$ *of* R, $V(\sum_{\lambda \in \Lambda} I_\lambda) = \cap_{\lambda \in \Lambda} V(I_\lambda)$.

Proof.

(a) and **(b)** are straightforward.

(c) Since $IJ \subseteq I \cap J$ and $I \cap J$ is contained in both I and J, (a) implies that $V(IJ) \supseteq V(I \cap J) \supseteq V(I) \cup V(J)$. On the other hand, if $a \notin V(I) \cup V(J)$, there exist $f \in I$ and $g \in J$ such that $f(a) \neq 0$ and $g(a) \neq 0$. Now $fg(a) \neq 0$ so $a \notin V(IJ)$. We deduce that $V(IJ) \subseteq V(I) \cup V(J)$.

(d) Since $\sum_{\lambda \in \Lambda} I_\lambda \supseteq I_\mu$ for all $\mu \in \Lambda$, $V(\sum_{\lambda \in \Lambda} I_\lambda) \subseteq \cap_{\lambda \in \Lambda} V(I_\lambda)$. On the other hand, if $a \in \cap_{\lambda \in \Lambda} V(I_\lambda)$ and $f \in \sum_{\lambda \in \Lambda} I_\lambda$, write $f = f_{\lambda_1} + \cdots + f_{\lambda_m}$ with $\lambda_1, \ldots, \lambda_m \in \Lambda$ and verify that $f(a) = f_{\lambda_1}(a) + \cdots + f_{\lambda_m}(a) = 0$. □

We use the notation $\mathbb{A}^n$, for k^n considered as an algebraic set and we call $\mathbb{A}^n$ the n-**dimensional affine space** over k.

Definition

For any subset $X \subseteq \mathbb{A}^n$ we define

$$I(X) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \text{ for all } x \in X\}.$$

Lemma

$I(X)$ is a radical ideal of $k[x_1, \ldots, x_n]$.

Proof is a straightforward exercise.

Example

Let $X = \{\lambda_1, \ldots, \lambda_n\} \subset \mathbb{A}^1$. Then

$$I(X) = \big((x - \lambda_1) \cdots (x - \lambda_n)\big) \subset k[x].$$

Proposition

Let k be a field.

(a) *For any $U \subseteq V \subseteq \mathbb{A}^n$, $\mathrm{I}(U) \supseteq \mathrm{I}(V)$.*

(b) $\mathrm{I}(\emptyset) = k[x_1, \ldots, x_n]$ *and if k is infinite,* $\mathrm{I}(\mathbb{A}^n) = 0$.

(c) *For any collection $\{U_\lambda\}_{\lambda \in \Lambda}$ of subsets of k^n,* $\mathrm{I}(\cup_{\lambda \in \Lambda} U_\lambda) = \cap_{\lambda \in \Lambda} \mathrm{I}(U_\lambda)$.

(d) *If $X \subseteq k^n$ is an algebraic set, then $V(I(X)) = X$.*

Proof.

(a) and first part of (b) are easy.

Assume k is infinite. We need to show that for any non-zero $f \in k[x_1, \ldots, x_n]$ there exists a $a \in k^n$ such that $f(a) \neq 0$.

We proceed by induction on n, the case $n = 1$ being well known.

Write $f = g_d x_n^d + \cdots + g_0$ where $g_0, \ldots, g_d \in k[x_1, \ldots, x_{n-1}]$. If there exists a $b \in k^{n-1}$ for which $g_i(b) \neq 0$ for some $0 \leq i \leq d$ then the case $n = 1$ produces an $a \in k$ such that $f(a, b) \neq 0$. If no such b exists, the induction hypothesis implies that $g_0, \ldots, g_d = 0$ hence $f = 0$.

As for (c),

$$\begin{aligned} f \in \mathsf{I}(\cup_{\lambda\in\Lambda} U_\lambda) &\Leftrightarrow f(a) = 0 \text{ for all } a \in \cup_{\lambda\in\Lambda} U_\lambda \\ &\Leftrightarrow \text{ for all } \lambda \in \Lambda, f(a) = 0 \text{ for all } a \in U_\lambda \\ &\Leftrightarrow f \in \cap_{\lambda\in\Lambda} \mathsf{I}(U_\lambda) \end{aligned}$$

To prove (d) write $X = V(J)$ for some ideal $J \subseteq k[x_1, \ldots, x_n]$. Now $I(V(J)) \supseteq J$ and so $V(I(V(J))) \subseteq V(J) = X$. The reverse inclusion is straightforward. □

Remark

If k is a finite field, e.g. $k = \mathbb{Z}/p$, then there exist polynomials $f \in k[x_1, \ldots, x_n]$ which are zero for every point $a \in k^n$, so that $I(\mathbb{A}^n) \neq 0$. For example: $f(x) = x^p - x$ is zero for every $a \in \mathbb{Z}/p$ by Fermat's Little Theorem. Thus in this case $I(\mathbb{A}^1) \neq 0$.

We are going to establish a bijection between algebraic sets and radical ideals given by $X \mapsto I(X)$ and $I \mapsto V(I)$ in the case when k is algebraically closed. The next step is:

Theorem (Hilbert Nullstellensatz, second form)

Let k be an algebraically closed field, let $J \subseteq k[x_1, \ldots, x_n]$ be an ideal. We have $\mathrm{I}(V(J)) = \sqrt{J}$.

We write $R = k[x_1, \ldots, x_n]$.

Proof of the second form of Hilbert Nullstellensatz begins

The proof is a bit complicated, because the statement we are up to is strong and nontrivial!

- The inclusion $I(V(J)) \supset J$, is obvious. Now since $I(V(J))$ is a radical ideal we also have $I(V(J)) \supset \sqrt{J}$.
- We need to show the opposite inclusion $I(V(J)) \subset \sqrt{J}$.
- Assume that $f \notin \sqrt{J}$. We will prove that $f(a) \neq 0$ for some $a \in V(J)$.
- Since $\sqrt{J} = \bigcap_{P \supset J} P$, we have $f \notin P$ for some prime ideal $P \supset J$.
- We now find a maximal ideal $m \supset P \supset I$ such that $f \notin m$.

