Algebra II
BMS - Basic Course Commutative Algebra
Wintersemester 2007/08

Personal notes of
Yves Radunz

Contents

Chapter 1

Modules

1.1 Rings

Lecture on 2007-10-18

Let $A = (A, +, \cdot)$ a *ring*, i.e.,

1. $(A, +)$ is an abelian group.
   (0 is the neutral element, $-a$ is the additive inverse of $a \in A$, $\forall a, b \in A : a + b = b + a$)
2. $(A, \cdot)$ is a semi-group.
3. distributivity:
   $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(b + c) \cdot a = b \cdot a + c \cdot a$

Assumption for most of the course

1. The multiplication is commutative.
2. $\forall a \in A : \exists 1 \in A : 1 \cdot a = a = a \cdot 1$

Remark
The following should be known:

1. $B \subseteq A$: a *subring*
2. $\mathfrak{a} \subseteq A$: an *ideal* ($\mathfrak{a} \cdot A = \mathfrak{a} = A \cdot \mathfrak{a}$)
3. $A/\mathfrak{a}$: *quotient ring* ($\pi : A \to A/\mathfrak{a}$, defined by $a \mapsto a + \mathfrak{a}$)
4. $f : A \to B$ *ring homomorphism*
   $(\forall a_1, a_2 \in A : f(a_1 + a_2) = f(a_1) + f(a_2), f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2))$
5. K *field*

Lemma 1.1. (1) *Let A be a ring, $\mathfrak{a} \supseteq A$ an ideal and $\pi : A \to A/\mathfrak{a}$ the canonical projection. Then, there is a bijection*
$\{\mathfrak{b} \subseteq A \text{ ideal} | \mathfrak{b} \supseteq \mathfrak{a}\} \overset{1:1}{\longleftrightarrow} \{\overline{\mathfrak{b}} \subseteq A/\mathfrak{a}, \text{ ideal}\}$.

Proof:
$\mathfrak{b} \mapsto \pi(\mathfrak{b}) =: \overline{\mathfrak{b}}$
$\overline{\mathfrak{b}} \mapsto \pi^{-1}(\overline{\mathfrak{b}}) =: b$
The two maps are inverses of each other, hence we get the desired bijection. □

Remark (recall)

1. *unit* (Einheit):
   $a \in A : \exists a^{-1} \in A : a \cdot a^{-1} = 1 = a^{-1} \cdot a$
   $A^\times = \{a \in A | a \text{ is a unit}\} \ni 1$ is a multiplicative group
2. *zero divisor* (Nullteiler):
   $0 \neq a \in A$ is a zero divisor iff $\exists 0 \neq b \in A : a \cdot b = 0$.
3. *nilpotent elements*:
   $a \in A$ is nilpotent iff $\exists n \in N : a^n = 0$.

Definition (prime ideal, spectrum)

1. An ideal $\mathfrak{p} \subset A$ is a *prime ideal*, iff $x \cdot y \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
   The *spectrum* of A is defined by $\text{Spec}(A) = \{\mathfrak{p} \subseteq A | \mathfrak{p} \text{ is a prime ideal}\}$.
2. An ideal $m \subset A$ is a *maximal ideal*, iff there is no ideal $\mathfrak{a}$ satisfying $m \subset \mathfrak{a} \subset A$.
   $\text{Max}(A) = \{m \supset A | m \text{ maximal ideal}\}$

Lemma 1.2. (2) *Let A be a ring.*
Then wie have the following:

1. *$\mathfrak{p}$ is a prime ideal $\Leftrightarrow$ $A/\mathfrak{p}$ is an* ingegral domain *(Integritätsbereich).*
2. *m is maximal $\Leftrightarrow$ $A/\mathfrak{m}$ is a field.*
3. *There exists a maximal ideal $\mathfrak{m} \subseteq A$.*

Proof:
$\rightarrow$ Problem 1 of the 1st Problem Set. □

Corollary 1.1. *Let A be a ring as before.*
Then, we have:

1. *Let $\mathfrak{a} \subseteq A$ be a fixed ideal. Then there is a miximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.*
2. *Each non-unit is contained in a maximal ideal.*

Proof:

1. Slight adaption of the proof of Lemma 2 3.
2. Let $a \in A \setminus A^\times$, then $\mathfrak{a} := (a) = \{a \cdot b | b \in A\} \subset A$.
   Now apply 1. to $\mathfrak{a} = (a) \subset A$: $\exists \mathfrak{m} \in \text{Max}(A) : a \in \mathfrak{m}$

□

Definition (local ring)
A is called a *local ring*, iff there is exactly one maximal ideal $\mathfrak{m}$.
$K = A/\mathfrak{m}$ is called the *residue field* of the local ring.

Definition (nilradical)
The set $\mathfrak{n}_A = \{x \in A | \exists n \in \mathbb{N}_{>0} : x^n = 0\}$ is called the *nilradical* of A.

Lemma 1.3. (3) *With the above notations, we have:*

1. $\mathfrak{n}_A \subseteq A$ *is an ideal.*
2. $\mathfrak{n}_A = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$

Proof:

1. $x, y \in \mathfrak{n}_A : \exists n_1, n_2 \in \mathbb{N}_{>0} : x^{n_1} = 0 = y^{n_2}$
   $(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j} = 0$
   $\Rightarrow x + y \in \mathfrak{n}_A$
   $x \in \mathfrak{n}_A : \exists n_1 \in \mathbb{N}_{>0} : x^{n_1} = 0$
   $a \in A \Rightarrow (a \cdot x)^{n_1} = a^{n_1} \cdot x^{n_1} = 0$
   $\Rightarrow ax \in \mathfrak{n}_A$
2. $\mathfrak{n} = \mathfrak{n}_A$, $\mathfrak{n}' = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$
   We want to show: $\mathfrak{n} = \mathfrak{n}'$.
   (a) $\mathfrak{n} \subseteq \mathfrak{n}'$
   Let $a \in \mathfrak{n}$ and $\mathfrak{p} \in \mathrm{Spec}(A)$.
   $\exists n \in \mathbb{N}_{>0} : a^n \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$
   $\Rightarrow a \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \Rightarrow a \in \mathfrak{n}'$
   $\Rightarrow \mathfrak{n} \subseteq \mathfrak{n}'$
   (b) $n' \subseteq n$
   We show this by showing $a \notin \mathfrak{n} \Rightarrow a \notin \mathfrak{n}'$:
   Let $a \notin \mathfrak{n}$, put $\Sigma = \{\mathfrak{a} \subseteq A | \forall n \in \mathbb{N}_{>0} : a^n \notin \mathfrak{a}\}$. Since $a \notin \mathfrak{n}$ we have $(0) \in \Sigma \Rightarrow \Sigma \neq \emptyset$.
   Using Zorn's Lemma, find a maximal ideal $\mathfrak{p} \in \Sigma$.
   We show: $\mathfrak{p} \in \mathrm{Spec}(A) : x, y \notin \mathfrak{p} \Rightarrow x \cdot y \notin \mathfrak{p}$
   Let $x, y \notin \mathfrak{p}$
   $\Rightarrow \mathfrak{p} + (x) = \{a + bx | a \in \mathfrak{p}, b \in A\}, \mathfrak{p} + (y)$ are *sum ideals*
   Since $x, y \notin \mathfrak{p}$, $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ are strictly bigger than $\mathfrak{p}$, hence $\mathfrak{p} + (x), \mathfrak{p} + (y) \notin \Sigma$ (since $\mathfrak{p}$ is maximal in Σ).
   $\Rightarrow \exists m, n \in \mathbb{N}_{>0} : a^m \in \mathfrak{p} + (x), a^n \in \mathfrak{p} + (y)$
   Multiplying yields $a^{m+n} \in \mathfrak{p} + (x \cdot y) \notin \Sigma$.
   $\Rightarrow x \cdot y \notin \mathfrak{p} \Rightarrow \mathfrak{p} \in \mathrm{Spec}(A)$
   In particular, we have $a \notin \mathfrak{p}$.
   $\Rightarrow a \notin \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} \Rightarrow a \notin \mathfrak{n}'$

□

Definition (jacobson radical)
The *Jacobson radical* $\mathcal{R}_A$ of A ist given by $\mathcal{R}_A := \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}$.

Lemma 1.4. (4) *With the above notations we have the equivalence:*
$x \in \mathcal{R}_A \Leftrightarrow \forall y \in A : 1 - x \cdot y \in A^\times$

Proof:

1. $\Rightarrow$

   Let $x \in \mathcal{R}_A$. Contrary to the claim assume, $1 - x \cdot y \notin A^\times$.

   $\Rightarrow \exists \mathfrak{m} \in \mathrm{Max}(A) : 1 - x \cdot y \in \mathfrak{m}$

   Since $x \in \mathfrak{m}'$ for all $\mathfrak{m}' \in \mathrm{Max}(A)$ hence $1 \in \mathfrak{m}$. $\Rightarrow \mathfrak{m} \in A \Rightarrow$ contradiction

   $\Rightarrow \forall y \in A : 1 - x \cdot y \in A^\times$

2. $\Leftarrow$

   We prove: $x \notin \mathcal{R}_A \Rightarrow 1 - x \cdot y \notin A^\times$ for any $y \in A$.

   Let $x \notin \mathcal{R}_A \Rightarrow \exists \mathfrak{m} \in \mathrm{Max}(A)$ such that $x \notin \mathfrak{m}$. Hence, $m + (x) = A \ni 1$.

   $\Rightarrow \exists y \in A, m \in \mathfrak{m} : m + x \cdot y = 1 \Rightarrow 1 - x \cdot y = m \in \mathfrak{m}$

   $\Rightarrow 1 - x \cdot y \notin A^\times$

□

Some comments on operations with ideals
Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals:

1. sum: $\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$

   inductively: define finite sum of ideals.

2. intersection: $\mathfrak{a} \cap \mathfrak{b} = \{a \in A | a \in \mathfrak{a}, a \in \mathfrak{b}\}$

   One can definie infinite intersections of ideals.

3. product: $\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{j=0}^{n} a_j \cdot b_j | a_j \in \mathfrak{a}, b_j \in \mathfrak{b}, n \in \mathbb{N}\}$

   inductively one can define finite products of ideals

Sum, intersection and product are commutative and assoziative respectively.
Distributivity between sums and intersection, i.e. $(\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot \mathfrak{c} + \mathfrak{b} \cdot \mathfrak{c}$, but distributivity fails for the intersections.

Definition (coprime)
Two ideals $\mathfrak{a}, \mathfrak{b}$ are called *coprime*, iff $\mathfrak{a} + \mathfrak{b} = (1)$.

Lemma 1.5. (5) *if* $\mathfrak{a}, \mathfrak{b}$ *are coprime, then* $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$.

Proof:
We show: $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$:
$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cdot A = \mathfrak{a}$
$\mathfrak{a} \cdot \mathfrak{b} \subseteq A \cdot \mathfrak{b} = \mathfrak{b}$
$\Rightarrow \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$
Now show: $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \cdot \mathfrak{b}$:
$\mathfrak{a} \cap \mathfrak{b} = A \cdot (\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a} \cdot (\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b} \cdot (\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a} \cdot \mathfrak{b}$. □

Remark
The union of two ideals need not to be an ideal!

Definition (ideal quotient, annihilator)
Let $\mathfrak{a}, \mathfrak{b}$ be two ideals of A.
Then, the *ideal quotient* $(\mathfrak{a} : \mathfrak{b})$ of $\mathfrak{a}$ and $\mathfrak{b}$ is defined by $(\mathfrak{a} : \mathfrak{b}) = \{x \in A | x \cdot \mathfrak{b} \subseteq \mathfrak{a}\}$
In particular, if $\mathfrak{a} = (0)$, then wie write $((0) : \mathfrak{b}) = (0 : \mathfrak{b}) =: \mathrm{Ann}(\mathfrak{b})$ which we call the *annihilator* of $\mathfrak{b}$.
$\mathrm{Ann}(\mathfrak{b}) = \{x \in A | x \cdot \mathfrak{b} = 0\}$

Notation
$b \in A : \mathrm{Ann}(b) = Ann((b)) = (0 : (b)) = \{x \in A | x \cdot b = 0\}$
Note: If $b \neq 0$ and $\mathrm{Ann}(b) \neq 0$ then we have zero divisors.

Remark

1. One verifies easily that $(\mathfrak{a} : \mathfrak{b})$ is in fact an ideal, as well as the annihilator.
2. $D = \bigcup_{0 \neq x \in A} \mathrm{Ann}(x)$ is the set of zero divisors of A.

Definition (radical)
Let $\mathfrak{a} \subseteq A$ be an ideal. The *radical* $\mathfrak{r}(\mathfrak{a})$ of $\mathfrak{a}$ is defined as $\mathfrak{r}(\mathfrak{a}) = \{x \in A | \exists n \in \mathbb{N}_{>0} : x^n \in \mathfrak{a}\}$.

Remark
$\mathfrak{a} = (0) \Rightarrow \mathfrak{r}((0)) = \mathfrak{n}_A$
$x, y \in \mathfrak{r}(\mathfrak{a}) \Rightarrow x + y, a \cdot x \in \mathfrak{r}(\mathfrak{a})$
$(x+y)^{n_x+n_y} = \sum_{j=0}^{n_x+n_y} \binom{n_x+n_y}{j} x^j y^{n_x+n_y-j}$
$\mathfrak{r}(\mathfrak{a})$ is an ideal.

Lemma 1.6. (6) *Let $\mathfrak{a} \subseteq A$ be an ideal and $\pi : A \to A/\mathfrak{a}$ the canonical projection. Then, we have* $\mathfrak{r}(\mathfrak{a}) = \pi^{-1}(\mathfrak{n}_{A/\mathfrak{a}})$

Proof:
The proof is left to the reader.
$\to$ Problem 1.2*c* □

Lemma 1.7. (7) *The radical $\mathfrak{r}(\cdot)$ has the following properties:*

1. $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$
2. $\mathfrak{r}(\mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{r}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{r}(\mathfrak{a}) \cap \mathfrak{r}(\mathfrak{b})$
3. $\mathfrak{r}(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$
4. $\mathfrak{r}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{r}(\mathfrak{r}(\mathfrak{a}) + (b))$
5. $\forall \mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{r}(\mathfrak{p}^n) = \mathfrak{p}$

Proof:
The proof is the solution of the problem 1.3. □

1.2 Modules

In this section A will be a ring (commutative, with 1).

Definition (module)
An *A-module* M is an abelian group $(M, +)$ together with an action $A \times M \to M$ satisfying:

1. $\forall x, y \in M, a \in A : a \cdot (x + y) = a \cdot x + a \cdot y$
2. $\forall x \in M, a, b \in A : (a + b) \cdot x = a \cdot x + b \cdot x$
3. $\forall x \in M, a, b \in A : a \cdot (b \cdot x) = (a \cdot b) \cdot x$
4. $1 \cdot x = x$

Example

1. $A = (A, +, \cdot)$ is an A-module itself
2. $A = \mathbb{Z}$ and G any abelian Group then G can be considered as a $\mathbb{Z}$-module.
3. $A = K$ a field, then the A-module M becomes a K-vector space.

Lecture on 2007-10-25

Definition (module homomorphism)
Let M, N be A-modules. A map $f : M \to N$ is called *A-module homomorphism* (or homomorphism of A-modules) iff

1. $\forall x, y \in M : f(x +_M y) = f(x) +_N f(y)$
2. $\forall \lambda \in A, x \in M : f(\lambda \cdot_M x) = \lambda \cdot_N f(x)$

If f is bijective, wa call it an *A-isomorphism* (short: isomorphism).
We denote by $\mathrm{Hom}_A(M, N)$ the *set of all homomorphisms* of A-modules from M to N.
This set has the structure of on A-module by

1. $\forall f, g \in \mathrm{Hom}_A(M, N) : (f + g)(x) = f(x) + g(x)$
2. $\forall \lambda \in A : (\lambda \cdot f)(x) = \lambda \cdot f(x)$

Example

1. If A=K is a field, homomorphisms of modules are linear maps and $\mathrm{Hom}_K(M, N)$=$\mathcal{L}(M, N)$.
2. If $M = A$, we have a map $\varphi : \mathrm{Hom}(A, N) \to N$ (defined by $f \mapsto f(1)$), which is itself an isomorphism of A-modules.

Definition (submodule)

1. Let be an A-module. A subset $N \subseteq M$ is called *submodule* of M, iff $(N, +)$ is a subgroup of $(M, +)$ and N is closed under scalar multiplication.
2. If $N \subseteq M$ is a submodule, we define the M/N in the following way: We endow the abelian factor grup M/N with the scalar multiplication $\forall \lambda \in A, m \in M : \lambda \cdot (m + N) = (\lambda \cdot m) + N$.

   Claim: M/N is indeed an A-module.

Definition (kernel)
Let f be in $\mathrm{Hom}_A(M, N)$. We define the *kernel* of f as $\ker f = \{m \in M | f(m) = 0\}$ and the *cokernel* of f as the factor module $coker(f) = N/\operatorname{im}(f)$.
Note: $\ker f$ is a submodule of M and $\operatorname{im}(f)$ is a submodule of N.

Theorem 1.1. (Fundamental Theorem of Homomorphism) *Let $f \in \mathrm{Hom}_A(M, N)$.*
Then $\operatorname{im}(f) \cong M/\ker(f)$.
Alternatively: There exists $\overline{f}$ such that $\overline{f}$ is injective and $\overline{f} \circ \pi = f$, where $\pi : M \to M/\ker f$ is the canonical projection.

Proof:
Analogous to the case of groups, vector spaces, rings, ... □

Corollary 1.2. (Isomorphism theorems)

1. *$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$ for A-submodules $M_1, M_2 \subseteq M$.*

2. $(M/M_1)/(M_2/M_1) \cong M/M_2$ *for* A*-submodules* $M_1 \subseteq M_2 \subseteq M$.

Note that finite intersections of submodules are again submodules.
Let $(M_i), i \in I$ *be a family of submodules of* M.
The sum $\sum_{i\in I} M_i = \{\sum_{i\in I} x_i | x_i \in M_i,$ *almost all* $x_i = 0\}$ *is a submodule of* M.

Proof:

1. Consider the map $\varphi : M_2 \to (M_1 + M_2)/M_1$ given by $\varphi(m_2) = m_2 + M_1$, which is a homomorphism and apply the theorem of homomorphisms with $\ker\varphi = M_1 \cap M_2$.
2. The map $\psi : M/M_1 \to M/M_2$ given by $m + M_1 \mapsto m + M_2$ is well defined since $M_1 \subseteq M_2$. We have $\ker\psi = M_2/M_1$. □

Definition

1. Let M be an A-module and $\mathfrak{a} \subseteq A$ an ideal. We define $\mathfrak{a}\cdot M = \{\sum_{k=1}^{r} a_k \cdot x_k | a_k \in \mathfrak{a}, x_k \in M\}$. This is a submodule of M.
2. Let $M_1, M_2 \subseteq M$ submodules. We definie $(M_1 : M_2) = \{a \in A | a \cdot M_2 \subseteq M_1\}$. $(M_1 : M_2)$ is an ideal of A.
3. Especially, the *annihilator* $\mathrm{Ann}(M) = (0 : M)$ is an ideal of A.

Remark
Note that M is an $A/\mathrm{Ann}(M)$-module, more generally:
If $\mathfrak{a} \subseteq \mathrm{Ann}(M)$ is an ideal of A, then $\underbrace{(a+\mathfrak{a})}_{\in A/\mathfrak{a}} + x = a \cdot x$ makes M into an $A/\mathfrak{a}$-module.
We produce a Ring with smaller annihilator in this way, namely $\mathrm{Ann}_{A/Ann_A(M)}(M) = 0_{A/\mathrm{Ann}_A(M)}$.