Proof of the second form of Hilbert Nullstellensatz ends

- For that consider the quotient $B = R/P$, and then localize $C = B[1/\overline{f}]$. This gives a composition of k-algebra homomorphisms
$$R \to B \to C.$$
- Let m_C be a maximal ideal in C; since the image of f is a unit in C we have $\overline{f} \notin m_C$. Let m be the preimage of m_C to R. One way to see that this is a maximal ideal (contractions of maximal ideals are not maximal in general!) is to note that by Zariski Lemma $C/m_C = k$, so that $R/m = k$ as well.
- We have found a maximal ideal $m \supset J$ in R such that $f \notin m$.
- By the first form of Hilbert Nullstellensatz we have $m = m_a$ for some $a \in k^n$.
- Now $a \in V(J)$, but $f(a) \neq 0$ (because the value $f(a)$ equals to the class of f modulo m_a).
- Done!

Theorem

Let k be an algebraically closed field. The assignment $J \mapsto V(J)$ gives an order-reversing bijection:

$$\{\textit{Radical ideals in } k[x_1, \ldots, x_n]\} \leftrightarrow \{\textit{Algebraic subsets of } \mathbb{A}^n\}$$

with the inverse bijection given by $X \mapsto I(X)$.

Proof.

- We've seen that $J \mapsto V(J)$ is order reversing, and that $V(I(X)) = X$ for an algebraic set X
- Hilbert Nullstellensatz tells us that $J(V(I)) = I$ for radical ideals I.

□

From now on until the end of the chapter k is an algebraically closed field.

Polynomial functions on an algebraic set

Definition

Let X be an algebraic set. Then $R_X = k[x_1, \ldots, x_n]/I(X)$ is called the **algebra of polynomial functions on** X.

To clarify the definition, let $f, g \in k[x_1, \ldots, x_n]$. We have

$$f(a) = g(a) \text{ for all } a \in X \iff f - g \in I(X).$$

Thus elements of R_X give well-defined (polynomial) functions on X.

Example

- Let $X = V(y) \subset \mathbb{A}^2$ be the horizontal axis. Then $I(X) = (y)$ and $R_X = k[x, y]/(y) = k[x]$. This shows that the polynomial functions on the line $y = 0$ in $\mathbb{A}^2$ are polynomials in x.
- Let $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$ be the "circle over k". Then $R_X = k[x, y]/(x^2 + y^2 - 1)$.

Points as maximal ideals

Proposition

Let $X \subset \mathbb{A}^n$ be an algebraic set, and let $R_X = k[x_1, \ldots, x_n]/I(X)$ be its algebra of functions. Then there is a bijection between the set of points $a \in X$ and the set of maximal ideals in R_X given by

$$a = (a_1, \ldots, a_n) \mapsto (\overline{x_1} - a_1, \ldots, \overline{x_n} - a_n) \subset R_X.$$

Proof.

- When $X = \mathbb{A}^n$, this statement is known to us as the first form of Hilbert Nullstellensatz. We need to check which ideals $m_a \subset k[x_1, \ldots, x_n]$ contain $I(X)$ (and thus descend to R_X).
- Now we notice that: $a \in X \iff m_a = I(a) \supset I(X)$. Thus a point a lies in X if and only if the corresponding maximal $m_a \subset k[x_1, \ldots, x_n]$ ideal contains $I(X)$ and descends to give a maximal ideal $\overline{m_a} \subset R_X$.

Irreducible algebraic sets

Definition

A non-empty algebraic set $X \subseteq \mathbb{A}^n$ is called **reducible** if there exist algebraic sets $Y, Z \subset \mathbb{A}^n$ properly contained in X for which $X = Y \cup Z$. An algebraic set which is not reducible is called **irreducible**.

Example

- $V(x_2 - x_1^2) \subset k^2$ is irreducible.
- $V(x_1 x_2 x_3) \subset k^2$ is reducible as

$$V(x_1 x_2 x_3) = V(x_1) \cup V(x_2) \cup V(x_3)$$

In the case

$$X = X_1 \cup \cdots \cup X_s$$

with X_i irreducible and $X_i \not\subset X_j$ we call the X_i's irreducible components of X.

Proposition

Let $X \subset \mathbb{A}^n$ be an algebraic set. The following conditions are equivalent:

(a) *X is irreducible*

(b) *$I(X) \subset R = k[x_1, \ldots, x_n]$ is a prime ideal*

(c) *$R_X = R/I(X)$ is a domain*

Proof of (a) $\Longrightarrow$ (b) $\Longleftrightarrow$ (c).

(b) and (c) are equivalent by one of the characterizations of prime ideals. Suppose that X is irreducible and suppose that $fg \in \mathrm{I}(X)$ for some $f, g \in R$. Now $X \subseteq V(fg) = V(f) \cup V(g)$ and so $X = (V(f) \cap X) \cup (V(g) \cap X)$.
Both sets in the union are algebraic, and since X is irreducible we deduce that either $X = V(f) \cap X$ or $X = V(g) \cap X$, i.e., $X \subseteq V(f)$ or $X \subseteq V(g)$, and we deduce that $f \in \mathrm{I}(X)$ or $g \in \mathrm{I}(X)$.

Proof of (b) $\implies$ (a).

Assume that $\mathsf{I}(X)$ is prime and that $X = X_1 \cup X_2$ where X_1 and X_2 are algebraic sets. We assume further that $X \neq X_1$ and show that $X = X_2$. Since $X \supsetneq X_1$, $I(X) \subsetneq I(X_1)$ and we can pick a $f \in I(X_1) \setminus I(X)$. Now for all $g \in I(X_2)$ we have $fg \in I(X)$, and since $I(X)$ is prime, we deduce that $g \in I(X)$. We conclude that $I(X_2) \subseteq I(X)$, and since the reverse inclusion also holds, we conclude that $I(X_2) = I(X)$ and hence that $X = X_2$. $\square$

Theorem

Every algebraic set $X \subseteq \mathbb{A}^n$ is the union of finitely many irreducible components. Irreducible components are uniquely defined.

Proof.

- According to the bijection between algebraic subsets of $\mathbb{A}^n$ and ideals of $k[x_1, \ldots, x_n]$, presenting X as a finite union of irreducible algebraic subsets X_i with $X_i \not\subset X_j$ is equivalent to presenting $I(X)$ as a finite intersection of prime ideals P_i with $P_i \not\supset P_j$.
- Since $k[x_1, \ldots, x_n]$ is Noetherian and $I(X)$ is radical, such a presentation exists and is unique up to ordering.

□

The dimension of algebraic sets

Definition

The **dimension** of an algebraic set $X \subseteq \mathbb{A}^n$ is the dimension of the ring of functions $R_X = k[x_1, \ldots, x_n]/I(X)$.

Theorem

Let $X \subseteq \mathbb{A}^n$ be an algebraic set, let $I = I(X) \subseteq k[x_1, \ldots, x_n]$. The following numbers are equal:

(a) *The dimension of X*

(b) *The maximal length of a chain of primes containing I*

(c) *The maximal length of a chain of irreducible algebraic sets contained in X*

Proof.

Follows from the bijection between the following sets: (a) prime ideals in R_X; (b) prime ideals in $k[x_1, \ldots, x_n]$ which contain $I(X)$; (c) irreducible algebraic subsets of X. □

Examples

- A point $P \in \mathbb{A}^n$ is algebraic set whose dimension is zero. More generally, any finite set $\{P_1, \ldots, P_r\} \subset \mathbb{A}^n$ of points is an algebraic set of dimension zero.
- The affine n-space $\mathbb{A}^n$ has dimension n. A maximal chain of irreducible subsets is

$$pt = \mathbb{A}^0 \subset \mathbb{A}^1 \subset \cdots \subset \mathbb{A}^n.$$

- The next example would be a **plane curve** $X = V(f) \subset \mathbb{A}^2$, e.g. $x^2 + y^2 = 1$. To show that $\dim(X) = 1$ we use Krull's Principal Ideal Theorem.

Geometric interpretation of Krull's Principal Ideal Theorem

Theorem

Let $X \subseteq \mathbb{A}^n$ be an irreducible algebraic set of dimension d and let $f \in R = k[x_1, \ldots, x_n]$. Either

(a) $X \cap V(f) = \emptyset$,

(b) $X \cap V(f) = X$, *or*

(c) *every irreducible component of $X \cap V(f)$ has dimension $d - 1$.*

Corollary

If $X = V(f_1, \ldots, f_r)$ and X is not empty, then every irreducible component of X has dimension at least $n - r$.

Example

The dimension of every irreducible component of a **hypersurface** (that is algebraic set given by one nonconstant equation $f \in k[x_1, \ldots, x_n]$), $V(f) \subset \mathbb{A}^n$ equals $n - 1$.

Proof of the Theorem.

- Write $X = V(P)$ for a prime $P \subset R$.
- We have $X \cap V(f) = V(P + fR)$ so (a) and (b) occur when $P + fR = R$ and $f \in P$, respectively.
- Thus (a), (b) don't occur precisely when the image $\overline{f}$ of f in R/P is not zero and not a unit.
- Irreducible components of $V(P + fR)$ correspond to minimal primes Q over $P + fR$, and by Krull's Principal Ideal Theorem applied to $Q/P = (\overline{f}) \subset R/P$, $\operatorname{ht} Q/P = 1$.
- We use the fact that polynomial algebras are catenary (Exercises for Chapter on Integral Dependence) to deduce that $\dim R/Q = \dim(R/P)/(Q/P) = \dim(R/P) - \operatorname{ht} Q/P = \dim X - 1$.

□

Proof of the Corollary.

Induction on r. □

Tangent spaces

Let R be a ring, and and let $m \subset R$ be a maximal ideal with quotient field $k = R/m$. Consider an R-module $V = m/m^2$ with an obvious action $r \cdot \overline{x} = \overline{rx}$. Since m annihilates V, V is an R/m-module, i.e. a vector space over k.

Definition

The dual k-vector space $V^* = (m/m^2)^*$ is called the tangent space to R at m. In the case of $R = R_X$ for an algebraic set $X \subset \mathbb{A}^n$ we will refer to the tangent space to R at $m = m_a$ as the tangent space to X at a. Notation: $T_{m,R}$, $T_{a,X}$.

Example

$R = k[x_1, \ldots, x_n]$, $m = (x_1 - a_1, \ldots, x_n - a_n)$. Let $y_i = x_i - a_i$. We have $f \in m \iff f(y_1, \ldots, y_n) = \sum_{i=1}^n A_i y_i + O(y^2)$ and $f \in m^2 \iff f(y_1, \ldots, y_n) = \sum_{i,j=1}^n B_{ij} y_i y_j + O(y^3)$. Hence m/m^2 consists of $A_1\overline{y_1} + \cdots + A_n\overline{y_n}$, $A_i \in k$. We may write $dy_i = \overline{y_i}$, so that the dual space $T_{0,\mathbb{A}^n} = (m/m^2)^*$ is spanned by "directional derivatives" ∂_i.

Tangent space geometrically

Proposition

Let $X = V(f_1, \ldots, f_r) \subset \mathbb{A}^n$ be an algebraic set. The tangent space to X at $a \in X$ can be identified with the following vector subspace of $\mathbb{A}^n$:

$$\{(\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n \mid \frac{\partial f_i(a)}{\partial x_1}\alpha_1 + \cdots + \frac{\partial f_i(a)}{\partial x_n}\alpha_n = 0 \ \ \forall i = 1 \ldots r\}.$$

Proof.