Definition (faithful)
An A-module M is called *faithful*, if $\mathrm{Ann}(M) = 0$. (M *is a faithful* $A/\mathrm{Ann}(M)$*-module.*)
Note: $\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$

Definition (generated module)
Let M be an A-module.

1. Let $x \in M$. We define $\langle x\rangle = A \cdot x = \{a \cdot x | a \in A\}$.
2. Let $(x_i)_{i\in I}$ be a family of elements of M.
   We define $\langle x_i\rangle_{i\in I} = \sum_{i\in I} A \cdot x_i = \{\sum_{i\in I} a_i \cdot x_i | a_i \in A, a_i = 0$ for almost all $i \in I\}$.
   $\langle x_i\rangle_{i\in I}$ is called the *submodule generated by* $(x_i)_{i\in I}$.
3. If there exists a family $(x_i)_{i\in I}, x_i \in M$ such that $M = \langle x_i\rangle_{i\in I}$ we call M generated by (x_i). If I is finite, M is called *finitely generated*.

Remark
The representation $x = \sum_{k=1}^{n} a_k x_k$ by the generators x_i is usually not unique, even if $\{x_k\}_{i=1}^{r}$ is minimal.
Example: $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module. But we have $0 \cdot 1 = n \cdot 1 \in \mathbb{Z}/n\mathbb{Z}$.

Definition (direct sum, direct product)
Let $(M_i)_{i\in I}$ be a family of A-modules.

1. We define the *direct sum* $\bigoplus_{i\in I} M_i = \{(x_i)_{i\in I} | x_i \in M_i, x_i = 0$ for almost all $i \in I\}$.
2. We define the *direct product* $\Pi_{i\in I} M_i = \{(x_i)_{i\in I} | x_i \in M_i\}$.

Both sets are A-modules, if we define $+$ and $\cdot$ via the components.

Definition (free module)
An A-module M is called *free*, iff $M = \bigoplus_{i \in I} M_i$ and $\forall i \in I : M_i \cong A$.

Remark

1. If $A = K$ is a field, then every finitely generated K-module is a free module of finite rank.
2. $\mathbb{Z}/n\mathbb{Z}$ is not a free $\mathbb{Z}$-module.
3. If $f : V \to W$ is a linear map of K-vector spaces with $rk(f) < \infty$ we have $rk(f) = rk_K \operatorname{im}(f)$.

Proposition 1.1. *An A-module M is finitely generated iff there exists a surjektion $A^n \to M$, $n \in \mathbb{N}$, i.e. M is isomorphic to a factor of the free module A^n.*

Proof:

1. $\Rightarrow$

   M is finitely generated, i.e. $M = \langle x_1, ..., x_n \rangle, x_i \in M$.

   We define $\varphi : A^n \to M$ by $\varphi(a_1, ..., a_n) = \sum_{j=1}^n a_j x_j$. (Check that φ as a homomorphism $M \cong A^n / \ker \varphi$.)

2. $\Leftarrow$

   Let $M \cong A^n/N$ for some $n \in \mathbb{N}$. Then there existes a surjective map $A^n \to M \cong A^n/N$.

   Claim: $\varphi(e_j) = x_j, e_j = (0, ..., 0, 1, 0, ..., 0)$

   Take $x \in M$, φ surjective.

   Then there exists $(a_1, ..., a_n) \in A^n : \varphi(a_1, ..., a_n) = x$.

   $\Rightarrow x = \sum_{j=1}^n a_j \varphi(e_j) = \sum_{j=1}^n a_j x_j$ □

Proposition 1.2. *Let M be a finitely generated A-module and $\mathfrak{a} \subseteq A$ an ideal.*
Let $\varphi \in \operatorname{End}_A(M) = \operatorname{Hom}_A(M, M)$ be an endomorphism *of M such that $\operatorname{im}(\varphi) \subseteq \mathfrak{a} \cdot M$. Then there exists $n \in \mathbb{N}$ and $a_1, ..., a_n \in \mathfrak{a}$ such that $\varphi^n + a_1 \varphi^{n-1} + ... + a_n id = 0$.*

Proof:
Take generators $x_1, ..., x_n$ of M.
Then we have $\operatorname{im}(\varphi) \subseteq \mathfrak{a} \cdot M \Rightarrow \exists a_{k,j} \in \mathfrak{a}$ such that $\forall j = 1, ..., n : \varphi(x_j) = \sum_{k=1}^n a_{k,j} x_k$.
$\Leftrightarrow \sum_{k=1}^n (\delta_{k,j} \varphi - a_{k,j} \cdot id)(x_k) = 0$
We multiply this equation from the left-hand side by the adjoint matrix of $(\delta_{k,j} \varphi - a_{k,j} \cdot id)_{1 \le j,k \le n}$.
$\Rightarrow$ We get $\forall k = 1, ..., n : \det(\delta_{k,j} \varphi - a_{k,j} \cdot id) \in \operatorname{Ann}(\langle x_k \rangle)$.
$\Rightarrow \det(\delta_{k,j} \varphi - a_{k,j} \cdot id) = 0$ in $\operatorname{End}_A(M)$ □

Remark
If $A = K$ is a field, this is the theorem of Cayley-Hamilton.

Corollary 1.3. *Let M be a finetly generated A-module, and $\mathfrak{a} \subseteq A$ an ideal, such that $\mathfrak{a} \cdot M = M$ then there exists $x \equiv 1 \mod \mathfrak{a}$ (i.e. $1 - x \in \mathfrak{a}$) such that $x \cdot M = 0$.*

Proof:
Apply Proposition to $id_n : M \to M$.
$\Rightarrow \exists a_1, ..., a_n \in \mathfrak{a} : (1 + a_1 + ... + a_n) id_n = 0$
$\Rightarrow$ Choose $x = 1 + \underbrace{a_1 + ... + a_n}_{\in \mathfrak{a}}$. □

Proposition 1.3. (Lemma of Nakayama) *Let M be a finitely generated A-module, $\mathfrak{a} \subseteq A$ an ideal, such that $\mathfrak{a}$ is contained in the Jacobson radical R. Then $\mathfrak{a} \cdot M = M$ implies $M = 0$.*

Proof:
From the preceding corollary we know that there exists an $x, 1-x \in \mathfrak{a}, x \cdot M = 0$.
$1-x \in \mathfrak{a} \subseteq R \Rightarrow x$ is a unit by Lemma 4.
$\Rightarrow M = x^{-1}(\underbrace{x \cdot M}_{=0}) = 0$ □

Corollary 1.4. *Let M be a finitely generated A-module, $N \subseteq M$ a submodule, $\mathfrak{a} \subseteq R$ ($\leftarrow$ Jacobson radical).*
Then $M = \mathfrak{a} \cdot M + N \Rightarrow M = N$.

Proof:
For M/N we have $\mathfrak{a} \cdot (M/N) = (\mathfrak{a} \cdot M)/N \cong (\mathfrak{a} \cdot M + N)/N = M/N$. By Nakayama we have $M/N = 0$, i.e. $M = N$. □

Remark
If $\mathfrak{a} = \mathfrak{m}$ is a maximal ideal, we have $\mathfrak{m} \subseteq \mathrm{Ann}(M/(\mathfrak{m}M))$. Then $M/(\mathfrak{m}M)$ is an $A/\mathfrak{m}$-module, i.e. a K-vector space for the field $K = A/\mathfrak{m}$.

Proposition 1.4. *Let M be an A-module, $\mathfrak{m} \in \mathrm{Max}(A)$, $K = A/\mathfrak{m}$ and $x_1, ..., x_n \in M$ forming a K-basis $\{x_1 + \mathfrak{m}M, ..., x_n + \mathfrak{m}M\}$ of $M/\mathfrak{m}M$. Then $x_1, ..., x_n$ are generators of M.*

Proof:
$N = \langle x_1, ..., x_n \rangle$, then $\varphi : N \to M/\mathfrak{m}M$, defined by $N \xrightarrow{\subseteq} M \xrightarrow{\pi} M/\mathfrak{m}M$, is surjective, because the basis is contained in φ (since $\varphi(x_j) = x_j + \mathfrak{m}M$). Hence $\mathfrak{m}M + N = M$, apply corollary.
$\Rightarrow \langle x_1, ..., x_n \rangle = M$ □

Definition (exact sequence)
A sequence $... \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_i} M_{i+1} \to ...$ of A-modules M_j and homomorphisms f_j is called *exact at the place i* iff $\ker(f_{i+1}) = \mathrm{im}(f)_i$.
It is called *exact*, iff it is exact at all places i.

Example

1. $0 \to N' \xrightarrow{f} N$ is exact, iff f is injective.
2. $N \xrightarrow{g} N'' \to 0$ is exact, iff q is surjective.
3. $0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$ is exact iff f is injective, g is surjective and $\mathrm{im}(f) = \ker(g)$, i.e. $N/\mathrm{im}(f) \cong N''$. This is called *short exact sequence*. f is a *monomorphism* and g is an *epimorphism*.

Remark
Every exact sequence $\cdots \to M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} M_{i+2} \to \cdots$ can be written as a composition of short exact sequences $0 \to \ker(f_{i+2}) \to M_{i+1} \to \mathrm{coker}(f_{i+1}) \to 0$.

Proposition 1.5. (7) *The sequence $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact iff for all A-modules N the following sequence is exact: $0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{g^*} \mathrm{Hom}_A(M, N) \xrightarrow{f^*} \mathrm{Hom}_A(M', N)$*
The sequence $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact iff for all A-modules M the following sequence is exact: $0 \to \mathrm{Hom}_A(M, N') \xrightarrow{f_*} \mathrm{Hom}_A(M, N) \xrightarrow{g_*} \mathrm{Hom}_A(M, N'')$
Where the map $f^* : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$ is defined by $\varphi \mapsto \varphi \circ f$ and the homomorphism $f_* : \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N)$ is defined by $\varphi \mapsto f \circ \varphi$.

Proof:
The proof is left to the reader. (Problem Set 2, Problem 3) □

Proposition 1.6. (Snake Lemma (8)) *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & M' & \xrightarrow{u'} & M & \xrightarrow{v'} & M'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of A-modules and A-module homomorphisms with exact rows. Then, there is an exact sequence

$$0 \longrightarrow \ker(f') \xrightarrow{\overline{u}} \ker(f) \xrightarrow{\overline{v}} \ker(f'') \xrightarrow{d} \underbrace{\operatorname{coker}(f')}_{=N'/\operatorname{im}(f')} \xrightarrow{\overline{u}'} \underbrace{\operatorname{coker}(f)}_{=N/\operatorname{im}(f)} \xrightarrow{\overline{v}'} \underbrace{\operatorname{coker}(f'')}_{=N''/\operatorname{im}(f'')} \longrightarrow 0$$

where $\overline{u}, \overline{v}, \overline{u}'$ and $\overline{v}'$ are A-module homomorphisms which will explained in course of the proof.

Proof:

1. Definition of $\overline{u}$.

   We need to define $\overline{u} : \ker(f') \to \ker(f)$. We put $\overline{u}(m') = u(m')$.

   Question/Claim: $u(m') \in \ker(f)$?

   $\Rightarrow f(u(m')) = f(\circ u)(m') = (u' \circ f')(m') = u'(f'(m')) = u'(0) = 0$

   $\Rightarrow u(m') \in \ker(f)$

2. Definition of $\overline{v}$.

   We want to define $\overline{v} : \ker(f) \to \ker(f'')$ by $\overline{v} = v|_{\ker(f)}$. Again, we have to show, that $\overline{v}(m) \in \ker(f'')$.

   $\Rightarrow f(\overline{v}(m)) = f''(v(m)) = (f'' \circ v)(m) = (v' \circ f)(m) = v'(f(m)) = v'(0) = 0$

3. Definition of d (connecting homomorphism).

   Need to define: $d : \ker(f'') \to \operatorname{coker}(f') = N'/\operatorname{im}(f)$.

   $$M \xrightarrow{v} M''$$

   $$\begin{array}{ccccc} & & \exists m : m & \xmapsto{v} & m'' \in M'' \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ \exists n' : n' & \longmapsto & f(m) & \xmapsto{v'} & 0 \end{array}$$

   Where $f(m) \in \ker(v') = \operatorname{im}(u')$.

   We define $d(m'') = n' + \operatorname{im}(f') \in \operatorname{coker}(f')$. Is this well defined?

   Using the diagram

   $$\begin{array}{ccccc} m' & \xmapsto{u} & m - \tilde{m} & \xmapsto{v} & 0 \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ f'(m') & \xmapsto{u'} & f(m - \tilde{m}) = f(m) - f(\tilde{m}) & \xmapsto{v'} & 0 \end{array}$$

   with $m - \tilde{m} \in \operatorname{im}(u) = \ker(v)$, we see, that d is well defined.

4. Definition of $\overline{u}'$.

   Need to define $\overline{u}' : \operatorname{coker}(f') \to \operatorname{coker}(f)$.

   Consider the diagram:

$$\begin{array}{ccc} N' & \xrightarrow{u'} & N \\ \downarrow & & \downarrow \\ \operatorname{coker}(f') = N'/\operatorname{im}(f') & \xrightarrow{\overline{u}'} & N/\operatorname{im}(f) = \operatorname{coker}(f) \end{array}$$

The induced map $\overline{u}'$ is well-definied, if $u'(\operatorname{im}(f')) \subseteq \operatorname{im}(f)$.

$n \in \operatorname{im}(f') \Rightarrow n = f'(n')$ with $n' \in M'$.

$\Rightarrow u'(n) = u'(f'(n')) = (u' \circ f')(n') = (f \circ u)(n') = f(u(n')) \in \operatorname{im}(f)$

5. Definition of $\overline{v}'$.

   We need to define $\overline{v}' : \operatorname{coker}(f) \to \operatorname{coker}(f'')$.

$$\begin{array}{ccc} N & \xrightarrow{v'} & N'' \\ \downarrow & & \downarrow \\ \operatorname{coker}(f) = N/\operatorname{im}(f) & \xrightarrow{\overline{v}'} & N''/\operatorname{im}(f'') = \operatorname{coker}(f'') \end{array}$$

   We juse the same argument as before to show well-definedness.

6. Exactness at $\ker(f')$.

   One has to show that $\overline{u}$ is injective. This is clear, since $\overline{u} = u|_{\ker(f')}$, and u is injective.

7. Exactness at $\ker(f)$.

   Claim: $\operatorname{im}(\overline{u}) = \ker(\overline{v})$.

   (a) $\operatorname{im}(\overline{u}) \subseteq \ker(\overline{v})$
   Let $m \in \operatorname{im}(\overline{u})$.
   $\Rightarrow m = u(m'), (m' \in \ker(f'))$
   $\Rightarrow \overline{v}(m) = v(u(m')) = (v \circ u(m')) = 0$, by exactness.

   (b) $\ker(\overline{v}) \subseteq \operatorname{im}(\overline{u})$
   Let $m \in \ker(\overline{v}) \Rightarrow v(m) = 0$.
   $\Rightarrow m \in \ker(v) = \operatorname{im}(u) \Rightarrow m = u(m')$
   Check: $m' \in \ker(f')$
   $\Rightarrow 0 = f(m) = f(u(m')) = (f \circ u)(m') = (u' \circ f')(m') = u'(f'(m'))$
   $\Rightarrow f'(m') = 0$, since u' is injective.
   $\Rightarrow m' \in \ker(f')$

8. Exactness at $\ker(f'')$.

   Show: $\operatorname{im}(\overline{v}) = \ker(d)$

   (a) $\operatorname{im}(\overline{v}) \subseteq \ker(d)$
   $m'' \in \operatorname{im}(\overline{m})$
   $\Rightarrow \exists m \in \ker(f) : m'' = \overline{v}(m) = v(m)$

$$\begin{array}{ccccc} & & m & \xmapsto{\overline{v}} & m'' \\ & & \downarrow & & \downarrow \\ \exists n' : n' & \xmapsto{u'} & f(m) = 0 & \xmapsto{v'} & 0 \end{array}$$

   Since u' is injective, we have $n' = 0$.
   $\Rightarrow d(m'') = 0 \in \operatorname{coker}(f') \Rightarrow m'' \in \ker(d)$

(b) $\ker(d) \subseteq \mathrm{im}(\overline{v})$
Let be $m'' \in \ker(d)$ $(\subseteq \ker(f'') \subseteq M'')$.

$$\begin{array}{ccccc} \exists m' & & m & \overset{v}{\longmapsto} & m'' \\ \Big\downarrow{\scriptstyle f'} & & \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle f''} \\ \exists n' : n' & \overset{u'}{\longmapsto} & f(m) & \overset{v'}{\longmapsto} & 0 \end{array}$$

Now, we apply u to m' and get $u(m')$.
Then, we apply f to $m - u(m')$ and get $f(m) - f(m) = 0$:

$$\begin{array}{ccc} \ker(f) \ni m - u(m') & \overset{v}{\longmapsto} & v(m) - 0 = m'' \\ \Big\downarrow{\scriptstyle f} & & \\ 0 = f(m) - f(m) & & \end{array}$$

$\Rightarrow m'' \in \mathrm{im}(\overline{v})$

9. $\mathrm{im}(d) = \ker(\overline{u}')$
   (a) $\mathrm{im}(d) \subseteq \ker(\overline{u}')$
   Let $n' + \mathrm{im}(f') \in \mathrm{im}(d)$.
   $\overline{u}'(n' + \mathrm{im}(f')) = u'(n') + \mathrm{im}(f)$
   We want to show: $n' + \mathrm{im}(f') \in \ker(\overline{u}')$, i.e. $u'(n') \in \mathrm{im}(f)$.
   We have $u'(n') = f(m)$...
   (b) $\ker(\overline{u}') \subseteq \mathrm{im}(d)$
   $\underbrace{\overline{u}'(n' + \mathrm{im}(f'))}_{=u'(n')+\mathrm{im}(f)} = \mathrm{im}(f) = 0 \in \mathrm{coker}(f)$
   $\Rightarrow u'(n') \in \mathrm{im}(f)$
   $\Rightarrow \exists m \in M : u'(n') = f(m)$
10. The rest is left to the reader.

□

1.3 Homology & cohomologie

Fix A, a commutative ring with 1.

Definition (category)
A *category* $\mathcal{C}$ consists of objects X, Y, ... and morphisms $\mathrm{Mor}(X, Y)$ for every pair of objects X, Y. Corresponding morphisms can be composed in an associative way. For every object X we have the identity morphism $id_X \in \mathrm{Mor}(X, X)$ given by $\forall x \in X : id_X(x) = x$.
Notation: $Ob(\mathcal{C})$ denotes the objects of the category $\mathcal{C}$ $(X \in Ob(\mathcal{C}))$.

Example

1. The categorie $\mathcal{C} = \mathfrak{M}_A$ is given as follows:
   (a) $Ob(\mathfrak{M}_A) = \{X | X \text{ is an } A\text{-module}\}$
   (b) $\forall X, Y \in Ob(\mathfrak{M}_A) : \mathrm{Mor}(X, Y) = \mathrm{Hom}_A(X, Y)$

   $\mathfrak{M}_A$ is the categorie of A-modules.
2. $\mathcal{C} = \mathcal{T}$ = category of topological spaces:
   (a) $Ob(\mathcal{T}) = \{X | X \text{ is a topological space}\}$
   (b) $\forall X, Y \in Ob(\mathcal{T}) : \mathrm{Mor}(X, Y) = \mathrm{Cont}(X, Y)$ which is the set of continous maps from X to Y.