We consider m/m^2, and then take the dual vector space. We change the coordinates to $y_j = x_j - a_j$ and write Taylor expansions for every f_i:

$$f_i(y_1, \ldots, y_n) = 0 + \frac{\partial f_i(a)}{\partial x_1} y_1 + \cdots + \frac{\partial f_i(a)}{\partial x_n} y_n + O(y^2).$$

Computing $m_a/m_a^2 = (y_1, \ldots, y_n)/((y_i y_j)_{i,j=1}^n + I(f))$ yields a quotient k-vector space

$$\frac{k dy_1 \oplus \cdots \oplus k dy_n}{(\frac{\partial f_i(a)}{\partial x_1} dy_1 + \cdots + \frac{\partial f_i(a)}{\partial x_n} dy_n)_{i=1}^r} = V/L$$

and the dual space is the one we need:

$$(V/L)^* = L^\perp = \{(\alpha_1, \ldots, \alpha_n) : \sum_{i=1}^n \frac{\partial f_i(a)}{\partial x_i} \alpha_i = 0\} \subset V^* = k^n.$$

Tangent space to a hypersurface

Example

If $X = V(f) \subset \mathbb{A}^n$, i.e. X is given by one equation

$$f(x_1, \ldots, x_n) = 0,$$

then the tangent space to X at $a \in X$ has the form

$$T_{a,X} = \{(\alpha_1, \ldots, \alpha_n) \in k^n : \frac{\partial f(a)}{\partial x_1}\alpha_1 + \cdots + \frac{\partial f(a)}{\partial x_n}\alpha_n = 0\} \subset k^n.$$

Thus there are two cases: $T_{a,X} = k^n$ (when all partial derivatives of f are zero at a), or $T_{a,X}$ has dimension $n-1$ (when at least one of the partial derivatives of f is not zero at a).

Dimension of the tangent space

Proposition

Let (R, m) be a local Noetherian ring. Then

1. $\dim T_{m,R} =$ *minimal number of generators of* $m \subset R$
2. $\dim T_{m,R} \geq \dim R$

Proof.

1. This follows from Nakayama's Lemma (see Chapter on Modules) applied to R-module $M = m$.
2. Let $d = \dim T_{m,R}$. Part (1) implies that m is generated by d elements $f_1, \ldots, f_d \in m$. Now by Krull's principal ideal theorem applied inductively we get

$$\dim R/(f_1, \ldots, f_j) \geq \dim R - j.$$

In particular, for $j = d$ we get

$$0 = \dim R/m \geq \dim R - d$$

Regular rings and non-singular algebraic sets

Definition

- A local ring (R, m) is called **regular** if $\dim R = \dim T_{m,R}$.
- A ring R is called regular if for every maximal $m \subset R$ the localization R_m is regular.
- An irreducible algebraic set X is called **nonsingular** if the ring R_X is regular.

Example

Let $X = V(f) \subset \mathbb{A}^n$. Then $\dim X = \dim(R_X)_m = n - 1$ for every maximal ideal $m \subset R_X$. It follows from the description of the tangent space $T_{a,X}$ given previously that X is nonsingular if and only if for every $a \in X$ the derivatives $\partial f / \partial x_i(a)$ do not vanish simultaneously.

Thus $y = x^2$ is a nonsingular plane curve, and $y^2 = x^3$ is singular at $(0, 0)$.

Proposition (Jacobian criterion)

Let $X = V(f_1, \ldots, f_r) \subset \mathbb{A}^n$ be an algebraic set. If the Jacobian matrix

$$J = \left(\frac{\partial f_i}{\partial x_j}(a) \right)_{i=1\ldots r, j=1\ldots n}$$

has rank r for every $a \in X$, then X is non-singular of dimension $n - r$.

Proof.

Note that if $X \neq \emptyset$, then by Krull's principal ideal theorem we have $\dim(X) \geq n - r$. We've seen that the tangent space $T_{a,X}$ to X at a is given by the kernel of $J : k^n \to k^r$. Since J has rank r, the kernel has dimension $n - r$. Thus we have

$$\dim T_{a,X} = n - r \leq \dim X$$

and the converse inequality holds always. □

Hom is left exact

For R-modules M and N we write $\mathrm{Hom}(M, N)$ for the set of R-module homomorphisms. In fact, $\mathrm{Hom}(M, N)$ is an R-module under the operations

$$(f + g)(m) = f(m) + g(m), \quad (r \cdot f)(m) = r \cdot (f(m)).$$

Lemma

The functor Hom *is left exact in both arguments, i.e. if*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

is a short exact sequence of R-modules, then for every R-module N we have a exact sequences

$$0 \to \mathrm{Hom}(N, M') \xrightarrow{i_*} \mathrm{Hom}(N, M) \xrightarrow{p_*} \mathrm{Hom}(N, M'') \qquad (1)$$

and

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{p^*} \mathrm{Hom}(M, N) \xrightarrow{i^*} \mathrm{Hom}(M', N). \qquad (2)$$

Proof.

This is what is called "diagram chase" or "abstract nonsense". I will prove (1) in detail, and (2) is very similar.

To show that (1) is exact, I need to check that i_* is injective and that $Ker(p_*) = Im(i_*)$.

i_* is injective for the following reason: if $f \in \mathrm{Hom}(N, M')$ and $i_*(f) = i \circ f : N \to M$ is a zero homomorphism, then since i is injective, f itself is zero.

For the second claim, let $g \in \mathrm{Hom}(N, M)$. We have

$$g \in Ker(p_*) \iff p \circ g = 0 \iff Im(g) \subset M',$$

which is equivalent to existence of $f \in Hom(N, M')$ such that

$$g = i \circ f.$$

Hom is not exact

Example

Consider short exact sequence of $\mathbb{Z}$-modules (note: $\mathbb{Z}$ modules are same things as abelian groups):

$$0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n \to 0.$$

Apply $\mathrm{Hom}(\bullet, \mathbb{Z})$ to this sequence:

$$0 \to \mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \to 0.$$

Here $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}$, but the first term is zero: $\mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}) = 0$ as there are no non-trivial homomorphisms $\mathbb{Z}/n \to \mathbb{Z}$. Thus the sequence rewrites as

$$0 \to 0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to 0.$$

It is not exact as the multiplication by n map is not surjective!