Definition (covariant functor)
Let $\mathcal{C}$ and $\mathcal{D}$ be two categories.
A map $F : \mathcal{C} \to \mathcal{D}$ is called a *covariant functor*, iff F associates to every $X \in Ob(\mathcal{C})$ an object $F(X) \in Ob(\mathcal{D})$ and to every $f \in \mathrm{Mor}(X, Y)$ a morphism $F(f) \in \mathrm{Mor}(F(X), F(Y))$ such that $\forall f, g \in \mathrm{Mor}(X, Y) : F(f \circ g) = F(f) \circ F(g)$ and $\forall X \in Ob(\mathcal{C}) : F(id_X) = id_{F(X)}$.

Remark
The above functor is called *contravariant*, iff $\forall f, g \in \mathrm{Mor}(X, Y) : F(f \circ g) = F(g) \circ F(f)$. Note that $\mathrm{Mor}(X, Y) \ni f \mapsto F(f) \in \mathrm{Mor}(F(Y), F(X))$.

Example
Consider $\mathcal{C} = \mathcal{D} = \mathfrak{M}_A$.

1. Fix $M \in Ob(\mathfrak{M}_A)$ and consider the functor $\mathrm{Hom}_A(M, \cdot)$.
   $N \in Ob(\mathfrak{M}_A) : N \mapsto \mathrm{Hom}_A(M, N) \in Ob(\mathfrak{M}_A)$
   $\Rightarrow \mathrm{Hom}(M, \cdot)$ is a covariant functor from $\mathfrak{M}_A$ to itself.
2. Fix $N \in Ob(\mathfrak{M}_A)$ and consider the functor $\mathrm{Hom}_A(\cdot, N)$.
   For $M \in Ob(\mathfrak{M}_A)$ we have $M \mapsto \mathrm{Hom}_A(M, N) \in Ob(\mathfrak{M}_A)$.
   $\Rightarrow \mathrm{Hom}(\cdot, N)$ is a contravariant functor from $\mathfrak{M}_A$ to itself.

Definition (chain complex)
A *chain complex* $\mathbf{C} : ... \to C_{n+1} \overset{\delta_{n+1}}{\to} C_n \overset{\delta_n}{\to} C_{n-1} \to ...$ consists of A modules $\{C_n\}_{n\in\mathbb{Z}}$ and A module homomorphisms $\{\delta_n\}_{n\in\mathbb{Z}}$ satisfying $\delta_n \circ \delta_{n+1} = 0$, i.e. $\mathrm{im}(\delta_{n+1}) \subseteq \ker(\delta_n)$ for all $n \in \mathbb{Z}$. Let $\mathbf{C}$ and $\mathbf{D}$ be chain complexes. A morphism $\varphi : \mathbf{C} \to \mathbf{D}$ is given by A-module homomorphisms $\varphi_n : C_n \to D_n$, $n \in \mathbb{Z}$, such that the following diagram commutes:

$$\begin{array}{ccc} C_n & \xrightarrow{\varphi_n} & D_n \\ {\scriptstyle\delta_n}\downarrow & & \downarrow{\scriptstyle\delta_n} \\ C_{n-1} & \xrightarrow{\varphi_{n-1}} & D_{n-1} \end{array}$$

From this, we get the following cummutative diagram:

$$\begin{array}{lccccccccc} \mathbf{C}: & \cdots & \xrightarrow{\delta_{n+2}} & C_{n+1} & \xrightarrow{\delta_{n+1}} & C_n & \xrightarrow{\delta_n} & C_{n-1} & \xrightarrow{\delta_{n-1}} & \cdots \\ {\scriptstyle\varphi}\downarrow & & & \downarrow{\scriptstyle\varphi_{n+1}} & & \downarrow{\scriptstyle\varphi_n} & & \downarrow{\scriptstyle\varphi_{n-1}} & & \\ \mathbf{D}: & \cdots & \xrightarrow{\delta_{n+2}} & D_{n+1} & \xrightarrow{\delta_{n+1}} & D_n & \xrightarrow{\delta_n} & D_{n-1} & \xrightarrow{\delta_{n-1}} & \cdots \\ {\scriptstyle\psi}\downarrow & & & \downarrow{\scriptstyle\psi_{n+1}} & & \downarrow{\scriptstyle\psi_n} & & \downarrow{\scriptstyle\psi_{n-1}} & & \\ \mathbf{E}: & \cdots & \xrightarrow{\delta_{n+2}} & E_{n+1} & \xrightarrow{\delta_{n+1}} & E_n & \xrightarrow{\delta_n} & E_{n-1} & \xrightarrow{\delta_{n-1}} & \cdots \end{array}$$

Definition (cycles, boundaries, homology)
Let $\mathbf{C}$ be a chain complex.

1. $Z_n(\mathbf{C}) = \ker(\delta_n) \subseteq C_n$ is called the A-module of *n-cycles* of $\mathbf{C}$.
2. $B_n(\mathbf{C}) = \mathrm{im}(\delta_{n+1}) \subseteq C_n$ is called the A-module of *n-boundaries* of $\mathbf{C}$.
3. (recall: $B_n(\mathbf{C}) \subseteq Z_n(\mathbf{C})$)
   The quotient module $H_n(\mathbf{C}) = Z_n(\mathbf{C})/B_n(\mathbf{C})$ is called the n-th *homology* of $\mathbf{C}$ ($n \in \mathbb{Z}$).

Remark
Let $\varphi : \mathbf{C} \to \mathbf{D}$ be a morphism of chain complexes:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\delta_{n+1}} & C_n & \xrightarrow{\delta_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \varphi_{n+1}} & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & \\
\cdots & \longrightarrow & D_{n+1} & \xrightarrow{\delta_{n+1}} & D_n & \xrightarrow{\delta_n} & D_{n-1} & \longrightarrow & \cdots
\end{array}$$

Claim: We want to have a morphism φ_{n*} from $H_n = Z_n(\mathbf{C})/B_n(\mathbf{C})$ to $Z_n(\mathbf{D})/B_n(\mathbf{D}) = H_n(\mathbf{D})$.
In short: Building homology gives rise to covariant functor from the category of chain complexes (over A) to the category of graded A-modules.

Long exact sequences in homology
Consider chain complexes $\mathbf{C}, \mathbf{D}, \mathbf{E}$ and the short exact sequence $0 \to \mathbf{C} \xrightarrow{\varphi} \mathbf{D} \xrightarrow{\psi} \mathbf{E} \to 0$, i.e.

$$0 \longrightarrow \mathbf{C} \xrightarrow{\varphi} \mathbf{D} \xrightarrow{\psi} \mathbf{E} \longrightarrow 0$$

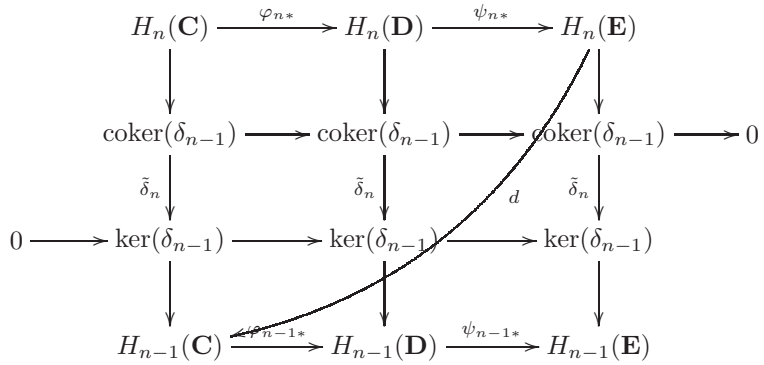
$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_{n+1} & \xrightarrow{\varphi_{n+1}} & D_{n+1} & \xrightarrow{\psi_{n+1}} & E_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta_{n+1}} & & \downarrow{\scriptstyle \delta_{n+1}} & & \downarrow{\scriptstyle \delta_{n+1}} & & \\
0 & \longrightarrow & C_n & \xrightarrow{\varphi_n} & D_n & \xrightarrow{\psi_n} & E_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Then, there is a long exact sequence in homology:
$\ldots \to H_n(\mathbf{C}) \xrightarrow{\varphi_{n*}} H_n(\mathbf{D}) \xrightarrow{\psi_{n*}} H_n(\mathbf{E}) \xrightarrow{d_n} H_{n-1}(\mathbf{C}) \xrightarrow{\varphi_{n-1*}} H_{n-1}(\mathbf{D}) \xrightarrow{\psi_{n-1*}} H_{n-1}(\mathbf{E}) \to \ldots$
Proof:
Consider the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker(\delta_n) & \longrightarrow & \ker(\delta_n) & \longrightarrow & \ker(\delta_n) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_n & \xrightarrow{\varphi_n} & D_n & \xrightarrow{\psi_n} & E_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta_n} & & \downarrow{\scriptstyle \delta_n} & & \downarrow{\scriptstyle \delta_n} & & \\
0 & \longrightarrow & C_{n-1} & \xrightarrow{\varphi_{n-1}} & D_{n-1} & \xrightarrow{\psi_{n-1}} & E_{n-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{coker}(\delta_n) & \longrightarrow & \operatorname{coker}(\delta_n) & \longrightarrow & \operatorname{coker}(\delta_n) & &
\end{array}$$

Note: $\operatorname{im}(\delta_{n+1}) \subseteq \ker(\delta_n)$, which gives
$C_n/\operatorname{im}(\delta_{n+1}) \to C_n/\ker(\delta_n) \cong \operatorname{im}(\delta_n) \subseteq \ker(\delta_{n-1})$
$\Rightarrow \operatorname{coker}(\delta_{n+1}) \xrightarrow{\tilde{\delta}_n} \ker(\delta_{n-1})$
Note further:
$\ker(\tilde{\delta}_n) = \ker(\delta_n)/\operatorname{im}(\delta_{n+1}) = H_n(\mathbf{C})$
$\operatorname{coker}(\tilde{\delta}_n) = \ker(\delta_{n-1})/\operatorname{im}(\tilde{\delta}_n) = \ker(\delta_{n-1})/\operatorname{im}(\delta_n) = H_{n-1}(\mathbf{C})$

Now, we can use the Snake Lemma in the following commutative diagram:



Note, that we have:
$\ker(\delta_n) = H_n(\mathbf{C}) = H_n(\mathbf{D}) = H_n(\mathbf{E})$ and $\ker(\tilde{\delta}_n) = H_n(\mathbf{C}_{n-1}) = H_n(\mathbf{D}_{n-1}) = H_n(\mathbf{E}_{n-1})$

Lecture on 2007-11-08

Definition (cochain complex)

A *cochain complex* $\mathbf{C}$ is given by a sequence $\mathbf{C} : \cdots \to C_{n-1} \overset{\delta_{n-1}}{\to} C_n \overset{\delta_n}{\to} C_{n+1} \to \cdots$ which has the following properties:

1. C_n $(n \in \mathbb{Z})$ are A-modules
2. δ_n $(n \in \mathbb{Z})$ are A-module homomorphisms such that $\delta_n \circ \delta_{n-1} = 0$

Definition (cohomology)
The n-th *cohomology* of $\mathbf{C}$ is given by

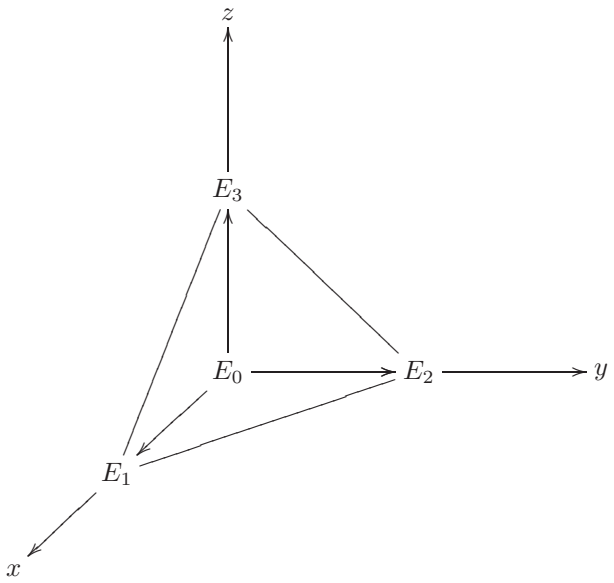
1. $H^n(\mathbf{C}) = \ker(\delta_n)/\operatorname{im}(\delta_{n-1}), n \in \mathbb{Z}$
2. $Z^n(\mathbf{C}) = \ker(\delta_n)$ are the *n-cocycles* of $\mathbf{C}$
3. $B^n(\mathbf{C}) = \operatorname{im}(\delta_{n-1})$ are the *n-coboundaries* of $\mathbf{C}$

Remark
Define the morphism $\varphi : \mathbf{C} \to \mathbf{D}$ of cochain complexes analogous to morphisms of chain complexes. $\rightsquigarrow$ Category of cochain complexes. A morphism $\varphi : \mathbf{C} \to \mathbf{D}$ of cochain complexes induces (as before) a morphism $\varphi_n^* : H^n(\mathbf{C}) \to H^n(\mathbf{D})$. We get a covariant functor from the category of cochain complexes to the category of graded A-modules.
There exists a long exact sequence in cohomology.

Example

1. Topology (singular homology)

   Let $\Delta_n \subseteq \mathbb{R}^N, n = 0, ..., N$ be the standard simplex, i.e. $\Delta_n = \langle E_0, E_1, ..., E_n \rangle$ where $E_0, ..., E_N$ is the affine standard basis in $\mathbb{A}^N(\mathbb{R}) \cong \mathbb{R}^N$ and $\langle ... \rangle$ denotes the convex hull:



Aim: Construct a functor from the category of topological spaces to the category of (graded) $\mathbb{Z}$-modules:

Let X be topoogical space:

We define $\tilde{\Delta}_n = \{\sigma_n | \Delta_n \to X | \sigma_n \text{ is continous } \}$ is called a simplex.

Additionally we define $C_n(X) =< \sigma_n | \sigma_n \in \tilde{\Delta}_n >$ the free abelian group generated by the simplices, i.e. $C_n(X) \ni c_n = \sum_\nu \lambda_\nu c_n^{(\nu)}$ (finite and $\lambda_n \in \mathbb{Z}$).

c_n is called singular chain.

Note: $C_n(X)$ is a $\mathbb{Z}$ module ($C_n(X) = 0$, if $n < 0$).

Boundary map: $\delta_n C_n(X) \to C_{n-1}(X)$, defined by $\sigma_n \mapsto \delta_n(\sigma_n)$.

$\delta_n(\sigma_n) := \sum_{i=0}^{n} (-1)^i \tilde{\delta}_i(\sigma_n)$ with $\tilde{\delta}_i(\delta_n) := \sigma_n|_{\langle E_0,\dots,\hat{E}_i,\dots,E_n\rangle} \in \tilde{\Delta}_{n-1}$ where $\langle E_0, ..., \hat{E}_i, ..., E_n\rangle$ is a standard simplex of dimension $n-1$.

We get a $\mathbb{Z}$-linear map $\delta_n : C_n(X) \to C_{n-1}(X)$.

Exercise: Show that $\delta_{n-1} \circ \delta_n = 0$.

$\Rightarrow \mathbf{C}(X) : \cdots \to C_n(X) \overset{\delta_n}{\to} C_{n-1}(X) \overset{\delta_{n-1}}{\to} \cdots \to C_0(X) \to 0 \to 0 \to \cdots$ is a chain complex of $\mathbb{Z}$-modules.

$\Rightarrow H_n(X, \mathbb{Z}) = H_n(\mathbf{C}(X))$ is the n-th singular homology of X with coefficients in $\mathbb{Z}$.

The aim of topology is to classify topological spaces up to homeomorphisms, i.e. bijective bicontinous maps. ($X \approx Y \Leftrightarrow \exists f : X \to Y$ cont., bij. and $Y \to X$ continous.)

Now, lets consider the N-dimensional sphere $S^N = \{x \in \mathbb{R}^{N+1} \big| \|x\| = 1\}$.

Wie get $H_n(S^N, \mathbb{Z}) \cong \begin{cases} \mathbb{Z} & , n = 0, N \\ 0 & , \text{otherwise} \end{cases}$.

If $N = 2$, we get $X \cong S^2 \Leftrightarrow H_n(X, \mathbb{Z}) \cong H_n(S^2, \mathbb{Z})$.

If $N = 3$, we have $X \cong S^3 \Leftrightarrow H_n(X, \mathbb{Z}) \cong H_n(S^3, \mathbb{Z})$
$\Rightarrow \surd$
$\Leftarrow$ Poincaré-Coryechre - proven by Perelman

2. Differential forms

$\rightarrow$ de Rham cohomology (of manifolds)

Consider $X = \mathbb{R}^n$ (this is a (real) manifold). (Manifolds are structures, which look localy like $\mathbb{R}^n$.)

Let $C^0(\mathbb{R}^n) = \mathcal{C}^\infty(\mathbb{R}^n, \mathbb{R})$ the infinitely diff. real functions on $\mathbb{R}^n$.

Def:

A differential form ω on $\mathbb{R}^n$ of degree r is given by

$$\omega = \sum_{\{i_1,...i_r\}\subseteq\{1,...,n\}} f_{i_1,...,i_r}(x_1, ..., x_n)dx_{i_1}...dx_{i_r}$$

where $f_{i_1,...,i_r} \in C^0(\mathbb{R}^n)$.

The differentials $dx_1, ..., dx_n$ are subject to the relation $dx_i dx_j = -dx_j dx_i$ $(j, k = 1, ..., n)$. Hence, we get $dx_j dx_j = 0$ ($\Rightarrow$ if $r > n$ we get $\omega = 0$).

$\Rightarrow \omega = \sum_{1\leq i_1\leq ...\leq i_r\leq n} g_{i_1,...,i_r}(x_1, ..., x_n)dx_{i_1}...dx_{i_r}$.

$C^r(\mathbb{R}^n) = \{\omega | \omega \text{ is diff. form of degree } r\}$.

$\Rightarrow C^r(\mathbb{R}^n) = 0$, if $r > 0$. We put $C^r(\mathbb{R}^n) = 0$, if $r < 0$.

We want to get a cochain complex

$\cdots \xrightarrow{d} 0 \xrightarrow{d} 0 \xrightarrow{d} C^0(\mathbb{R}^n) \xrightarrow{d} C^1(\mathbb{R}^n) \xrightarrow{d} \cdots \xrightarrow{d} C^n(\mathbb{R}^n) \xrightarrow{d} 0 \xrightarrow{d} 0 \xrightarrow{d} \cdots$

where d is defined by $f \mapsto \sum_{i=1}^n \frac{\partial f dx_i}{\partial x_i}$

One has to check, that $d \circ d = 0$.

Generally one has $d\omega = \sum_{1\leq i_1\leq ...\leq i_r\leq n} \sum_{j=1}^n \frac{\partial g_{i_1,...,i_r} dx_j dx_{i_1}...dx_{i_r}}{\partial x_j}$

One can replace $\mathbb{R}^n$ by an n-dimensional manifold X. You get $H^r_{dR}(X, \mathbb{R})$, which is the r-th *de Rhan cohomology* of X.

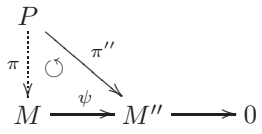
We have the Poincaré-duality: $H^r_{dR}(X) \cong H_r(X, \mathbb{R})$.

1.4 The functor Ext

Let $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$ be an exact sequence of A-modules.
Then, we get $0 \rightarrow \mathrm{Hom}(M, N') \rightarrow \mathrm{Hom}(M, N) \rightarrow \mathrm{Hom}(M, N'') \rightarrow ?$.
But ... what does the question mark stand for?