Projective modules

Definition

We call an R-module P **projective** if $\mathrm{Hom}(P, \bullet)$ is exact, i.e. for every s.e.s. $0 \to M' \to M \to M'' \to 0$ the corresponding sequence

$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'') \to 0$$

is exact.

Proposition

The following conditions are equivalent:

(a) *P is projective*

(b) *For every surjective homomorphism $p : N \to P$ there exists a homomorphism $j : P \to N$ satisfying $p \circ j = id_P$. (Such a j is autmoatically injective, and is called a* **section** *of p, or a splitting of p.)*

(c) *P is a direct summand of a free module*

In particular, free modules are projective.

Proof.

(a) $\Longrightarrow$ (b): consider a surjective homomorphism $p : N \to P$, a write the corresponding short exact sequence with $K = Ker(p)$: $0 \to K \to N \xrightarrow{p} P \to 0$. Applying the $\mathrm{Hom}(P, \bullet)$ functor using that P is projective we get a short exact sequence

$$0 \to \mathrm{Hom}(P, K) \to \mathrm{Hom}(P, N) \xrightarrow{p_*} \mathrm{Hom}(P, P) \to 0.$$

Since p_* is surjective the identity element $1_P \in \mathrm{Hom}(P, P)$ satisfies $1_P = p_*(j) = pj$ for some $j \in \mathrm{Hom}(P, N)$.

(b) $\Longrightarrow$ (c): every module is a quotient of a free module, which gives a surjective homomorphism $p : F \to P$. It admits a section j, which yields the direct sum decomposition $F = j(P) \oplus Ker(p)$.

(c) $\Longrightarrow$ (a): This follows from two statements, each of them is easy to see: a free module is projective and a direct summand of a projective module is projective.

Examples of projective modules

Example

If $R = k$ is a field, then every module is projective.

Example

- $\mathbb{Z}$ is a projective $\mathbb{Z}$-module.
- $\mathbb{Z}/n$ is not a projective $\mathbb{Z}$-module, as the surjective homomorphism $p : \mathbb{Z} \to \mathbb{Z}/n$ has no sections.

Remark

More generally, over a PID R (such as $\mathbb{Z}$ or $K[x]$) a module M is projective if and only if it is torsion-free, i.e.

$$rm = 0 \implies r = 0 \text{ or } m = 0.$$

Intuition for projective modules

Algebraic Number Theory

Let $K/\mathbb{Q}$ be a finite field extension, and $\mathcal{O}_K$ be the ring of integers. Then $\mathcal{O}_K$ is what is called a **Dedekind domain**: a Noetherian regular domain of dimension one. In this case non-zero (fractional) ideals $I \subset \mathcal{O}_K$ are the same as projective $\mathcal{O}_K$-modules of rank 1. Here free modules correspond to principal ideals.

Algebraic Geometry / Topology

Let $X \subset K^n$ be an algebraic set, and let

$$R = R_X = K[x_1, \ldots, x_n]/I(X)$$

be its coordinate ring. Then for every finitely generated projective module M over X there is a vector bundle $\widetilde{M} \to X$ such that M is the set of global sections of $\widetilde{M} \to X$. This establishes a bijection between algebraic vector bundles on X and finitely generated projective R-modules. Here free modules correspond to trivial vector bundles.

The Grothendieck group of a ring R

Definition

Let R be a ring. The **Grothendieck group** $K_0(R)$ is a free abelian group with generators $[P]$ for every isomorphism class of finitely generated projective R-modules modulo relations:

$$[P \oplus Q] - [P] - [Q] = 0.$$

The Grothendieck group $K_0(R)$ has a structure of a commutative ring with multiplication induced by $[P] \cdot [Q] = [P \otimes Q]$ and $1 = [R]$ (exercise!).

This group measures the difference between projective and free modules over R, and is the algebraic analog of topological $K_0(X)$ of vector bundles on X.

Remark

There is a surjective homomorphism $rk : K_0(R) \to \mathbb{Z}$ which maps every free module R^n to its rank n. If every projective module is free, rk is an isomorphism.

The Grothendieck group of a ring R: Examples

Example

For $R = k$, a field we have $K_0(k) = \mathbb{Z}$, as every module is free.

Example

For $R = \mathbb{Z}$ we have $K_0(R) = \mathbb{Z}$ as every finitely generated projective module is free. More generally if $R = \mathcal{O}_K$ is a ring of integers in a number field K, we have

$$K_0(\mathcal{O}_K) = \mathbb{Z} \oplus Cl(K)$$

($Cl(K)$ is the ideal class group of K).

Example

If $R = k[x_1, \ldots, x_n]$, then $K_0(R) = \mathbb{Z}$. To prove this requires some cohomological machinery. Morally this follows from the fact that the corresponding algebraic set, $\mathbb{A}^n$ is contractible.

Projective resolutions

For an R-module M we can construct its **projective resolution**:

$$\cdots \to P_n \to \cdots \to P_2 \to P_1 \to P_0 \to M.$$

By definition a projective resolution is an exact sequence as above with all terms P_i's being projective. Sometimes the resolution is **finite** i.e. has the form

$$\cdots \to 0 \to \cdots \to 0 \to P_n \to \cdots \to P_2 \to P_1 \to P_0 \to M,$$

in which case we omit zeros at the left, and call n the length of the resolution.

Example

$\mathbb{Z}/n$ has a finite projective resolution: $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n$. This resolution has length 1.

Existence of projective resolutions

Projective resolutions exist, but they are not always finite. To construct a resolution we may use free modules as follows. Start with a surjective homomorphism $F_0 \to M$ from a free module F_0, extend to an exact sequence

$$0 \to K_0 \to F_0 \to M \to 0.$$

Then apply the same procedure to K_0:

$$0 \to K_1 \to F_1 \to K_0 \to 0,$$

and so on. The resulting short exact sequences can be put in one long exact sequence:

$$\cdots \to F_1 \to F_0 \to M$$

which is a free, and hence projective resolution of M.

Minimal free resolutions

Let R be Noetherian and M finitely generated. If we apply the inductive procedure above by choosing minimal set of generators of K_j to construct each of the free modules F_j, we get a **minimal** free resolution of M.

Lemma

Let R be a local Noetherian ring with maximal ideal m and let $F_\bullet$:

$$\cdots \to F_n \stackrel{d_n}{\to} F_{n-1} \stackrel{d_{n-1}}{\to} \ldots \stackrel{d_1}{\to} F_0 \to M \to 0$$

be a free resolution of M. Then $F_\bullet$ is a minimal resolution if and only if differentials in the complex $F_\bullet \otimes R/m$ are all zero.

Proof.

- We cut the resolution into short exact sequences with $K_j = \mathrm{Im}(d_j)$: $0 \to K_{j+1} \to F_j \to K_j \to 0$. By definition the resolution is minimal if the surjections $F_j \to K_j$ map a basis of F_j to the minimal set of generators of K_j. Let $e_1, \ldots, e_n$ be a basis of F_j, and let $x_1, \ldots, x_n$ be their images in K_j.
- By Nakayama's Lemma applied to $x_1, \ldots, x_n \in K_j$ these are minimal generators of K_j if and only if their images in K_j/m_jK_j form a basis. Thus the requirement of minimality is equivalent to all $F_j/m_jF_j \to K_j/m_jK_j$ being isomorphisms of k-vector spaces ($k = R/m$).
- Now recall we apply the right exact functor $\otimes_R k$ to the short exact sequence above: $K_{j+1} \otimes k \to F_j \otimes k \to K_j \otimes k \to 0$, and recall that $F_j \otimes k \simeq F_j/mF_j$ and similarly for K_j. Thus the resolution is minimal if and only if all the maps $K_{j+1} \otimes k \to F_j \otimes k$ are zero, and since $F_{j+1} \to K_{j+1}$ are all surjective, the condition on minimality is equivalent to the maps $F_{j+1} \otimes k \to F_j \otimes k$ being all zero.

Chain complexes and their homology

Definition

- A sequence (finite or infinite, but not necessarily an exact one)

$$\ldots \to C^{n-1} \overset{d^{n-1}}{\to} C^n \overset{d^n}{\to} C^{n+1} \to \ldots$$

  is called a **chain complex** if $d^n d^{n-1} = 0$ for every n.
- **Cohomology groups** of a chain complex are defined as

$$H^n(C) := Ker(d^n)/Im(d^{n-1}).$$

Example

- A chain complex is an exact sequence if and only all its homology groups are zero.
- Let $\mathbb{Z} \overset{\times d}{\to} \mathbb{Z} \overset{0}{\to} \mathbb{Z} \overset{\times d}{\to} \mathbb{Z} \overset{0}{\to} \mathbb{Z} \to \ldots$ be a complex with $\mathbb{Z}$ in degrees $n \geq 0$. Then all even degree cohomology groups are zero, and all odd degree cohomology groups $H^{2k+1} = \mathbb{Z}/d$.

Ext-groups

Definition

Let M, N be two R-modules. Then Ext-groups between them are defined as

$$\mathrm{Ext}^n(M, N) = H^n(\mathrm{Hom}(P_n, M)),\ n \geq 0,$$

where

$$\cdots \to P_n \to \cdots \to P_2 \to P_1 \to P_0 \to M$$

is any projective resolution of M. These are independent from a choice of the resolution (see the problem sheet).

Projective modules have no higher Ext-groups

Proposition

If P is projective, then for any N and any $n \geq 1$ we have

$$\mathrm{Ext}^n(P, N) = 0.$$

Proof.

A resolution of P is $P \to P$, so that

$$\mathrm{Ext}^n(P, N) = H^n(\mathrm{Hom}(P, N) \to 0 \to 0 \to \dots) = 0, \ n \geq 1.$$

Proposition

For any M,N we have a natural isomorphism

$$\mathrm{Ext}^0(M,N) = \mathrm{Hom}(M,N).$$

Proof begins.

Take a projective resolution of M:

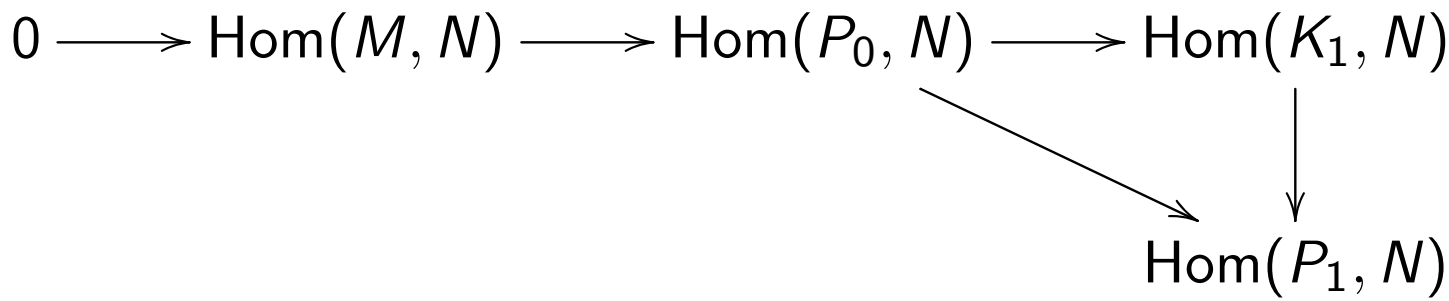
$$\cdots \to P_n \to \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to M.$$

Let $K_i = Im(d_i) = Ker(d_{i+1})$.
We may thus rewrite the original resolution as a list of short exact sequences:

$$0 \to K_1 \to P_0 \to M \to 0$$
$$0 \to K_2 \to P_1 \to K_1 \to 0$$
$$\cdots$$

Proof ends.