As usual we will denote by A a commutative ring with 1.

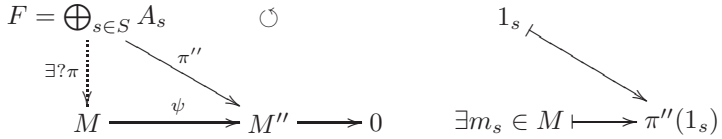
Definition (projective A-modules)



An A-module P is called *projective*, iff for every surjective A-module homomorphism $\psi : M \rightarrow M''$ and every A-module homomorphism $\pi'' : P \rightarrow M''$, there exists an A module homomorphism $\pi : P \rightarrow M$ such that $\psi \circ \pi = \pi''$.

Example

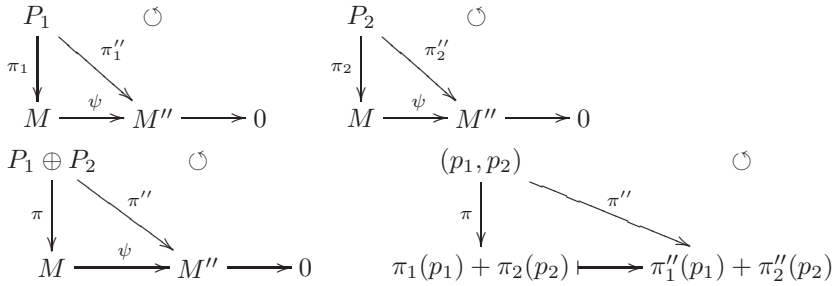
Free A-modules are projective (i.e. $M \cong \bigoplus_{s\in S} A_s$, with $A_s \cong A$).



Define $\pi(1_s) = m_s \in M$, extend linearly, denote the map by π again and ... this does the job.

Lemma 1.8. (1) *A direct sum $\sum_{i\in I} P_i$ of A-modules P_i $(i \in I)$ is projective iff each P_i is projective.*

Proof:



□

Definition (splitting sequences)

A short exact sequence $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ of A modules *splits*, iff there existes an A-module homomorphism $\sigma : M'' \to M$ such that $\psi \circ \sigma = \mathrm{id}_{M''}$.

Lemma 1.9. (2) *A short exact sequence $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ of A modules splits, iff we have an A-module isomorphism $M \cong M' \oplus M''$. We call this a* trivial extension *of M'' by M'.*

Proof:

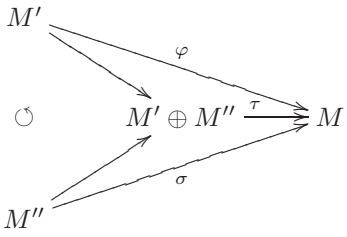
1. $\Leftarrow$

   Considering the sequence $0 \to M' \to M' \oplus M'' \to M'' \to 0$ with $m' \mapsto (m', 0)$ and $(m', m'') \mapsto m''$ we get $\sigma : M'' \to M' \oplus M''$ by $m'' \mapsto (0, m'')$.

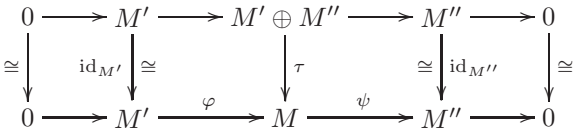
2. $\Rightarrow$

   This is a consequence of the 5-Lemma:

   We have (by the properties of direct sums):

   We rewrite this as follows

   $\Rightarrow \tau$ is an isomorphism. (This is called the 5-Lemma due to the 5 columns in the diagram. We have proven this in the exercise.) □

Lemma 1.10. (3) *Let $0 \to N' \xrightarrow{\varphi} N \xrightarrow{\psi} N'' \to 0$ be a short exact sequence and P a projective A-module.*
Then, the short sequence $0 \to \mathrm{Hom}_A(P, N') \to \mathrm{Hom}_A(P, N) \to \mathrm{Hom}_A(P, N'') \to 0$ is also exact.

Proof:
The proof is left for the exercise. □

Lemma 1.11. (4) *Let M be an A-module. Then, there exists a projective A-module P together with a surjective A-module homomorphism $P \to M \to 0$.*
Note: *One can take P even to be free.*

Proof:
$P := \bigoplus_{m \in M} A_m, A_m \cong A$
Consider the map $A_m \ni 1_m \mapsto m \in M$, extend linearly and you will get an A-module homomorphism $P = \bigoplus_{m \in M} A_m \to M$, which is obviously surjective. □

Definition (projective resolution)
Let M be an A-module. *A* chain complex $\mathbf{P} : \cdots \to P_n \to P_{n-1} \to \cdots \to P_0 \to 0$ is called *projective resolution* of M, if the following three properties hold:

1. The P_n are projective A-modules for $n \in \mathbb{N}$.
2. $H_n(\mathbf{P}) = 0$ for $n \in \mathbb{N}, n > 0$, i.e. the sequence of the chain complex is exact, except at P_0. One calls such a chain complex acyclic.
3. $H_0(\mathbf{P}) \cong M$

Remark
$\cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} H_0(\mathbf{P}) = \ker(\delta_0)/\operatorname{im}(\delta_1) = P_0/\operatorname{im}(\delta_1) \to 0$ is exact everywhere.
$\Rightarrow \cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0$ is also exact everywhere.

Lemma 1.12. (5) *Let M be an A-module. Then, M has a projective resolution.*

Proof:
By Lemma 4, there exist A-modules R_1, P_0 with P_0 projective such that we have a short exact sequence $0 \to R_1 \to P_0 \to M \to 0$.
Again applying Lemma 4 (namely for R_1), we get an exact sequence $0 \to R_2 \to P_1 \to R_1 \to 0$ with P_1 being projective.
Taken together this yields the sequence $P_1 \to P_0 \to M \to 0$. The exactness at P_0 is given by the construction.
Inductively, one constructs the claimed projective resolution
$\cdots \to P_n \to \cdots \to P_1 \to P_1 \to M \to 0$ □

Derived functors
Let $T : \mathfrak{M}_A \to \mathfrak{M}_A$ ($\mathfrak{M}_A$ = category of A-modules) be a covariant functor. Let be $M \in Ob(\mathfrak{M}_A)$ with projective resolution $\mathbf{P} : \cdots \xrightarrow{\delta_{n+1}} P_n \xrightarrow{\delta_n} \cdots \to P_1 \to P_0 \to M \to 0$.
Apply T to $\mathbf{P}$. In particular $\delta_n \circ \delta_{n+1} = 0 \Rightarrow T(\delta_n) \circ T(\delta_{n+1}) = T(0) = 0$.
$T\mathbf{P} : \cdots \to T(P_n) \to T(P_{n-1}) \to \cdots \to T(P_1) \to T(P_0) \to 0$ is a chain complex, but it does not have to be exact or projective.
Now, we can take homology of this chain complex.

Definition (left derived functor)
Using the above notations, the *left derived functor* $LT(M)$ of T is given by $L_nT(M) = H_n(T\mathbf{P}), n \in \mathbb{N}$.

Remark
$\mathfrak{M}_A \to$ graded $\mathfrak{M}_A$, defined by $M \mapsto (L_nT(M))_{n \in \mathbb{N}}$ is the derived functor.

Proposition 1.7. *The definition of the left derived functor $LT(M)$ is independend of the chosen projective resolution of M.*

Proof:
See Hilton-Stammbach: Homological algebra, p. 129. □

Definition (Ext)
For $\mathrm{Hom}_A(\cdot, N), N \in Ob(\mathfrak{M}_A)$ we define $\mathrm{Ext}^n_A(M,N) := R^n\mathrm{Hom}_A(M,N)$, where R denotes the *right derived functor* (created by $H^n(T\mathbf{P})$), defined by the cochain complex $\mathrm{Hom}_A(M,N)$.

Lecture on 2007-11-15

Lemma 1.13. (Characterisation of projective modules) *P is a projective module $\Leftrightarrow \exists P'$ such that $P \oplus P'$ is free.*

Proof:
No Proof. □

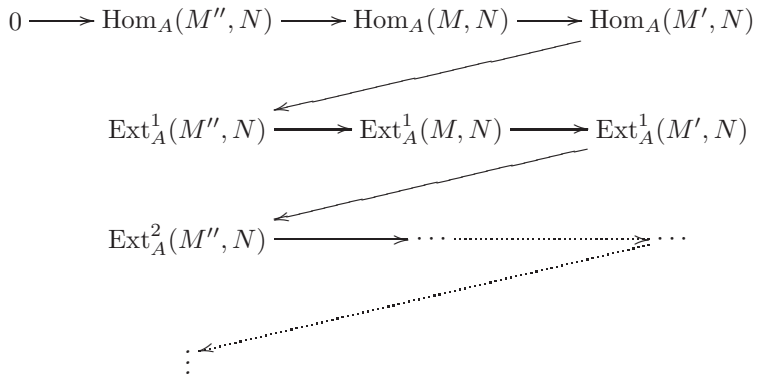
Example
$\mathrm{Ext}^n_A(M,N) = R^n\mathrm{Hom}_A(M,N)$ where R denotes the right derived functor of the contravariant functor $\mathrm{Hom}_A(\cdot, N)$.

Lemma 1.14. (6) *If M is projective, then $\mathrm{Ext}^n_A(M,N) = 0$ for all $n > 0$.*
(Additionally, $\mathrm{Ext}^0_A(M,N) = \mathrm{Hom}_A(M,N)$.)

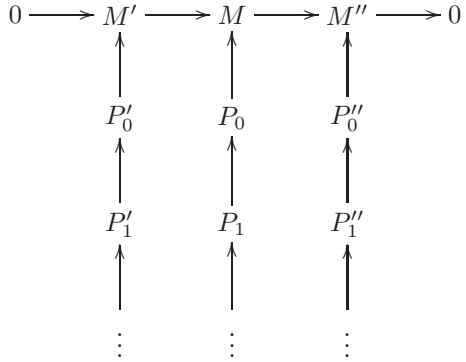
Proof:
M has the resolution $0 \to P_0 = M \xrightarrow{\mathrm{id}} M \to 0$.
Applying $\mathrm{Hom}_A(\cdot, N)$ to $0 \to M \to 0$ and computing the cohomology of $0 \to \mathrm{Hom}_A(M,N) \to 0$ we get the desired result. □

Example
Considering $\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$, we get the resolution $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$.
Applying $\mathrm{Hom}_{\mathbb{Z}}(\cdot, \mathbb{Z})$ to $0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to 0$ leads to $0 \leftarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \cong \mathbb{Z} \xleftarrow{\cdot n} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \leftarrow 0$.
$\Rightarrow \mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) = 0 = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}), \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}, \mathrm{Ext}^j_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) = 0, j \geq 2$

Theorem 1.2. (7) *For an exact sequence $0 \to M' \to M \to M'' \to 0$ there is a long exact sequence*



Proof:
This is a corollary from the long cohomology sequence, applied to



□

Remark
We could also consider a left derived functor of $\mathrm{Hom}_A(M, \cdot)$. It coincides again with Ext, i.e. for $0 \to N' \to N \to N'' \to 0$ there is a long exact sequence
$0 \to \mathrm{Hom}_A(M, N') \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'') \to \mathrm{Ext}^1_A(M, N')$

Aim
Aim: Give an interpretation of $\mathrm{Ext}^1_A(M, N)$ as extension.

Definition
For A-modules M, N we call a short exact sequence $0 \to N \to Q \to M \to 0$ an *extension* of M by N.
We know that Q is not uniquely determined by M and N:

1. $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$
2. $0 \to \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z} \to 0$

where we have $\mathbb{Z}/4\mathbb{Z} \ncong (\mathbb{Z}/2\mathbb{Z})^2$.

Definition
Two extensions Q and Q' are called *equivalent*, iff there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & Q & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\ 0 & \longrightarrow & N & \longrightarrow & Q' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

We denote the set of equivalence classes as $E_A(M, N)$.

Lemma 1.15. *If Q and Q' are equivalent, then $Q \cong Q'$.*

Proof:
This follows immediately from the 5-Lemma. ($\rightsquigarrow$ Problem 3.1c) □

Remark
We have $E_A(M, N) \neq \emptyset$, because there exists the sequence $0 \to N \to N \oplus M \to M \to 0$ with the maps $N \ni n \mapsto (n, 0) \in N \oplus M$ and $N \oplus M \ni (n, m) \mapsto m \in M$.

Theorem 1.3. *There is a bijection between $E_A(M, N)$ and $\mathrm{Ext}^1_A(M, N)$.*

Remark
Actually, both objects are isomorphic as A-modules.
Note: There is a sum of extensions definable in the following way:

1. There is a $\oplus : E_A(X, Y) \times E_A(X, Y) \to E_A(X \oplus X, Y \oplus Y)$, defined by
   $((0 \to Y \to Q \to X \to 0), (0 \to Y \to Q \to X \to 0)) \mapsto (0 \to Y \oplus Y \to Q \oplus Q \to X \oplus X \to 0)$
2. There is a diagonal map $Y \xrightarrow{\Delta} Y \oplus Y$ $(y \mapsto (y, y))$ and a codiagonal map $X \oplus X \xrightarrow{\nabla} X$ $((x, x') \mapsto x + x')$. The composition $\Delta \oplus \nabla$ gives a sum at $E_A(X, Y)$ (*Bear sum* $\leftarrow$ (Bear is a name)).

Idea of the proof

Take a sequence $0 \to R \to P \to M \to 0$, where P is projective and R is called the representation module.

We call this kind of exact sequence a *presentation of M*. They appear as the shorting of a resolution $\to P_1 \big| \xrightarrow{\varphi_1} P_0 \xrightarrow{\varphi_0} M \to 0$.

We take R as $\mathrm{im}(\varphi_1) = \ker(\varphi_0)$.

Theorem 7 gives an exact sequence

$0 \to \mathrm{Hom}_A(M,N) \xrightarrow{\psi^*} \mathrm{Hom}_A(P,N) \xrightarrow{\varphi^*} \mathrm{Hom}_A(R,N) \to \mathrm{Ext}^1_A(M,N) \to 0 = \mathrm{Ext}^1_A(P,N)$, i.e.

$\mathrm{Ext}^1_A(M,N) = \mathrm{coker}(\varphi^*)$.

We define a map $E_A(M,N) \to \mathrm{Ext}^1_A(M,N)$ and start with $[Q] \in E_A(M,N)$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\varphi} & P & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} & & \| & & \\ 0 & \longrightarrow & N & \xrightarrow[j]{} & Q & \xrightarrow[\chi]{} & M & \longrightarrow & 0 \end{array}$$

Since P is projective there exists $f : P \to Q$.

Since the sequences are exact, we have $f(\varphi(R)) \subseteq N$.

Let's start with $\varphi(r) \in P \Rightarrow \psi(\varphi(r)) = 0 \Rightarrow \chi(f(\varphi(r))) = 0 \Rightarrow f(\varphi(r)) \in \mathrm{im}(j)$ (we have $\chi \circ f = \psi$).

The restriction of f to $\mathrm{im}(\varphi) \cong R$ gives a map $g : R \to N$, i.e. $g \in \mathrm{Hom}_A(R,N)$.

We define $F : E_A(M,N) \to \mathrm{Ext}^1(M,N)$ by $[Q] \mapsto q + \mathrm{im}(\varphi^*) \in \mathrm{coker}(\varphi^*)$.

Note: We have to prove that F is

1. Well-defined,
2. bijective and
3. an isomorphism of modules.

About 3: One has to show that either the Baer sum is mapped to the sum in Ext^1 or just define $+$ at $\mathrm{Ext}_A(M,N)$ induced by F.

About 2: refer to literature, relatively easy.

About 1: One has to show that F is independent of the presentation.

Example

$\mathrm{Ext}^1_2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \ni 0 \longleftrightarrow 0 \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ with $z \mapsto (z,0)$ and $(z,\overline{z}) \mapsto \overline{z}$

$1 \longleftrightarrow 0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

Definition (homotopy)

Let $\mathbf{C}, \mathbf{D}$ be complexes, $\mathbf{f}, \mathbf{g} : \mathbf{C} \to \mathbf{D}$ homomorphisms

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & C_j & \xrightarrow{\delta_j} & C_{j-1} & \longrightarrow & \cdots & & \\ & \swarrow^{H_j} & \downarrow{\scriptstyle f,g} & \swarrow^{H_{j-1}} & \downarrow{\scriptstyle f,g} & & & & \\ D_{j+1} & \xrightarrow[\delta'_{j+1}]{} & D_j & \xrightarrow[\delta'_j]{} & D_{j-1} & \longrightarrow & \cdots & & \end{array}$$

A map $\mathbf{H}{:}\mathbf{C}{\to}\mathbf{D}[1]$ ($\leftarrow$ index shift for complexes) is called a *homotopy* of f and g if there holds $f - g = \delta'_{j+1} \circ \mathbf{H}_j + \mathbf{H}_{j-1} \circ \delta_j$.

Especially, you define homotopy-equivalent complexes and prove that homotopy-equivalent complexes have the same homology.

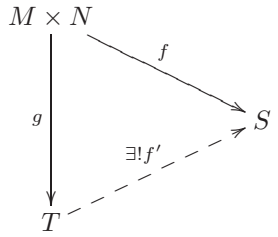
Apply this to resolution: Two resolutions are homotopy equivalent ($\Rightarrow$ derived functors are well-defined).

1.5 Tensor Product

Again, let A be a commutative ring with 1.

Theorem 1.4. (Definition of the tensor product (1)) *Let M, N be A-modules. There exists an A-module T and an A-bilinear map $g : M \times N \to T$ such that:*
$\forall A$-modules $S : \forall f : M \times N \to S$ bilinear: $\exists! f' : T \to S$ (A-module homomorphism):$f = f' \circ g$.

(*)



Warning: g, f are bilinear and f' is a homomorphism.
This T is uniquely determined up to isomorphisms of A-modules. We denote it by $M \otimes_A N$ and call it tensor produkt*.*

Proof:

1. Uniqueness:

   Assume, we have (T, g) and (T', g') with this property (*).

   Apply this property for (T, g) with $(S, f) = (T', g')$.

   $\exists! h : T \to T', g' = h \circ g$

   Vice versa, we obtain a map $h' : T' \to T$ such that $g = h' \circ g'$. (Apply (*) for (T', g') and $(S, f) = (T, g)$.) The uniqueness gives us $h' \circ h = \mathrm{id}_T$ and $h \circ h' = \mathrm{id}_{T'}$.

   $\Rightarrow h$ is an isomorphism of T and T'.

2. Existence:

   Define F as the free A-module freely generated by the elements of $M \times N$:

   $F = \bigoplus_{(m,n) \in M \times N} A = \{\sum_\nu a_\nu (x_\nu, y_\nu) | a_\nu \in A, x_\nu \in M, y_\nu \in N\}$

   Define the submodule $F_0 \subseteq F$ as the module generated by terms of type

   $$\begin{array}{l} (x + x', y) - (x, y) - (x', y) \\ (x, y + y') - (x, y) - (x, y') \\ (ax, y) - a \cdot (x, y) \\ (x, ay) - a \cdot (x, y) \end{array} \qquad a \in A, x, x' \in M, y, y' \in N$$

   Define $T = F/F_0$ and denote the class $(x, y) + F_0$ as $x \otimes y$.

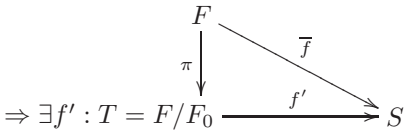
   Obviously, T is generated by $\{x \otimes y | x \in M, y \in N\}$, but no longer freely generated. In general T is much larger than $M \times N$.