We consider a commutative diagram (i.e. a graph with modules as vertices and homomorphisms as edges with the property that for all paths between two vertices the compositions of homomorphism along the path are the same):



Here the sequence in the top row is exact, because Hom is left exact. The vertical arrow is injective, for the same reason. Altogether this implies that

$$\begin{aligned}\mathrm{Hom}(M,N) &= Ker(\mathrm{Hom}(P_0,N) \to \mathrm{Hom}(K_1,N)) = \\ &= Ker(\mathrm{Hom}(P_0,N) \to \mathrm{Hom}(P_1,N)) = \mathrm{Ext}^0(M,N).\end{aligned}$$

Ext-groups for $\mathbb{Z}$-modules

Example

We compute $Ext^i(\mathbb{Z}/p, \mathbb{Z}/q)$, where p and q are primes. By definition we may use projective resolution $0 \to \mathbb{Z} \stackrel{\times p}{\to} \mathbb{Z} \to \mathbb{Z}/p$ and then apply $\mathrm{Hom}(\bullet, \mathbb{Z}/q)$:

$$C^0 = \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/q) \to C^1 = \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/q)$$

which as a chain complex is $\mathbb{Z}/q \stackrel{d}{\to} \mathbb{Z}/q$, with d given by multiplication by p. We have

$$Ext^0(\mathbb{Z}/p, \mathbb{Z}/q) = Ker(d)$$
$$Ext^1(\mathbb{Z}/p, \mathbb{Z}/q) = \mathbb{Z}/q \Big/ Im(d)$$
$$Ext^{\geq 2}(\mathbb{Z}/p, \mathbb{Z}/q) = 0$$

If $p = q$, then $\mathrm{Ext}^0(\mathbb{Z}/p, \mathbb{Z}/p) = \mathrm{Ext}^1(\mathbb{Z}/p, \mathbb{Z}/p) = \mathbb{Z}/p$.
If $p \neq q$, then $\mathrm{Ext}^0(\mathbb{Z}/p, \mathbb{Z}/q) = \mathrm{Ext}^1(\mathbb{Z}/p, \mathbb{Z}/q) = 0$.

Ext-groups give long exact sequences

Proposition

If $0 \to M' \to M \to M'' \to 0$ *is a short exact sequence, then for any* N *we get long exact sequences:*

$$\begin{aligned} 0 &\to \mathrm{Hom}(N, M') \to \mathrm{Hom}(N, M) \to \mathrm{Hom}(N, M'') \to \\ &\to \mathrm{Ext}^1(N, M') \to \mathrm{Ext}^1(N, M) \to \mathrm{Ext}^1(N, M'') \to \\ &\to \mathrm{Ext}^2(N, M') \to \mathrm{Ext}^2(N, M) \to \mathrm{Ext}^2(N, M'') \to \dots \end{aligned}$$

and

$$\begin{aligned} 0 &\to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M'', N) \to \\ &\to \mathrm{Ext}^1(M'', N) \to \mathrm{Ext}^1(M, N) \to \mathrm{Ext}^1(M'', N) \to \\ &\to \mathrm{Ext}^2(M'', N) \to \mathrm{Ext}^2(M, N) \to \mathrm{Ext}^2(M'', N) \to \dots \end{aligned}$$

Proof.

See the problem sheet. □

Example

Consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z} \stackrel{\times n}{\to} \mathbb{Z}/n \to 0$$

and apply $\mathrm{Hom}(\bullet, \mathbb{Z})$ to it. We get a long exact sequence:

$$\begin{aligned} 0 \to \mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \stackrel{\times n}{\to} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \to \\ \to \mathrm{Ext}^1(\mathbb{Z}/n, \mathbb{Z}) \to \mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z}) \stackrel{\times n}{\to} \mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z}) \to 0. \end{aligned}$$

Using $\mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}) = 0$, $\mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z}) = 0$, the terms evaluate to:

$$\begin{aligned} 0 \to 0 \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \stackrel{\times n}{\to} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \to \\ \to \mathrm{Ext}^1(\mathbb{Z}/n, \mathbb{Z}) \to 0 \to 0 \to 0. \end{aligned}$$

Since the sequence is exact this computes

$$\mathrm{Ext}^1(\mathbb{Z}/n, \mathbb{Z}) = \mathbb{Z}/n.$$

Definition

Let M be an R-module. Its **projective dimension** is defined as

$$\mathrm{pd}(M) = \sup\{n : \exists N, Ext^n(M, N) \neq 0\}.$$

Proposition

The following conditions are equivalent:

(a) $\mathrm{pd}(M) = 0$

(b) $\mathrm{Ext}^1(M, N) = 0$ *for every R-module N*

(c) *M is projective*

Proof.

The proof goes as (a) $\implies$ (b) $\implies$ (c) $\implies$ (a).
For (b) $\implies$ (c) one needs the long exact sequence of Ext-groups, the rest follows from definitions. $\square$

Characterization of projective dimension

Theorem

Let R be a ring and M an R-module. The following conditions are equivalent:

(a) *There exists a projective resolution of M of length n.*

(b) $\mathrm{pd}(M) \leq n$.

(c) *For every projective resolution*

$$\cdots \to P_n \xrightarrow{d_n} P_{n-1} \to \cdots \to P_1 \to P_0$$

the kernel $Ker(d_n)$ is projective.

Proof.

(c) $\implies$ (a) $\implies$ (b) is straightforward using the definitions. For (b) $\implies$ (c) we write the long exact sequence

$$0 \to Ker(d_n) \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M$$

and using Dimension Shifting Lemma we get $\mathrm{pd}(Ker(d_n)) = 0$. $\square$

Dimension Shifting Lemma

If $0 \to M' \to P_{n-1} \to \dots P_0 \to \cdots \to M \to 0$ is a long exact sequence with all P_j's projective, then

$$\mathrm{pd}(M') = \max(\mathrm{pd}(M) - n, 0).$$

Proof.