   By the definition of F_0, the map $g : (x, y) \mapsto x \otimes y$ is bilinear, since we have

   $(x + x') \otimes y = x \otimes y + x' \otimes y, x \otimes (y + y') = x \otimes y + x \otimes y', (ax) \otimes y = a(x \otimes y)$ and $x \otimes (ay) = a(x \otimes y)$.

   Let $f : M \times N \to S$ be a bilinear map. There is a formal extension $\overline{f} : F \to S$, where $\overline{f}$ is a homomorphism of A-modules.

   Since f is bilinear, $\ker(\overline{f}) \supseteq F_0$.



f' is by construction a homomorphism of A-modules.

$f' \circ g = f$ holds because it coincides for elements of $M \times N$ by definition. It is unique because the extension to F is unique.

Hence, f' is unique. □

Remark

(a) Don't use this construction for practical purposes. Use the (*)-property instead.

(b) We may think of $M \otimes_A N$ as the *space of all A-bilinear maps from* $M \times N \to A$.

Example

1. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$

2. Let V, W be finite-dimensional K-vector spaces.

   There is a natural isomorphism $V \otimes_A W \cong \mathrm{Hom}_K(\mathrm{Hom}_K(V, K), W)$.

   Check that

$$\begin{array}{ccccc} V \times W & \ni & (v, w) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_K(\mathrm{Hom}_K(V,K), W) & \ni & \mathrm{Hom}_K(V,K) \ni \varphi \mapsto \varphi(v) = w \end{array}$$

   has the property (*).

   We have $\dim(V \otimes_K W) = \dim V \cdot \dim W$.

Theorem 1.5. (Definition of the tensor product (2)) *Let $M_1, ..., M_r$ be A-modules.*
There exists an A-module T and an A-multilinear map $g : M_1 \times ... \times M_r \to T$ such that for all multilinear $f : M_1 \times ... \times M_r \to S$ holds: $\exists! f' : T \to S : f = f' \circ g$.
Again, (T, g) is uniquely determined up to isomorphism. We denote it by $M_1 \otimes_A M_2 \otimes_A ... \otimes_A M_r$.
Definiton: Analogous.

Proposition 1.8. (3)

1. $M \otimes_A N \cong N \otimes_A M$

2. $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P) \cong M \otimes_A N \otimes_A P$

3. $A \otimes_A M \cong M$

Proof:
Check that the universal properties are fulfilled. □

Warning
Many people like physicists and differential geometers use elements of tensor products coefficentwise: $\sum g_{k,l}^{i,j} \in \underbrace{V_1^* \otimes V_2^*}_{\text{dual vectorspaces}} \otimes \underbrace{V_3 \otimes V_4}_{\text{vectorspaces}}$.

Functoriality
Let $f : M \to M', g : N \to N'$ be homomorphisms of A-modules. Then, $h : M \times N \to M' \otimes_A N'$ (defined by $(x, y) \mapsto f(x) \otimes g(y)$) is bilinear.
$\Rightarrow \exists! f \otimes g : M \otimes_A N \to M' \otimes_A N'$ (homomorphism of A-modules), i.e. $(M \otimes_A \_)$ and $(\_ \otimes_A N)$ are covariant functors from A-modules to A-modules.

Restriction/Extension of scalars:
Let $f : A \to B$ be a homomorphism of rings and N be a B-module. By $a \cdot x = f(a) \cdot x$ we can regard N also as an A-module (restriction of scalars).
If N is a freely generated B-module and B is a freely generated A-module, then N is also a freely generated A-module. We can invert this by using the tensor product.
If M is an A-module, the module $M_B = B \otimes_A M$ is a B-module (*extension of scalars*).
If M is a freely generated A-module, then M_B is a freely generated B-module. (Note that in general for freely generated M and N, $M \otimes_A N$ is also freely generated.)

Lemma 1.16. (4) *Let M, N, P be A-modules.*
Then, $\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$.

Proof:
Let be $f' \in \mathrm{Hom}_A(M \otimes_A N, P)$. This induces an A-bilinear map.
$f : M \times N \to P$
This gives $\varphi : M \to \mathrm{Hom}_A(N, P)$, defined by $x \mapsto f(x, \_)$.
$\Rightarrow$ We have a homomorphism $F : \mathrm{Hom}_A(M \otimes_A N, P) \to \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$ with $f' \mapsto \varphi$.
Let $\varphi \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$.
By sending $(x, y) \mapsto \varphi(x)(y)$ we obtain a bilinear map $f : M \times N \to P$.
By the universal property we get $\exists! f' : M \otimes_A N \to P : f'(x \otimes y) = f(x, y)$.
$\varphi \mapsto f'$ is just the inverse map of F. □

Lemma 1.17. (5) *Let N be an A-module and $\mathcal{E} : M' \xrightarrow{\varphi} M \to M'' \to 0$ an exact sequence.*
Then $\mathcal{E} \otimes_A N : M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0$ is exact.

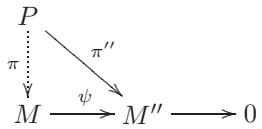
Proof:
$\mathcal{E}$ is exact $\Rightarrow \mathrm{Hom}_A(\mathcal{E}, \mathrm{Hom}_A(N, P))$ is exact. Use lemma 4 to obtain the exactness of the isomorphic sequence $\forall P : \mathrm{Hom}_A(\mathcal{E} \times N, P)$.
$\Rightarrow \mathcal{E} \otimes_A N$ is exact. □

Remark
Again, we can try to complete the exact sequence on the left hand side:
$? \to M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to$.

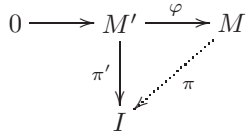
Lecture on 2007-11-22

Remark
We have an interpretation of $\mathrm{Ext}^1_A(M, N)$ as the isomorphism classes of extensions Q of the sequence $0 \to M \to Q \to N \to 0$.

Remark (duality of projective and injective modules)
Remember: P is projective, iff for every surjective A-module homomorphism $\psi : M \to M'$ and A-module homomorphism $\pi'' : P \to M''$, there exists an A module homomorphism $\pi : P \to M$ such that $\psi \circ \pi = \pi''$:



A module is *injective*, iff for every injective A-module homomorphism $\varphi : M' \to M$ and every A-module homomorphism $\pi' : M \to I$, there exists an A module homomorphism $\pi : M \to I$ such that $\pi' = \pi \circ \varphi$:



Now, we can define *injective resolutions* $\mathbf{I} : 0 \to I_0 \to I_1 \to I_2 \to \cdots$ of M by the following properties:

1. I_n are injective for all $n \in \mathbb{N}$.
2. $\forall n \in \mathbb{N}_{>0} : H^n(\mathbf{I}) = 0$
3. $H^0(\mathbf{I}) \cong M$

We can apply a covariant functor to $\mathbf{I}$ to get a right derived functor or we can apply a contravariant functor, to get a left derived functor.

1.6 The functor Tor

We continue to fix A as a commutative ring with 1. Furthermore, fix $N \in Ob(\mathfrak{M}_A)$ and consider the covariant, right-exact functor $\_ \otimes_A N : \mathfrak{M}_A \to \mathfrak{M}_A$.
We want to apply the concept of left-derived functors to $\_ \otimes_A N$: We take $M \in Ob(\mathfrak{M}_A)$, choose a projectve resolution of M, i.e. $\mathbf{P} : \cdots \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to 0$, apply $\_ \otimes_A N$ to $\mathbf{P}$ and get the chain complex $\mathbf{P} \otimes_A N : \cdots \to P_n \otimes_A N \to P_{n-1} \otimes_A N \to \cdots \to P_1 \otimes_A N \to P_0 \otimes_A N \to 0$.
Now, we take homology of $\mathbf{P} \otimes_A N$ and get the left-derived functor of $\_ \otimes_A N$.

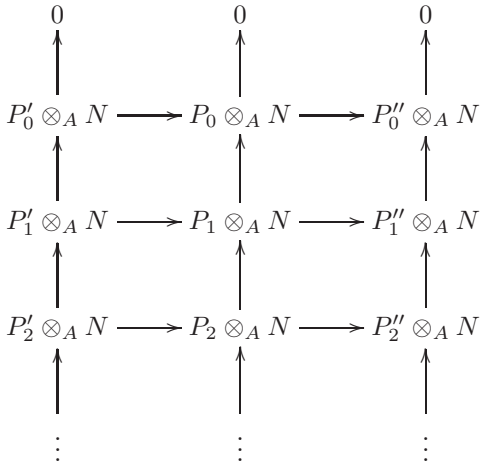
Definition (Tor)
$\mathrm{Tor}_n(M, N) = L_n(\_ \otimes_A N)(M) = H_n(P \otimes_A N)$ is called the n-th Tor-*module* of M and N.
One can show, that this is independent of $\mathbf{P}$.

Remark

1. P projective $\Rightarrow \forall n \in \mathbb{N}_{>0} \mathrm{Tor}_n^A(P, N) = 0$.
2. $\mathrm{Tor}_0^A(M, N) = M \otimes_A N$
3. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of A-modules. Then, we get the long exact sequence

$$\cdots \longrightarrow \mathrm{Tor}_1^A(M', N) \longrightarrow \mathrm{Tor}_1^A(M, N) \longrightarrow \mathrm{Tor}_1^A(M'', N)$$
$$M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0$$

in the diagram



$$\mathbf{P}' \otimes_A N \longrightarrow \mathbf{P} \otimes_A N \longrightarrow \mathbf{P}'' \otimes_A N$$

4. Hint of how to (possibly) compute $\mathrm{Tor}_1^A(M,N)$:

   Given $M \in Ob(\mathfrak{M}_A)$, choose a projective presentation $0 \to \ker\psi = R \xrightarrow{\varphi} P \xrightarrow{\psi} M \to 0$.

   Apply $\mathrm{Tor}_1^A(\_\,, N)$ and get $R \otimes_A N \xrightarrow{\varphi_*} P \otimes_A N \xrightarrow{\psi_*} M \otimes_A N \to 0$ where $\varphi_* = \varphi \otimes_A \mathrm{id}_N$ and $\psi_* = \psi \otimes_A \mathrm{id}_N$.

   From this we get the sequence

   $\mathrm{Tor}_1^A(R,N) \to \mathrm{Tor}_1^A(P,N) \to \mathrm{Tor}_1^A(M,N) \to R \otimes_A N \xrightarrow{\varphi_*} P \otimes_A N \xrightarrow{\psi_*} M \otimes_A N \to 0$ with $\mathrm{Tor}_1^A(P,N) = 0$ (by remark 1).

   We finally get the exact sequence $0 \to \mathrm{Tor}_1^A(M,N) \to R \otimes_A N \xrightarrow{\varphi_*} P \otimes_A N \xrightarrow{\psi_*} M \otimes_A N \to 0$.
   $\Rightarrow \mathrm{Tor}_1^A(M,N) = \ker(\varphi_*)$

1.7 Tensor algebra

Fix a commutative ring A with 1.

Definition (algebra)
Let B be a, not necessarily commutative, ring and $f : A \to B$ a ring homomorphism.
By setting $a \cdot b = f(a) \cdot b$ $(a \in A, b \in B)$, B can be viewed as an A-module.
Hence, B has two structures:

1. B has a multiplicative structure (from the ring structure)
2. B has an A-module structure (from $f : A \to B$)

In this situation B is called an *A-algebra*.

Example

1. $A = \mathbb{R}, B = \mathbb{H}$ (*Hamilitonians*)
   $\mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R}$ with $\{1,i,j,k\}$ linear independent.
   We have a homomorphism $f : \mathbb{R} \hookrightarrow \mathbb{R} + i \cdot 0 + j \cdot 0 + k \cdot 0$.
   Further: $i^2 = j^2 = k^2 = -1, k = ij = -ji, i = jk = -kj, j = ki = -ik$
   $\Rightarrow (a+bi+cj+dk)\cdot(a'+b'i+c'j+d'k) = aa'-bb'-cc'-dd'+(a'b+ab'+cd'-dc')i+(...)j+(...)k$

2. Let be $A = K$ a field and $B = K[X_1, ..., X_n]$ the polynomials in n variables.

   $\Rightarrow K[X_1, ..., X_n]$ is a K-algebra.

   $f : K \to K[X_1, ..., x_n]$ is defined by $\alpha \mapsto \alpha =$ constant polynomial.

   $\sum_{i_1,...,i_n \in \mathbb{N}} \alpha_{i_1,...,i_n} X_1^{i_1} \cdots X_n^{i_n} = p(X_1, ..., x_n) \in K[X_1, ..., X_n]$

Definition (finitely generated)
An A-algebra is *finitely generated* if there exist $b_1, ..., b_n \in B$ such that every element $b \in B$ can be expressed as a (finite) sum of products of b_1,...,b_n, i.e. in the commutative case we get $b = \sum_{i_1,...,i_n \in \mathbb{N}} \alpha_{i_1,...,i_n} b_1^{i_1} \cdots b_n^{i_n}$ with $\alpha_{i_1,...,i_n} \in A$ and non-zero only for finitely many tuples $(i_1, ..., i_n)$.

Example
$k[X_1, ..., X_n]$ is finitely generated (as a K-algebra), namely by $X_1, ..., X_n$.

Remark
Let B be a finitely generated, commutative A-algebra.
Get a surjective ring homomorphism by mapping
$K[X_1, ..., X_n] \to B = \{\sum_{i_1,...,i_n \in \mathbb{N}} \alpha_{i_1,...,i_n} b_1^{i_1} \cdots b_n^{i_n}\}$ with $X_j \mapsto b_j$.
Conclusion: B is the quotient ring of $K[X_1, ..., X_n]$ by some ideal $\mathfrak{a}$: $B = K[X_1, ..., X_n]/\mathfrak{a}$

Observation
Let B, C be A-algebras (in particular B, C are A-modules). Consider the tensor product $B \oplus_A C$. This is an A-module. We have to carry over the multiplicative structures of B, C to the tensor product, via the generators of $B \oplus_A C$:
$(b_a \otimes c_1) \cdot (b_2 \otimes c_2) = (b_1 \cdot b_2) \otimes (c_1 \cdot c_2)$
This has to be linearly extended.
Now, we get $(\sum_i \alpha_i b_i \otimes c_i) \cdot (\sum_j \alpha_j b'_j \otimes c'_j) = (\sum_{i,j} \alpha_i \alpha_j (b_i \otimes c_i)(b'_i \otimes c'_i)$.

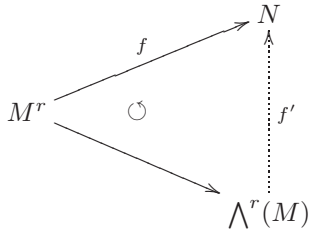
Tensor algebra
Let now M be an A-module.
We define $T^r(M) = \begin{cases} A & r = 0 \\ M^{\otimes r} & r > 0 \end{cases}$ where $M^{\otimes r}$ denotes the tensor product $\underbrace{M \otimes \cdots \otimes M}_{r \text{ times}}$.
We set $T(M) = \bigcup_{r=0}^{\infty} T^r(M)$.
$T(M)$ is an A-module. We want to make $T(M)$ an A-algebra:
One has to define, how tensors can be multiplied.
We define $(x_1 \otimes ... \otimes x_r) \cdot (y_1 \otimes ... \otimes y_s) = (x_1 \otimes ... \otimes x_r \otimes y_1 \otimes ... \otimes y_s)$ and extend this definition linearly. In this way $T(M)$ receives a multiplicative structure (which is associative and distributive). All in all, $T(M)$ becomes an A-algebra. (We use the map $A \to T(M)$, which is defined by $\alpha \mapsto (\alpha, 0, ..., 0)$.)
Note: The product needs not to be commutative!

Definition (Tensor algebra)
$T(M)$ is called the *tensor algebra* of M.

Remark
$T(M)$ (as an A-algebra) is generated by the elements of $M = T^1(M)$.

Example (exterior algebra, alternating algebra, Graßmann algebra (1))
In the r-fold tensor product $T^r(M) = M^{\otimes r}$ consider the submodule $T_a^r(M)$, generated by th tensors of the form $x_1 \otimes ... \otimes x_r$ with $x_i = x_j$ for some $i, j, i \neq j, i, j = 1, ..., r$. Define the quotient module $\bigwedge^r(M) = T^r(M)/T_a^r(M)$.
We call $\bigwedge^r(M)$ the *r-fold exterior* (or *alternating*) *product* of M.
Denote the image of $x_1 \otimes ... \otimes x_r \in T^r(M)$ in $\bigwedge^r(M)$ by $x_1 \wedge ... \wedge x_r$.
Note: Let $x, y \in M$, then $x \wedge y = -y \wedge x$ in $\bigwedge^2(M)$.
$$0 = (x+y) \wedge (x+y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y$$
$$\uparrow$$
$$(x+y) \otimes (x+y) = 0 + x \wedge y + y \wedge x + 0$$
$$\Rightarrow x \wedge y = -y \wedge x$$

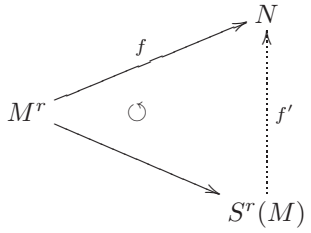
Remark
$\bigwedge^r(M)$ has the following universal mapping property:
Given $f : M^r \to N$ an A multilinear and alternating map, then there exists a unique A-module homomorphism $f' : \bigwedge^r(M) \to N$ such that the following diagram commutes:



Example (exterior algebra, alternating algebra, Graßmann algebra (2))
Let be $A = K$ a field, $M = V$ a K-vector space of dimension $\dim_K V = n$ and $\{b_1, ..., b_n\}$ a K-basis.
$$\Rightarrow \dim_K \bigwedge^r(V) = \begin{cases} 0 & r > n \\ \binom{n}{r} & 0 \leq r \leq n \end{cases}$$
In the case of $r = n$ we have $\dim_K \bigwedge^n(V) = 1$, i.e. $b_1 \wedge ... \wedge b_n$ is a basis for $\bigwedge^n(V)$.
Let $x_1, ..., x_n \in V$ be n vectors:
$x_j = \sum_{k=1}^n \alpha_{k,j} b_k$ (expand).
$x_1 \wedge ... \wedge x_n = b_1 \wedge ... \wedge b_n = \det(\alpha_{k,j}) \cdot b_1 \wedge ... \wedge b_n$
Finally, consider $T_a(M) = \bigoplus_{r=0}^\infty T_a^r(M) \subseteq T(M) = \bigoplus_{r=0}^\infty T^r(M)$
Check: $T_a(M)$ is an ideal in $T(M)$.
Consider the quotient ring/algebra:
$\bigwedge(M) = T(M)/T_a(M) = \bigoplus_{r=0}^\infty \bigwedge^r(M)$
$\bigwedge(M)$ is an A-algebra.
It is called the *exterior* (or *alternating*, or *Graßmann*) *algebra* of M.

Example (Symmetric algebra (1))
In the r-fold tensor product $T^r(M)$, consider the submodule $T_s^r(M)$ generated by elements of the form $x_1 \otimes ... \otimes x_r - x\pi(1) \otimes ... \otimes x_{\pi(r)}$, where $\pi \in S_n$ (the *symmetric group* of n letters).
Put $S^r(M) = T^r(M)/T_s^r(M)$ and call it the *r-fold symmetric product* of M.
Define the image of $x_1 \otimes ... \otimes x_r \in T^r(M)$ by $x_1 \cdot ... \cdot x_r \in S^r(M)$. Note, that the product does not depend on the order.

Remark (Symmetric algebra)
$S^r(M)$ has the following universal mapping property:
Given $f : M^r \to N$, an A-multilinear and symmetric ($\forall \pi \in S_r : f(x_1, ..., x_r) = f(x_{\pi(1)}, ..., x_{\pi(r)})$) map, then there exists a unique A-module homomorphism $f' : S^r(M) \to N$ such that the following diagram commutes:



Example (Symmetric algebra (2))
Finally, consider
$T_s(M) = \bigoplus_{r=0}^{\infty} T_s^r(M) \subseteq T(M)$.
Check: $T_s(M) \subseteq T(M)$ is an ideal.
Consider the quotient ring (= A-algebra) $S(M) = \bigoplus_{r=0}^{\infty} T^r(M)/T_s^r(M) = \bigoplus_{r=0}^{\infty} S^r(M)$. This is the *symmetric algebra* of M.

Lecture on 2007-11-29

1.8 Localization

1.8.1 Localization of rings

Assumption: Let A be a commutative ring with 1.

Definition (multiplicative, multiplicatively closed)
A subset $S \subseteq A$ is called *multiplicative* (or *multiplicatively closed*), iff

1. $1 \in S$
2. $\forall s_1, s_2 \in S : s_1 \cdot s_2 \in S$

Note: $(S, \cdot)$ is a monoid.

Example
$A = \mathbb{Z}, S = \mathbb{Z} \setminus \{0\}$

Construction (equivalence relation)
Let A be as above and $S \subseteq A$ multiplicative.
On $A \times S$, consider the relation $(a, s) \sim (b, t) \overset{Def.}{\iff} \exists u \in S : (a \cdot t - b \cdot s) \cdot u = 0$.
Claim: This defines an equivalence relation on $A \times S$. **Proof:**

1. Reflexive: trivial
2. Symmetry: trivial
3. Transitivity:
   Assume: $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$
   We have to show $(a, s) \sim (c, u)$:
   $(a, s) \sim (b, t) \Leftrightarrow \exists v \in S : (a \cdot t - b \cdot s) \cdot v = 0 \Rightarrow atv - bsv = 0$
   $(b, t) \sim (c, u) \Leftrightarrow \exists w \in S : (b \cdot u - c \cdot t) \cdot w = 0 \Rightarrow buw - ctw = 0$
   $\Rightarrow (atv)uw - (bsv)uw = 0$ and $(buw)sv - (ctw)sv = 0$
   $\Rightarrow (au)(tvw) - (cs)(tvw) = 0 \Rightarrow (au - cs)(tvw) = 0$
   Since $t \cdot v \cdot w \in S$, we have $(a, s) \sim (c, u)$. □

Definition
Set $S^{-1}A = (A \times S)/\sim$, i.e. $S^{-1}A$ is the set of equivalence classes of the relation $\sim$ on $A \times S$, i.e. $S^{-1}A = \{[a,s] | (a,s) \in A \times S\}$ and $[a,s] = \{(b,t) \in A \times S | (b,t) \sim (a,s)\}$.
$S^{-1}A$ is called the *localization* of A in S. A more standard notation for $[a,s]$ is $[a,s] = \frac{a}{s} = a/s$.

Lemma 1.18. (1) *Let $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ and put $\frac{a}{s} + \frac{b}{t} = \frac{a \cdot t + b \cdot s}{s \cdot t} \in S^{-1}A$ and $\frac{a}{s} \cdot bt = \frac{a \cdot b}{s \cdot t} \in S^{-1}A$. These two operations are well-defined and independent on the choice of representatives. With this addition and multiplication $S^{-1}A$ becomes a commutative ring with $\frac{1}{1}$.*

Proof:
Exercises. □

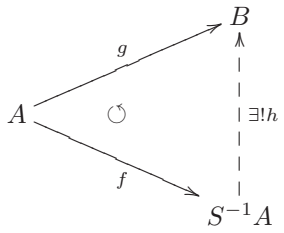
Example

1. $A = \mathbb{Z}, S = \mathbb{Z} \setminus \{0\} \Rightarrow S^{-1}A = \mathbb{Q}$
2. $A =$ integral domain, $S = A \setminus \{0\} \Rightarrow S^{-1}A = \mathrm{Quot}(A)$

Note: In $S^{-1}A$ the element $\frac{a}{s}$ has a multiplicative inverse, if $a \in S$, namely $(\frac{a}{s})^{-1} = \frac{s}{a}$. (Indeed: $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = \frac{1}{1}$)

Remark
Let $A, S^{-1}A$ be as above and define $f : A \to S^{-1}S$ by $a \mapsto \frac{a}{1}$.
One easily checks, that f is a ring homomorphism.
Question: Is f injective?
Assume: $f(a) = \frac{a}{1} = \frac{0}{1}$
$\Rightarrow [a,1] = [0,1] \Rightarrow (a,1) \sim (0,1) \Rightarrow \exists s \in S : (a \cdot 1 - 0 \cdot 1) \cdot s = 0 \Rightarrow \exists s \in S : s \cdot a = 0$
So, in general, injectivity of f fails (if there are zero divisors).

Proposition 1.9. *Let $g : A \to B$ be a ring homomorphism satisfying $g(S) \subseteq B^\times$, with $S \subseteq A$ multiplicative subset.*
Then, there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$, i.e.



Proof:

1. Uniqueness (give a formula for h)

   Assume, h exists: $h : S^{-1}A \to B$ and $g = h \circ f$.

   $a \in A \Rightarrow h(\frac{a}{1}) = h(f(a)) = g(a)$.

   $s \in S \Rightarrow h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = g(s)^{-1}$

   Now, we get the formula $h(\frac{a}{s}) = h(\frac{a}{1} \cdot \frac{1}{s}) = h(\frac{a}{1}) \cdot h(\frac{1}{s}) = g(a) \cdot g(s)^{-1}$.

2. Existence

   By above analysis, set $h(\frac{a}{s}) = g(a) \cdot g(s)^{-1}$. It is immediate to show that h is a ring homomorphism (since g is one) and that $g = h \circ f$.

   What is not clear, is the well-definedness of h!

3. Well-definedness of h

   Let $(a,s),(a',s')$ be representatives of $\frac{a}{s}$.

   Show: $g(a)\cdot g(s)^{-1} = g(a')\cdot g(s')^{-1}$:

   $(a,s)\sim(a',s') \Leftrightarrow \exists t\in S : (a\cdot s' - a'\cdot s)\cdot t = 0$

   $\Rightarrow (g(a)g(s') - g(a')g(s))g(t) = 0 \Rightarrow g(a)g(s') = g(a')g(s) \Rightarrow g(a)\cdot g(s)^{-1} = g(a')\cdot g(s')^{-1}$

Example

1. $\mathfrak{p}\in \mathrm{Spec}(A) \Rightarrow S = A\setminus\mathfrak{p}$ is multiplicative closed.

   $A_p = S^{-1}A \ni \frac{a}{s} \Leftrightarrow a\in A, s\notin\mathfrak{p}$

   $\mathfrak{m} = \{\frac{a}{s} | a\in\mathfrak{p}, s\notin\mathfrak{p}\}$ is an ideal in $A_\mathfrak{p}$.

   Claim: $\mathfrak{m}\subset A_\mathfrak{p}$ is maximal:

   Let $\frac{b}{t}\notin\mathfrak{m}$. $\Rightarrow b\notin\mathfrak{p} \Rightarrow \frac{b}{t}$ has inverse in $A_\mathfrak{p}$. $\Rightarrow 1\in\mathfrak{m} + (\frac{b}{t}) \Rightarrow \mathfrak{m}$ is maximal.

   In fact, we have shown, that $\mathfrak{m}\subset A_\mathfrak{p}$ is the only maximal ideal of $A_\mathfrak{p}$. Hence, $A_\mathfrak{p}$ is a local ring.

   In the case of $A=\mathbb{Z}$ and $\mathfrak{p} = (p), p\in\mathbb{P}$, we have $A_\mathfrak{p} = \mathbb{Z}_{(p)} = \{\frac{a}{s}\in\mathbb{Q} | s,a\in\mathbb{Z}, p\not| s\}$.

2. Let $f\in A$ and $S = \{f^n | n\in\mathbb{N}\}$. S is multiplicatively closed and $S^{-1}A$ is denoted by A_f.

   We get the natural map $A\to A_f$ by $a\mapsto\frac{a}{1}$. Applying the contravariant functor Spec, we get $\mathrm{Spec}(A) \xleftarrow{\varphi^*} \mathrm{Spec}(A_f)$ with $\varphi^{-1}(\mathfrak{q}) \hookleftarrow \mathfrak{q}$. In fact, one has $\varphi^*(\mathrm{Spec}(A_f))\subseteq\mathrm{Spec}(A)$.

1.8.2 Localization of modules

Let A be a commutative ring with 1, $S\subseteq A$ a multiplicative subset and M an A-module.
We define (on $M\times S$): $(m,s)\sim(m',s') \Leftrightarrow \exists t\in S : t\cdot(s'\cdot m - s\cdot m') = 0$.
As before check that $\sim$ is an equivalence relation.

Definition (localization)
We define $S^{-1}M = (M\times S)/\sim$ and call $S^{-1}M$ the *localization* of M in S.

Remark
$S^{-1}M$ is an $S^{-1}A$-module via $\frac{a}{s}\cdot\frac{m}{t} = \frac{am}{st}\in S^{-1}M$.
Again, we have to show the indepence on the choise of representatives.

Lemma 1.19. (3) *Let A,S be as above, M,N A-modules and $f: M\to N$ an A-module homomorphism. Then, f induces an $S^{-1}A$-homomorphism $S^{-1}f: S^{-1}M\to S^{-1}N$ by $\frac{m}{s}\mapsto\frac{f(m)}{s}$.*

Proof:
Just check the properties. □

Summary
S^{-1} is a covariant functor $\mathfrak{M}_A\to\mathfrak{M}_{S^{-1}A}$.

Proposition 1.10. (4) *The functor S^{-1} is exact, i.e. if $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$ is an exact sequence of A-modules (and A-homomorphisms) then the sequence $S^{-1}M' \xrightarrow{S^{-1}\varphi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}M''$ of $S^{-1}A$-modules is also exact.*

Proof:
Exercise.
Show the implication $\mathrm{im}(\varphi) = \ker(\psi) \Rightarrow \mathrm{im}(S^{-1}\varphi) = \ker(S^{-1}\psi)$.
This, you do by showing $\mathrm{im}(S^{-1}\varphi)\subseteq\ker(S^{-1}\psi), \ker(S^{-1}\psi)\subseteq\mathrm{im}(S^{-1}\varphi)$. □

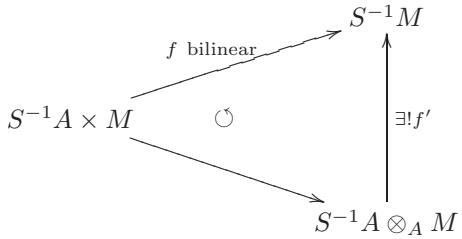
Proposition 1.11. (5) *The functor S^{-1} commutes with finite sums, finite intersections and quotients, i.e., let M', M'' be A-submodules of a (fixed) A-module M, then one has:*

1. $S^{-1}(M' + M'') = S^{-1}M' + S^{-1}M''$
2. $S^{-1}(M' \cap M'') = S^{-1}M' \cap S^{-1}M''$
3. $S^{-1}(M/M') \cong S^{-1}M/S^{-1}M'$

Proof:
Exercise.
Remark: 1. and 2. are straight-forward.
3. follows from proposition 4, namely:
$0 \to M' \to M \to M/M' \to 0$ is exact.
Localising at S yields $0 \to S^{-1}M' \to S^{-1}M \to S^{-1}(M/M') \to 0$ is exact.
$\Rightarrow S^{-1}M/S^{-1}M' \cong S^{-1}(M/M')$ □

Proposition 1.12. (6) *Let M be an A-module.*
Then, we have the isomorphism $S^{-1}A \otimes_A M \cong S^{-1}M$ (as A- and $S^{-1}A$-modules).

Proof:
We start by establishing the claimed A-module isomorphism.
Aim: Construct an A-module homomorphism $S^{-1}A \otimes_A M \to S^{-1}M$, which is surjective and injective.
Consider the map $f : S^{-1}A \times M \to S^{-1}M$, defined by $(\frac{a}{s}, m) \mapsto \frac{am}{s}$. It is immediate to show that f is bilinear. Hence, we have the diagram:



The universal property of $\otimes$ defines a unique A-module homomorphism $f' : S^{-1}A \otimes_A M \to S^{-1}M$. Here, f' is given by $f'(\frac{a}{s} \otimes m) = \frac{a \cdot m}{s}$ and the linear extension.

f' is surjective:
Let $\frac{m}{s} \in S^{-1}M$. Taking $\frac{1}{s} \otimes m \in S^{-1}A \otimes_A M$ you get $f'(\frac{1}{s} \otimes m) = \frac{1 \cdot m}{s} = \frac{m}{s}$.

It is a bit harder to show the injectivity of f': Take an arbitrary element of $S^{-1}A \otimes_A M$, i.e. take a finite sum $\sum_i \frac{a_i}{s_i} \otimes m_i$ such that $f'(\sum_i \frac{a_i}{s_i} \otimes m_i) = 0$, and show $\sum_i \frac{a_i}{s_i} \otimes m_i = 0$.

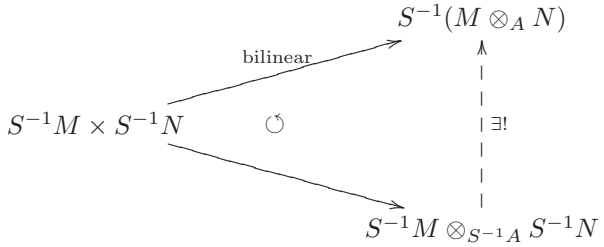
> **Brief interlude** (rewrite $\sum_i \frac{a_i}{s_i} \otimes m_i$)
> Let $s = \prod_j s_j \in S, t_i = \prod_{j \neq i} s_j \in S$.
> Compute: $\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i \cdot t_i}{s} \otimes m_i = \sum_i \frac{1}{s} \otimes (a_i t_i) \cdot m_i = \frac{1}{s} \otimes \sum_i (a_i t_i) \cdot m_i$

Assume: $f'(\frac{1}{s} \otimes m) = 0$ (we show $\frac{1}{s} \otimes m = 0$)
$\Rightarrow \frac{m}{s} = f'(\frac{1}{s} \otimes m) = 0 = \frac{0}{1}$
$\Rightarrow (m, s) \sim (0, 1) \Rightarrow \exists t \in S : t \cdot m = 0$
$\Rightarrow \frac{1}{s} \otimes m = \frac{t}{s \cdot t} \otimes m = \frac{1}{s \cdot t} \otimes t \cdot m = 0$
$\Rightarrow f'$ is injective
$\Rightarrow S^{-1}A \otimes_A M \cong S^{-1}M$ □

Example
Let M be a finitely generated $A = \mathbb{Z}$-module. Let $S = \mathbb{Z} \setminus \{0\}$.
$\overset{\text{Prop. } 6}{\Rightarrow} \mathbb{Q} \otimes_{\mathbb{Z}} M = S^{-1}\mathbb{Z} \otimes_{\mathbb{Z}} M \cong S^{-1}M$

Proposition 1.13. **(S^{-1} commutes with $\otimes$ (7))** *Let M, N be A-modules.*
Then, there is a unique $S^{-1}A$-module isomorphism $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N)$ induced by the map $\frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{s \cdot t}$.

Proof:
Exercise.
Use the following commutative diagram:



□

Proposition 1.14. **(8)** *For an A-module M the following three statements are equivalent:*

1. $M = 0$
2. $\forall \mathfrak{p} \in \operatorname{Spec}(A) : M_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}M = 0$
3. $\forall \mathfrak{m} \in \operatorname{Max}(A) : M_{\mathfrak{m}} = (A \setminus \mathfrak{m})^{-1}M = 0$

Proof:
The implications 1. $\Rightarrow$ 2. $\Rightarrow$ 3. are obious. So, we are left to show 3. $\Rightarrow$ 1..
Assume: $\forall \mathfrak{m} \in \operatorname{Max}(A) : M_{\mathfrak{m}} = 0$ and $M \neq 0$.
Derive a contradiction!
Since $M \neq 0$, there is $0 \neq x \in M$. Let $\mathfrak{a} = \operatorname{Ann}(x) = \{a \in A | a \cdot x = 0\}$ (this is an ideal).
Note: $\mathfrak{a} \neq A$ since $1 \notin A$ and $1 \cdot x = x \neq 0$.
$\Rightarrow \exists \mathfrak{m} \in \operatorname{Max}(A) : \mathfrak{a} \subseteq \mathfrak{m} \subset A$ $(A \setminus \mathfrak{a} \supseteq A \setminus \mathfrak{m} = S)$.
Since $M_{\mathfrak{m}} = 0$, get $\frac{x}{1} = 0$ (in $M_{\mathfrak{m}}$).
$\Rightarrow \exists s \in S = A \setminus \mathfrak{m} : s \cdot x = 0$
$\Rightarrow s \in \operatorname{Ann}(x) = \mathfrak{a}$
On the other hand: $s \in S = A \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{a}$.
$\Rightarrow$ contradiction □

Chapter 2

Noetherian Rings

2.1 Basic properties

Let A be a commutative ring with 1.

Definition
The ring A is called *noetherian*, if every ideal $\mathfrak{a} \subseteq A$ is finitely generated.

Theorem 2.1. (1) *A is noetherian, iff one of the following three properties is satisfied:*

1. *Every ideal $\mathfrak{a} \subseteq A$ is finitely generated.*
2. *Every ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ of ideals becomes stationary, i.e. there is an index n such that we have $\mathfrak{a}_n = \mathfrak{a}_{n+1} = ...$*
3. *Every non-empty set Σ of ideals in A has a maximal element.*

Proof:
We show 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 1..

1. (1) $\Rightarrow$ (2)

   Suppose (1) and let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ be an ascending chain of ideals.

   We define $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$. Since the $\mathfrak{a}_i$'s come from an ascending chain, $\mathfrak{a}$ is an ideal.

   By (1): $\mathfrak{a} = (a_1, ..., a_m)$.

   $\exists n : \mathfrak{a}_n \ni a_1, ..., a_m$

   $\Rightarrow \mathfrak{a}_n \subseteq \bigcup_i \mathfrak{a}_i = \mathfrak{a} \subseteq \mathfrak{a}_n$

   $\Rightarrow \mathfrak{a} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = ...$

Lecture on 2007-12-06

2. (2) $\Rightarrow$ (3)

   Let Σ be a non-empty set of ideals in A. Let $\mathfrak{a} \in \Sigma$. Either $\mathfrak{a}_1$ is maximal or not. If not, there is $\mathfrak{a}_2 \in \Sigma$, such that $\mathfrak{a}_2 \subset \mathfrak{a}_1$. Now, either $\mathfrak{a}_2$ is maximal ideal or not. Continuing this way, we either get a maximal ideal in Σ or we construct an ascending chain $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset ...$, which does not become stationary, contradicting (2).

3. (3) $\Rightarrow$ (1):

   So assume (3) and let $\mathfrak{a} \subseteq A$ be an arbitrary ideal. We want to show that $\mathfrak{a}$ is finitely generated. Let Σ be the set of ideals generated by finitely many elements of $\mathfrak{a}$:

$\Sigma = \{(a_1, ..., a_m) | a_1, ..., a_m \in \mathfrak{a}\} \supseteq \{(0)\} \neq \emptyset$.

By (3) there eists $\mathfrak{b} \in \Sigma$, which is maximal, say $\mathfrak{b} = (a_1, ..., a_m), a_1, ..., a_m \in \mathfrak{a}$. By construction we have $\mathfrak{b} \subseteq \mathfrak{a}$.