We first do the case $n = 1$: $0 \to M' \to P \to M \to 0$ with P projective. For any module N we write the long exact sequence of $\mathrm{Ext}^*(\bullet, N)$-groups, using that $\mathrm{Ext}^n(P, N) = 0,\ n \geq 0$. The long exact sequence splits into:

$$0 \to \mathrm{Ext}^n(M', N) \to \mathrm{Ext}^{n+1}(M, N) \to 0,\ n \geq 1$$

This means that projective dimension of M' is that of M decreased by one, or zero in the case M has projective dimension zero itself. The general case is done using cutting the long exact sequence above into short exact sequences: $0 \to K_{j+1} \to P_j \to K_j \to 0$ with $K_j = Im(d_j : P_j \to P_{j-1})$, via induction on n. □

Global dimension of a ring

Definition

Let R be a ring. Its global dimension is defined as

$$\operatorname{gldim}(R) := \sup_M \operatorname{pd} M = \sup\{n : \exists M, N : \ Ext^n(M, N) \neq 0\}.$$

Remark

Auslander's Theorem says that to compute $\operatorname{gldim}(R)$ it suffices to take the supremum of $\operatorname{pd}(M)$ over finitely generated R-modules M.

Example

- If k is a field, then $\operatorname{gldim}(k) = 0$: every module is projective
- If R is a PID, and not a field, e.g. $R = k[x]$ or $R = \mathbb{Z}$, then $\operatorname{gldim}(R) = 1$
- More generally we have $\operatorname{gldim}(k[x_1, \ldots, x_n]) = n$ (this is not at all obvious!).

Koszul resolution of k over $R = k[x, y]$

The resolution starts with

$$k[x, y] \to k, \quad x \mapsto 0, y \mapsto 0.$$

The kernel of this surjective homomorphism is the ideal (x, y), so we continue

$$k[x, y] \oplus k[x, y] \overset{(x,y)}{\to} k[x, y] \to k.$$

Now the first homomorphism is not injective again, as any pair $(yf(x, y), -xf(x, y))$ maps to zero. One can see that the kernel is the submodule generated by one element $(y, -x)$, hence we extend the exact sequence

$$k[x, y] \overset{\binom{y}{-x}}{\to} k[x, y] \oplus k[x, y] \overset{(x,y)}{\to} k[x, y] \to k.$$

This time the first homomorphism is injective, as $k[x, y]$ is a domain. Our free resolution is:

$$0 \to k[x, y] \overset{\binom{x}{y}}{\to} k[x, y] \oplus k[x, y] \overset{(y,-x)}{\to} k[x, y] \to k.$$

$\mathrm{Ext}^j(k,k)$ for $R = k[x,y]$

We apply the $\mathrm{Hom}(\bullet, k)$ to the resolution obtained on the previous page, the resulting complex is:

$$k \xrightarrow{0} k^2 \xrightarrow{0} k.$$

Here we used that $Hom(k[x,y],k) = k$ and that the differentials are induced by multiplication by x and y which act trivially on k. We see that

$$\mathrm{Ext}^0(k,k) = k \quad \mathrm{Ext}^1(k,k) = k^2 \quad \mathrm{Ext}^2(k,k) = k.$$

This implies that

$$\mathrm{gldim}(k[x,y]) \geq \mathrm{pd}\, k \geq 2.$$

In fact these are equalities, but showing this requires more work.

Remark

For any $n \geq 1$ one can write the Koszul resolution of k over $k[x_1, \ldots, x_n]$. This will have length n and one will get $\mathrm{Ext}^j(k,k) = \Lambda^j(k^n)$ (exterior powers of a vector space).

Infinite global dimension: Example $R = k[x]/x^2$

Global dimension can be infinite, even for nice and small rings, such as for an Artinian ring $R = k[x]/x^2$. Let us compute $\mathrm{Ext}^i(k, k)$ for an R-module k (x acts trivially).

We start writing projective resolution of k using the surjective map $R \to k$. Its kernel is generated by x and we have a short exact sequence: $0 \to k \cdot x \to R \to k \to 0$. The projective resolution continues inifinitely:

$$\ldots \xrightarrow{x} R \xrightarrow{x} R \xrightarrow{x} R \to k.$$

We apply $\mathrm{Hom}(\bullet, k)$ to this resolution, using that $\mathrm{Hom}(R, k) = k$:

$$k \xrightarrow{0} k \xrightarrow{0} k \xrightarrow{0} \ldots$$

The differential maps are all zero as they are induced by multiplication by x which acts as zero on k. We see that for every $n \geq 0$ we have $\mathrm{Ext}^n(k, k) = Ker(0)/Im(0) = k$, and this implies that projective dimension of k and global dimension of R are both infinite.

Auslander-Buchsbaum-Serre Theorem

We finish the course with a theorem from the 1950s which unites much of what we have learnt about, namely, dimension, regularity and global dimension:

Theorem

Let (R, m) be a local ring with $k = R/m$. Then the following conditions are equivalent:

(a) *R is regular*

(b) $\operatorname{gldim}(R) := \sup_M \operatorname{pd} M$ *is finite, i.e. projective dimensions of R-modules are bounded*

(c) $\operatorname{pd} k < \infty$

In this case $\dim R = \operatorname{gldim}(R) = \operatorname{pd} k$.

This theorem is a true gem of Commutative Algebra. Equivalence (b) $\iff$ (c) is proved in the Problem Sheet. We will prove (a) $\implies$ (c) using Koszul complexes. We do not prove (c) $\implies$ (a).

Proof of (a) $\Longrightarrow$ (c) of the ABS Theorem

- R is a regular local ring. We will show that $k = R/m$ admits a finite free resolution; this would imply that $\mathrm{pd}(k) < \infty$. In fact we will prove that $\dim(R) = \mathrm{pd}(k)$.
- Let $x_1, \ldots, x_n$ be the minimal set of generators of m (so that $\dim(R) = n$).
- These elements form a regular sequence, that is every x_{i+1} is not a zero-divisor of $R/(x_1, \ldots, x_i)$ (Problem Sheet).
- Form the Koszul complex $K(x_1, \ldots, x_n)$; this is a complex of length n. Because $x_1, \ldots, x_n$ form a regular sequence, Koszul complex is a minimal free resolution of $R/(x_1, \ldots, x_n) = R/m = k$.
- Therefore $\mathrm{pd}(k) = n = \dim(R)$.