We will show that $\mathfrak{b} = \mathfrak{a}$.

Assume: $\mathfrak{b} \subset \mathfrak{a}$, i.e. $\exists a \in \mathfrak{a} \setminus \mathfrak{b}$.

Now, we take $(a_1, ..., a_m, a)$. We have $(a_1, ..., a_m, a) \in \Sigma$ and $(a_1, ..., a_m, a) \subset \mathfrak{b}$, what is a contradiction to the maximality of $\mathfrak{b}$.

$\Rightarrow \mathfrak{a} = \mathfrak{b}$ is finitely generated. □

Example

1. The ring $A = \mathbb{Z}$ is noetherian. (Every ideal $\mathfrak{a} \subseteq \mathbb{Z}$ is generated by the smallest positive element $0 < a \in \mathfrak{a}$. This can be proven by dividing any element $b \in \mathfrak{a}$ by a with rest: $b = qa + r$. We see that $r = 0$.)
2. The ring $A = K[X]$ (K is a field) is also noetherian. (Use the same proof as in $\mathbb{Z}$.)

Definition
An A-module M is *noetherian*, if every ascending chain of submodules gets stationary.

Theorem 2.2. (2) *Let M be an A-module. Then, the following three statements are equivalent:*

1. *Every submodule of M is finitely generated.*
2. *Every ascending chain of submodules becomes stationary.*
3. *Every non-empty set Σ of submodules in M has a maximal element.*

Proof:
We proof this theorem analogously to the theorem 1. We just replace A by M and the word *ideal* by *submodule*. □

Proposition 2.1. (3) *The following three statements hold:*

1. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of A-modules. Then, M is noetherian if and only if M' and M'' are noetherian.*
2. *Let M_k $(k = 1, ..., n)$ be noetherien A-modules. Then, the direct sum $\bigoplus_{k=1}^{n} M_k$ is also noetherian.*
3. *Let A be an noetherian ring and M a finitely generated A-module. Then, M is noetherian.*

Proof:

1. Exercise.
2. Exercise.
3. Since A is noetherian, by 2. $A^n = \bigoplus_{k=1}^{n} A, n \in \mathbb{N}$ is a noetherian A-module.

   Since M is a finitely generated A-module, we have a surjective A-module homomorphism $\varphi: A^n \to M$, defined by $\varphi(a_1, ..., a_m) = \sum_{k=1}^{n} a_k m_k$.

   $\Leftrightarrow 0 \to \ker(\varphi) \to A^n \to M \to 0$ is exact

   $\Rightarrow M$ is noetherian. □

Theorem 2.3. (Hilbert's Basis Theorem (4)) *Let A be a notherian ring.*
Then, the polynomial ring $A[X]$ is also noetherian.

Proof:

We denote ideals in A by $\mathfrak{a}, \mathfrak{b}, ...$ and ideals in $A[X]$ by $\mathcal{A}, \mathcal{B}, ...$

We will show that every ascending chain $\mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \mathcal{A}_3 \subseteq ...$ if ideals in $A[X]$ becomes stationary.

The proof is divided into three parts, the first two of which are preparatory flavour.

1. For an ideal $\mathcal{A} \subseteq A[X]$, we put for $n \in \mathbb{N}$: $\mathfrak{a}_n = \{a \in A | \exists f \in \mathcal{A} : f(X) = aX^n + ...\}$. One easily checks that $\mathfrak{a}_n \subseteq A$ are ideals. Since $f \in \mathcal{A}$ implies $X \cdot f \in \mathcal{A}$, we see $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}, n \in \mathbb{N}$.

   Given $\mathcal{A} \subseteq A[X]$ an ideal, we have attached to it the ascending chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq ...$ of ideals in A.

2. Let now $\mathcal{A}, \mathcal{B} \subseteq A[X]$ be two ideals with associated chains $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq ...$ and $\mathfrak{b}_0 \subseteq \mathfrak{b}_1 \subseteq ...$, respectively. Obviously, the inclusion $\mathcal{A} \subseteq \mathcal{B}$ implies inclusions $\mathfrak{a}_n \subseteq \mathfrak{b}_n$ for all $n \in \mathbb{N}$.

   Claim: Assume $\mathcal{A} \subseteq \mathcal{B}$ and $\forall n \in \mathbb{N} : \mathfrak{a}_n = \mathfrak{b}_n$, then $\mathcal{A} = \mathcal{B}$.

   Proof: Induction on the degree of the polynomials in $\mathcal{B}$, in order to show $\mathcal{A} \supseteq \mathcal{B}$.

   Let $f \in \mathcal{B}$ be a polynomial of degree 0, i.e. a constant.

   Then, $f \in \mathfrak{b}_0 = \mathfrak{a}_0 =$ constant polynomials in $\mathcal{A}$, hence $f \in \mathcal{A}$.

   Now, assume that every polynomial of degree k $(0 \leq k < n)$ in $\mathcal{B}$ belongs to $\mathcal{A}$. We want to prove that this also holds for degree n.

   Let be $f(X) = aX^n + b_{n-1}X^{n-1} + ... + b_0 \in \mathcal{B}$.

   We have $a \in \mathfrak{b}_n = \mathfrak{a}_n$.

   $\Rightarrow \exists g \in \mathcal{A} : g(X) = aX^n + a_{n-1}X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathcal{A} \subseteq \mathcal{B}$

   Consider $f - g \in \mathcal{B}$, with $\deg(f - g) < n$.

   $\Rightarrow f - g \in \mathcal{A}$

   But, by construction, $g \in \mathcal{A}$, hence $f = (f - g) + g \in \mathcal{A}$ This completes the induction.

   $\Rightarrow \mathcal{B} \subseteq \mathcal{A}$

   $\Rightarrow \mathcal{A} = \mathcal{B}$

3. Let now by $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq ...$ be an ascending chain of ideals in $A[X]$. We want to show that it becomes stationary.

   Attached to $\mathcal{A}_k$ we have the chain $\mathfrak{a}_{k,0} \subseteq \mathfrak{a}_{k,1} \subseteq \mathfrak{a}_{k,2} \subseteq ....$

   We get the following scheme:

$$\begin{array}{c|ccccccc}
\mathcal{A}_0 & \mathfrak{a}_{0,0} & \subseteq & \mathfrak{a}_{0,1} & \subseteq & \mathfrak{a}_{0,2} & \subseteq & ... \\
\cap| & \cap| & & \cap| & & \cap| & & \\
\mathcal{A}_1 & \mathfrak{a}_{1,0} & \subseteq & \mathfrak{a}_{1,1} & \subseteq & \mathfrak{a}_{1,2} & \subseteq & ... \\
\cap| & \cap| & & \cap| & & \cap| & & \\
\mathcal{A}_2 & \mathfrak{a}_{2,0} & \subseteq & \mathfrak{a}_{2,1} & \subseteq & \mathfrak{a}_{2,2} & \subseteq & ... \\
\cap| & \cap| & & \cap| & & \cap| & & \\
\vdots & \vdots & & \vdots & & \vdots & & \ddots
\end{array}$$

   By construction, looking at the diagonal, we get the ascending chain $\mathfrak{a}_{0,0} \subseteq \mathfrak{a}_{1,1} \subseteq \mathfrak{a}_{2,2} \subseteq ...$ which has to become stationary. Hence, there exists $m \in \mathbb{N}$ such that

$$
\begin{array}{c|ccccccccccccc}
\mathcal{A}_0 & \mathfrak{a}_{0,0} & \subseteq & \mathfrak{a}_{0,1} & \subseteq & \mathfrak{a}_{0,2} & \subseteq & \ldots & \subseteq & \mathfrak{a}_{0,m} & \subseteq & \mathfrak{a}_{0,m+1} & \subseteq & \ldots \\
\cap| & \cap| & & \cap| & & \cap| & & & & \cap| & & \cap| & & \\
\mathcal{A}_1 & \mathfrak{a}_{1,0} & \subseteq & \mathfrak{a}_{1,1} & \subseteq & \mathfrak{a}_{1,2} & \subseteq & \ldots & \subseteq & \mathfrak{a}_{1,m} & \subseteq & \mathfrak{a}_{1,m+1} & \subseteq & \ldots \\
\cap| & \cap| & & \cap| & & \cap| & & & & \cap| & & \cap| & & \\
\mathcal{A}_2 & \mathfrak{a}_{2,0} & \subseteq & \mathfrak{a}_{2,1} & \subseteq & \mathfrak{a}_{2,2} & \subseteq & \ldots & \subseteq & \mathfrak{a}_{2,m} & \subseteq & \mathfrak{a}_{2,m+1} & \subseteq & \ldots \\
\cap| & \cap| & & \cap| & & \cap| & & & & \cap| & & \cap| & & \\
\vdots & \vdots & & \vdots & & \vdots & & \ddots & & \vdots & & \vdots & & \ddots \\
\cap| & \cap| & & \cap| & & \cap| & & & & \cap| & & \cap| & & \\
\mathcal{A}_m & \mathfrak{a}_{m,0} & \subseteq & \mathfrak{a}_{m,1} & \subseteq & \mathfrak{a}_{m,2} & \subseteq & \ldots & \subseteq & \mathfrak{a}_{m,m} & = & \mathfrak{a}_{m,m+1} & = & \ldots \\
\cap| & \cap| & & \cap| & & \cap| & & & & \| & \diagdown & \| & & \\
\mathcal{A}_{m+1} & \mathfrak{a}_{m+1,0} & \subseteq & \mathfrak{a}_{m+1,1} & \subseteq & \mathfrak{a}_{m+1,2} & \subseteq & \ldots & \subseteq & \mathfrak{a}_{m+1,m} & = & \mathfrak{a}_{m+1,m+1} & = & \ldots \\
\cap| & \cap| & & \cap| & & \cap| & & & & \| & & \| & & \\
\vdots & \vdots & & \vdots & & \vdots & & \ddots & & \vdots & & \vdots & & \ddots
\end{array}
$$

Further the m columns

$$
\begin{array}{c|c|c|c}
\mathfrak{a}_{0,0} & \mathfrak{a}_{0,1} & \ldots & \mathfrak{a}_{0,m-1} \\
\cap| & \cap| & & \cap| \\
\mathfrak{a}_{1,0} & \mathfrak{a}_{1,1} & \ldots & \mathfrak{a}_{1,m-1} \\
\cap| & \cap| & & \cap| \\
\mathfrak{a}_{2,0} & \mathfrak{a}_{2,1} & \ldots & \mathfrak{a}_{2,m-1} \\
\cap| & \cap| & & \cap| \\
\vdots & \vdots & & \vdots
\end{array}
$$

become also stationary. There exists an index $n \in \mathbb{N}$ such that starting from the n-th row, ALL columns become stationary.

Choosing $\mathcal{B} = \mathcal{A}_n$ and $\mathcal{A} = A_{n+1}$, we get $\mathcal{A}_n = \mathcal{A}_{n+1} = \mathcal{A}_{n+2} = ...$ □

Corollary 2.1. (5) *If A is a noetherian ring, then the polynomial ring $A[X_1, ..., X_n]$ in n variables is also noetherian.*

Proof:
Use theorem 4 inductively. □

Corollary 2.2. (6) *Let B be a finitely generated, commutative A-algebra.*
If A is noetherian, then also B (as a ring) is noetherian.

Proof:
Since B is finitely generated (say by the elements $b_1, ..., b_n$) as an A-algebra, there is a surjective ring homomorphism $\varphi : A[X_1, ..., X_n] \to B$, given by $X_j \mapsto b_j$. Now, by Hilbert's Basis Theorem, $A[X_1, ..., X_n]$ is noetherian (Corollary 5).
Hence, B - as surjective image of φ - is also noetherian. (We have to show, that every ideal $\mathfrak{a} \subseteq B$ is finitely generated. Take $\varphi^{-1}(\mathfrak{a}) \subseteq A[X_1, ..., x_n]$, this is finitely generated, hence $\mathfrak{a}$ itself is also finitely generated.) □

Theorem 2.4. (7) *Let $A \subseteq B \subseteq C$ be commutative rings. Furthermore assume:*

1. *A is noetherian*
2. *C is a finitely generated A-algebra*
3. *C is a finitely generated B-module*

Then, B is a finitely generated A-algebra.

Proof:
By 2.: Let $\{x_1, ..., x_m\}$ be a set of generators of C as an A-algebra.
By 3.: Let $\{y_1, ..., y_n\}$ be a set of generators of C as an B-module.
Write: $x_i = \sum_{j=1}^{n} b_{i,j} y_j, b_{i,j} \in B$ and $y_i y_j = \sum_{k=1}^{n} b_{i,j,k} y_k, b_{i,j,k} \in B$
Let B_0 be the A-algebra, generated by $b_{i,j}$ and $b_{i,j,k}$.
Note: B_0 is a finitely generated A-algebra (by construction). Since, by 1., A is noetherian, by Corollary 6, B_0 is also noetherian.
Let's recognize C as a finitely generated B_0-module: Let $c \in C : c = \sum_{i_1,...,i_n \in \mathbb{N}} a_{i_1,...,i_n} x_1^{i_i} \cdot ... \cdot x_m^{i_m}$.
By substitiuting the x_i's by sums of the y_i's and using the above formulae, c can be expressed as a linear combination of the y_j's with coefficients in B_0.
Hence, $y_1, ..., y_n$ generate C as a B_0-module, i.e. C is a finitely generated B_0-module. By Proposition 3, C is a noetherian B_0-module. Now, B viewed as a B_0-module is a submodule of the noetherian B_0-module C.
By definition, then B has to be a finitely generated B_0-module, hence it is finitely generated as B_0-algebra.
Situation: B is a finitely generated B_0-algebra and B_0 is a finitely generated A-algebra.
By transitivity, B is a finitely generated A-algebra. □

Theorem 2.5. (8) *Let K be a field and E a finitely generated K-algebra. If, in addition, E is a field, then E is a finite algebraic extension of K.*

Proof:
(We have to show that E does not contain transcendental elements.)
By assumption, we have $E = K[x_1, ..., x_n]$. In addition, E is supposed to be a field.
We have to options:

1. $x_1, ..., x_n$ are algebraic over K.

2. Not all of $x_1, ..., x_n$ are algebraic over K.

In the first case, we are done: $E = K[x_1, ..., x_n] = K(x_1, ..., x_n)$ is a finite algebraic extension of K.
In the second case, we will get a contradiction:
Assume: $x_1, ..., x_r$ (possibly after rearranging the elements) are algebraically independent over K, i.e. transendental over K, i.e. we can view $x_1, ..., x_r$ as r (independent) variables, and E is a finite algebraic extension over $K(x_1, ..., x_n)$.
Set $F = K(x_1, ..., x_r)$.
$\Rightarrow E$ is a finite dimensional F-vector-space.
$\Rightarrow E$ is a finitely generated F-module.
Now, we have the situation of Theorem 7: $A = K, B = F, C = E$, E is a finitely generated K-algebra, E is a finitely generated F-module. Hence, we can conclude that F is a finitely generated K-algebra, i.e. there are elements $y_1, ..., y_s \in F$ such that $F = K[y_1, ..., y_s]$.
In particular, we have $K(x_1, ..., x_r) \ni y_j = \frac{f_j}{g_j}$, where $f_j, g_j \in K[x_1, ..., x_r], j = 1, ..., s$.
Now, let h be an irreducible polynomial in $x_1, ..., x_r$, coprime to $g_1, ..., g_s$.
Since F is a field, $\frac{1}{h} \in F = K[y_1, ..., y_s]$ after substituting y_j by $\frac{f_j}{g_j}$, get $\frac{1}{h} = \frac{\mathcal{F}(x_1,...,x_r)}{g_1^{\alpha_1} \cdot ... \cdot g_s^{\alpha_s}} = \frac{\mathcal{G}(x_1,...,x_r)}{\mathcal{H}(x_1,...,x_r)}$, where $\mathcal{F}, \mathcal{G}, \mathcal{H} \in K[x_1, ..., x_r], (\mathcal{G}, \mathcal{H}) = 1$ and $\mathcal{H}$ is devided by irreducible polynomials dividing $g_1, ..., g_s$.
$\Rightarrow \mathcal{H} = \mathcal{G} \cdot h$
$\Rightarrow h | \mathcal{H}$
This is a contradiction by the choice of h (as an irreducible polynomial not matching one of the irreducible factors of the g_j's). □

2.2 Hilbert's Nullstellensatz

Theorem 2.6. ((1) Weak Nullstellensatz - algebraic version) *Let K be a field, A a finitely generated K-algebra and $\mathfrak{m} \in \mathrm{Max}(A)$.*
Then, the quotient ring $A/\mathfrak{m}$ is a finite algebraic extension of K. In particular, if K is algebraically closed, we have $A/\mathfrak{m} \cong K$.

Proof:
Let be $E = A/\mathfrak{m}$. Note that E is finitely generated K-algebra and a field. Applying Theorem 8, gives the desired result. □

Lecture on 2007-12-13

Theorem 2.7. ((2) Weak Nullstellensatz - geometric version) *Let K be an algebraically closed field, $f_j \in K[X_1, ..., X_n]$ $(j \in J, (\{f_j | j \in J\}) \neq K[X_1, ..., X_n])$, and X the affine algebraic variety defined by $f_j, j \in J$, i.e. $X = \{x = (x_1, ..., x_n) \in K^n | \forall j \in J : f_j(x_1, ..., x_n) = 0\}$.*
Then, we have $X \neq \emptyset$.

Proof:
Define $I(X) = \{g \in K[X_1, ..., X_n] | g(x_1, ..., x_n) = 0 \text{ for all } x = (x_1, ..., x_n) \in X\}$. One easily checks that $I(X) \subseteq K[X_1, ..., X_n]$ is an ideal.
(Note: Since $K[X_1, ..., X_n]$ is noetherian, $I(X)$ is finitely generated!)
Moreover, we note:

1. $\forall j \in J : f_j \in I(X)$
2. $g \in I(X), x = (x_1, ..., x_n) \in X$, then $\forall j = 1, ..., n : (X_j - x_j) | g$
   $\Rightarrow I(X) \subseteq (X_1 - x_1, X_2 - x_2, ..., X_n - x_n) \leftarrow$ maximal ideal

Furthermore, let $R(X) = K[X_1, ..., X_n]/I(X)$ denote the (affine) coordinate ring of X. We let $\pi : K[X_1, ..., X_n] \to R(n)$ be the natural projection. In particular, we put $\xi_j = \pi(X_j), j = 1, ..., n$.
We have, by assumption, $I(X) \subset K[X_1, ..., X_n]$.
$\Rightarrow R(X) \neq \{0\} \Rightarrow \mathrm{Max}(R(X)) \neq \emptyset$
The strategy of proof now consists in establishing a bijection $\varphi : X \to \mathrm{Max}(R(X))$. Once φ is constructed, we get $X \neq \emptyset$, since $Max(R(X)) \neq \emptyset$.

Construction of φ
Let $x = (x_1, ..., x_n) \in X$ be a point.
We define $ev_x : R(X) \to K$ by $h(\xi_1, ..., \xi_n) \mapsto h(x_1, ..., x_n)$
Note, that this map is well-defined, i.e. it is independend on the choice of representatives. Further, ev_x is surjective. Therefore, we have $R(X)/\ker(ev_x) \cong K$.
$\Rightarrow \mathfrak{m}_x = \ker(ev_x) \in \mathrm{Max}(R(X))$

Definition of φ
We define $\varphi : X \to \mathrm{Max}(R(X))$ by $x \mapsto \mathfrak{m}_x$. **Characterization of $\mathfrak{m}_x$**

Note: $(\xi_j - x_j) \in \mathfrak{m}_x$ $(x = (x_1, ..., x_n), j = 1, ..., n)$
$\Rightarrow (\xi_1 - x_1, ..., \xi_n - x_n) \subseteq \mathfrak{m}_x$
$\Rightarrow$ Since the former ideal is maximal, we get $\mathfrak{m}_x = (\xi_1 - x_1, ..., \xi_n - x_n)$.
(Note: $\pi^{-1}(\mathfrak{m}_x) = (X_1 - x_1, ..., X_n - x_n)$)

Injectivity of φ
Let $x = (x_1, ..., x_n) \in X$ and $x' = (x'_1, ..., x'_n) \in X$ such that $\mathfrak{m}_x = \varphi(x) = \varphi(x') = \mathfrak{m}_{x'}$. By pull-back via π, we find by the previous characterization $(X_1 - x_1, ..., X_n - x_n) = (X_1 - x'_1, ..., X_n - x'_n)$.
$\Rightarrow X_j - x_j = \sum_{k=1}^{n} g_k(X_1, ..., X_n) \cdot (X_k - x'_k)$ with $g_k \in K[X_1, ..., X_n]$.
By degree reason's and the independence of $X_1, ..., X_n$, we have $g_j = 1$ and $g_k = 0$ for all $k \neq j$.
$\Rightarrow X_j - x_j = X_j - x'_j \Rightarrow x'_j = x_j \Rightarrow x = x'$

Surjectivity of φ
Let be $\mathfrak{m} \in \text{Max}(R(X))$.
Claim: $\exists x = (x_1, ..., x_n) \in X : \varphi(x) = \mathfrak{m}$
Note: $R(X)$ is a finitely generated K-algebra, with generators $\xi_1, ..., \xi_n$.
$\Rightarrow R(X)/\mathfrak{m}$ is also a finitely generated K-algebra with generators $\xi_1 + \mathfrak{m}, ..., \xi_n + \mathfrak{m}$. In addition, it is a field (since $\mathfrak{m}$ is maximal). By theorem 1, we get $R(X)/\mathfrak{m} \cong K$ by $\xi_j + \mathfrak{m} \leftrightarrow x_j$.
Claim:

1. $x = (x_1, ..., x_n) \in X$
2. $\varphi(x) = \ker(ev_x) = \mathfrak{m}$ $(\Leftrightarrow \mathfrak{m}_x = \mathfrak{m})$

Ad 2) (Eventually, after identifying $R/\mathfrak{m}$ with K), we have $\xi_j + \mathfrak{m} = x_j$, i.e. $\xi_j - x_j \in \mathfrak{m}$.
$\Rightarrow (\xi_1 - x_1, ..., \xi_n - x_n) = \mathfrak{m}$.
Ad 1) We have $f_j \in I(X) \subseteq (X_1 - x_1, ..., X_n - x_n)$.
$\Rightarrow f_j(X_1, ..., X_n) = \sum_{k=1}^{n} g_{k,j}(X_1, ..., X_n)(X_j - x_j)$
$\Rightarrow \forall j \in J : f_j(x_1, ..., x_n) = 0$
$\Rightarrow x = (x_1, ..., x_n) \in X$ □

Remark
Let $n = |J| = 1$. Then $X = \{x_1 \in K | f_1(x_1) = 0\}$ where $f_1 \in K[X_1]$, non-constant. We have $X \neq \emptyset$, since K is algebraically closed.

Remark
Consider $X \subseteq K^n$, as above, with coordinate ring $R(X)$. Then, we have the bijection
$X \xrightarrow{\approx} \text{Max}(R(X)) \subseteq \text{Spec}(R(X))$ with $x(x_1, ..., x_n) \mapsto (\xi_1 - x_1, ..., \xi_n - x_n)$.
Using Zariski topology, X can made into topological space. One the other hand, $\text{Spec}(R(X))$ is also a topological space with basis of open sets $D(h)$, $h \in R(X)$ ($D(h) = \text{Spec}(R(X)) \setminus V(h)$, where $V(h)$ is defined by $V(h) = \{\mathfrak{p} \in \text{Spec}(R(X)) | h \in \mathfrak{p}\}$).
Then, we have $V(h)|_{\text{Max}(R(X))} = \{\mathfrak{m} \in \text{Max}(R(X)) | h \in \mathfrak{m}\}$.
In this way, X and $\text{Max}(R(X))$ become homeomorphic topological spaces. Furthermore, X can be viewed as a topological subspace of $\text{Spec}(R(X))$.

Example
$X = K^n \Rightarrow I(X) = (0)$
$\Rightarrow R(X) = K[X_1, ..., X_n]$
$\Rightarrow \text{Max}(R(X)) = \text{Spec}(R(X)) \setminus \{0\}$, since $R(X)$ is factorial.
$\Rightarrow K^n \approx \text{Max}(K[X_1, ..., X_n])$, by $(x_1, ..., x_n) \leftrightarrow (X_1 - x_1, ..., X_n - x_n)$
$\overline{\{(0)\}} = \text{Spec}(K[X_1, ..., X_n])$
(0) is called the generic point of $\text{Spec}(K[X_1, ..., X_n])$.

Theorem 2.8. ((3) Strong Nullstellensatz - geometric version) *Let K be an algebraically closed field, $\mathfrak{a} \subset K[X_1, ..., X_n]$ an ideal and X the affine algebraic variety defined by $\mathfrak{a}$, i.e.*

$$X = V(\mathfrak{a}) = \{x = (x_1, ..., x_n) \in K^n | \forall f \in \mathfrak{a} : f(x_1, ..., x_n) = 0\}$$

Furthermore, let $I(X) = \{g \in K[X_1, ..., X_n] | \forall x \in X : g(x) = 0\}$.
Then, we have $I(X) = \mathfrak{r}(\mathfrak{a})$.

Proof:
We have already observed: $\mathfrak{a} \subseteq I(X)$.
$g \in \mathfrak{r}(\mathfrak{a}) \Rightarrow \exists n \in \mathbb{N} : g^n \in \mathfrak{a} \Rightarrow \forall x \in X : g^n(x_1, ..., x_n) = 0 \Rightarrow \forall x \in X : g(x_1, ..., x_n) = 0$
This immediately shows also $\mathfrak{r}(\mathfrak{a}) \subseteq I(X)$.
It remains to show the opposite inclusion or, equivalently, the implication $f \notin \mathfrak{r}(\mathfrak{a}) \Rightarrow f \notin I(X)$.
So let be $f \notin \mathfrak{r}(\mathfrak{a})$.
Recall: $\mathfrak{r}(\mathfrak{a}) = \bigcup_{\mathfrak{p} \in \text{Spec}(A), \mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}$, where $A = K[X_1, ..., X_n]$.

Since $f \notin \mathfrak{r}(\mathfrak{a})$, hence $\exists \mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \subseteq \mathfrak{a}$ but $f \notin \mathfrak{p}$.
Define: $A = K[X_1, ..., X_n]$ and $B = A/\mathfrak{p}$, with $\overline{f} = f + \mathfrak{p}$ for $f \in A$. Furthermore let be $C = B_{\overline{f}} = B[1/\overline{f}]$ (localization of B at $S = \{1, \overline{f}, \overline{f}^2, ...\}$).
C is a finitely generated K-algebra (namely generated by $\overline{X}_1, ..., \overline{X}_n$ and $1/\overline{f}$).
Let be $\mathfrak{m} \in \mathrm{Max}(C)$. By Theorem 1, we have $C/\mathfrak{m} = K$.
Summarizing, we get:

$$\begin{array}{ccccccc} A & \to & B = A/\mathfrak{p} & \to & C = B_{\overline{f}} & \to & K = C/\mathfrak{m} \\ g & \mapsto & \overline{g} = g + \mathfrak{p} & \mapsto & \frac{\overline{g}}{1} & \mapsto & \overline{\overline{g}} = \frac{\overline{g}}{1} + \mathfrak{m} \\ x_j & \mapsto & \overline{x_j} & \mapsto & \frac{x_j}{1} & \mapsto & \overline{\overline{x}}_j \end{array}$$

We still want to show $\mathfrak{r}(\mathfrak{a}) \supseteq I(X)$. This is equivalent to $f \notin \mathfrak{r}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \subseteq \mathfrak{a}} \mathfrak{p} \Rightarrow f \notin I(X)$.
Put $x_j = \overline{\overline{x}}_j \in K, j = 1, ..., n$.

Claim:

1. $x = (x_1, ..., x_n) \in X$
2. $f(x) \neq 0$
3. (1.)&(2.) $\Rightarrow f \notin I(X)$

Ad 1.) Let $h \in \mathfrak{a}$, arbitrary.
Note: $\mathfrak{a} \subseteq \mathfrak{p}$
$\Rightarrow \overline{h}(X_1, ..., X_n) = h(\overline{X}_1, ..., \overline{X}_n) = 0$ in B
$\Rightarrow \overline{\overline{h}}(X_1, ..., X_n) = h(\overline{\overline{X}}_1, ..., \overline{\overline{X}}_n) = 0$ in K
$\Rightarrow x = (x_1, ..., x_n) \in X$

Ad 2.) Since $f \notin \mathfrak{p}$ we have $\overline{f}(X_1, ..., X_n) = f(\overline{X}_1, ..., \overline{X}_n) \neq 0$.
This was important to localize at $\overline{f}$!
$\Rightarrow \frac{\overline{f}}{1} \in C$ is a unit. $\Rightarrow \frac{\overline{f}}{1} \notin \mathfrak{m}$
$\Rightarrow \overline{\overline{f}}(X_1, ..., X_n) = f(\overline{\overline{X}}_1, ..., \overline{\overline{X}}_n) \neq 0$ in K
$\Rightarrow I(X) \supseteq \mathfrak{r}(\mathfrak{a})$
$\Rightarrow I(X) = \mathfrak{r}(\mathfrak{a})$ □

Remark

1. We have $I(V(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$. In particular, for a prime ideal $\mathfrak{p}$: $I(V(\mathfrak{p})) = \mathfrak{p}$.
2. Since $\mathfrak{a} \subset K[X_1, ..., X_n]$, we have $I(X) = \mathfrak{r}(\mathfrak{a}) \subset K[X_1, ..., X_n]$.
3. Note that - by Hilbert's basis theorem - $\mathfrak{a}$ is finitely generated, so finitely many polynomials define $X = V(\mathfrak{a})$.

Chapter 3

Primary decompositions

3.1 Basics

Let A be a commutative ring with 1.

Definition (Primary ideal)
An ideal $\mathfrak{q} \subset A$ is called *primary* if $x \cdot y \in \mathfrak{q}$ implies $x \in \mathfrak{q}$ or $\exists n \in \mathbb{N} : y^n \in \mathfrak{q}$.

Example
If $\mathfrak{p} \in \mathrm{Spec}(A)$, then $\mathfrak{p}$ is a primary ideal.

Equivalent definition
An ideal $\mathfrak{q} \subset A$ is primary, iff every zero divisor in $A/\mathfrak{q}$ is nilpotent:
$\overline{x} \cdot \overline{y} = \overline{0} \Rightarrow x \cdot y \in \mathfrak{q} \Rightarrow x \in \mathfrak{q}$ or $y^n \in \mathfrak{q} \Rightarrow \overline{x} = 0$ or $\overline{y}^n = 0$

Example

1. The primary ideals of $A = \mathbb{Z}$ are given by (0) and $(p^n), n \in \mathbb{N}_{>0}, p \in \mathbb{P}$.
2. In general, powers of prime ideals (i.e. ideals of the form $\mathfrak{p}^n$, $n \in \mathbb{N}_{>0}, \mathfrak{p} \in \mathrm{Spec}(A)$) are *not* primary.

Lemma 3.1. (1) *Let $\mathfrak{q} \subset A$ be a primary ideal. Then, the radical $\mathfrak{r}(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.*

Proof:
Let's first show that $\mathfrak{r}(\mathfrak{q})$ is a prime ideal. For this, let $x \cdot y \in \mathfrak{r}(\mathfrak{q})$ and show $x \in \mathfrak{r}(\mathfrak{q})$ or $y \in \mathfrak{r}(\mathfrak{q})$.
$x \cdot y \in \mathfrak{r}(\mathfrak{q}) \Rightarrow \exists n \in \mathbb{N}_{>0} : x^n \cdot y^n = (x \cdot y)^n \in \mathfrak{q}$
Since $\mathfrak{q}$ is a primary ideal, we have $x^n \in \mathfrak{q}$ or $\exists m \in \mathbb{N}_{>0} : y^{n \cdot m} = (y^n)^m \in \mathfrak{q}$. $\Rightarrow x \in \mathfrak{r}(\mathfrak{q})$ or $y \in \mathfrak{r}(\mathfrak{q})$
$\Rightarrow \mathfrak{r}(\mathfrak{q}) \in \mathrm{Spec}(A)$
Let's now prove minimality:
By known results from section 1, we have $\mathfrak{r}(\mathfrak{q}) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \supseteq \mathfrak{q}} \mathfrak{p}$.
We have $\mathfrak{r}(\mathfrak{q}) \in \mathrm{Spec}(A), \mathfrak{r}(\mathfrak{q}) \supseteq \mathfrak{q}$. Additionally, $\bigcap_{\mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \supseteq \mathfrak{q}} \mathfrak{p}$ is the minimal ideal containing $\mathfrak{q}$. Taken this together, yields the minimality statement. □

Definition ($\mathfrak{p}$-primary ideal)
Let $\mathfrak{q} \subset A$ be a primary ideal with $\mathfrak{r}(\mathfrak{q}) = \mathfrak{p} \in \mathrm{Spec}(A)$.
Then, we call $\mathfrak{q}$ $\mathfrak{p}$-*primary*.

Lemma 3.2. (2)

1. *Let $\mathfrak{a} \subseteq A$ be an ideal such that the radical $\mathfrak{r}(\mathfrak{a})$ is maximal. Then $\mathfrak{a}$ is primary.*
2. *In particular, the powers $\mathfrak{m}^n, n \in \mathbb{N}_{>0}$ of a maximal ideal $\mathfrak{m}$ are primary, in fact $\mathfrak{m}$-primary.*

Proof:

1. Let $\pi : A \to A/\mathfrak{a}$ denote the canonical ring homomorphism.
   Further, let be $\mathfrak{m} = \mathfrak{r}(\mathfrak{a}) \in \mathrm{Max}(A)$.
   Recall: $\pi^{-1}(\mathfrak{n}_{A/\mathfrak{a}}) = \mathfrak{r}(\mathfrak{a}) = \mathfrak{m}$, $\overline{\mathfrak{m}} = \pi(\mathfrak{m}) = \mathfrak{n}_{A/\mathfrak{a}} = \bigcap_{\overline{\mathfrak{p}} \in \mathrm{Spec}(A/\mathfrak{a})} \overline{\mathfrak{p}}$
   Claim: $\mathrm{Spec}(A/\mathfrak{a}) = \{\overline{\mathfrak{m}}\}$
   Let be $\overline{\mathfrak{p}} \in \mathrm{Spec}(A/\mathfrak{a})$ be any prime ideal. We want to show $\overline{\mathfrak{p}} = \overline{\mathfrak{m}}$.
   $\exists \mathfrak{p} \in \mathrm{Spec}(A) : \pi(\mathfrak{p}) = \overline{\mathfrak{p}}$ (We just take $\mathfrak{p} = \pi^{-1}(\overline{\mathfrak{p}})$.)
   Since $\pi(\mathfrak{a}) = \{0\} \subseteq \overline{\mathfrak{p}}$, we get $\mathfrak{p} \supseteq \mathfrak{a}$. Taking radicals yields $\mathfrak{p} = \mathfrak{r}(\mathfrak{p}) \supseteq \mathfrak{r}(\mathfrak{a}) = \mathfrak{m}$.
   By maximality of $\mathfrak{m}$ we get $\mathfrak{p} = \mathfrak{m}$.
   $\Rightarrow \overline{\mathfrak{p}} = \pi(\mathfrak{p}) = \pi(\mathfrak{m}) = \overline{\mathfrak{m}}$
   Consider now an element $\overline{a} \in A/\mathfrak{a}$. Then $\overline{a} \in \overline{\mathfrak{m}}$ or $\overline{a} \notin \overline{\mathfrak{m}}$.
   In the first case, we get $\overline{a} \in \mathfrak{n}_{A/a} \Rightarrow \overline{a}$ is nilpotent.
   In the second case, we have $\overline{a} \in (A/\mathfrak{a})^\times$, i.e. $\overline{a}$ is a unit.
   Let now $\overline{a} \in A/\mathfrak{a}$ a zero divisor, then $\overline{a} \notin (A/\mathfrak{a})^\times$. By the previous consideration $\overline{a}$ has to be nilpotent.
   $\Rightarrow \mathfrak{a}$ is primary.
2. Let $\mathfrak{a} = \mathfrak{m}^n$, $\mathfrak{m} \in \mathrm{Max}(A)$ and $n \in \mathbb{N}_{>0}$.
   $\Rightarrow \mathfrak{r}(\mathfrak{a}) = \mathfrak{r}(\mathfrak{m}^n) = \mathfrak{m} \in \mathrm{Max}(A)$
   By the first part, $\mathfrak{m}^n$ is primary. Since $\mathfrak{r}(\mathfrak{m}^n) = \mathfrak{m}$, it is $\mathfrak{m}$-primary. □

Lecture on 2007-12-20

Lemma 3.3. (3) *Let $\mathfrak{q}_1, ..., \mathfrak{q}_n$ be $\mathfrak{p}$-primary ideals of A.*
Then the intersection $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is also $\mathfrak{p}$-primary.

Proof:
Let $x \cdot y \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. We have to show that $y^n \in \mathfrak{q}$ for some $\mathfrak{n} \in \mathbb{N}_{>0}$ (or equivalently $y \in \mathfrak{r}(\mathfrak{q})$).
By the assumption, $x \notin \mathfrak{q}$, we find an index $i \in \{1, ..., n\}$ such that $x \notin \mathfrak{q}_i$. But, of course, $x \cdot y \in \mathfrak{q}_i$ for all $i \in \{1, ..., n\}$.
Since q_i is primary, there is $n_i \in \mathbb{N}_{>0} : y^{n_i} \in \mathfrak{q}_i$, i.e. $y \in \mathfrak{r}(\mathfrak{q}_i) = \mathfrak{p}$.
Using the properties of the radical, we compute $\mathfrak{r}(\mathfrak{q}) = \mathfrak{r}(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n \underbrace{\mathfrak{r}(\mathfrak{q}_i)}_{=\mathfrak{p}} = \mathfrak{p}$ (*).
All in all: $y \in \mathfrak{r}(\mathfrak{q})$, as wanted.
$\Rightarrow \mathfrak{q}$ is primary.
By the computation (*), we conclude in fact that $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary. □

Lemma 3.4. (4) *Let $x \in A$ and $\mathfrak{q} \subset A$ a $\mathfrak{p}$-primary ideal. Then, we have*

1. *If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = A$.*
   Remember: $(\mathfrak{a} : \mathfrak{b}) = \{x \in A | x \cdot \mathfrak{b} \subseteq \mathfrak{a}\}$. We define $(\mathfrak{a} : y) = (\mathfrak{a} : (y))$ for the principal ideal (y).
2. *If $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.*
3. *If $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.*

Proof:

1. Using the definition of the ideal quotient, we have

   $(\mathfrak{q} : x) = \{y \in A | x \cdot y \cdot A \subseteq \mathfrak{q}\} = \{y \in A | x \cdot y \cdot 1 \in \mathfrak{q}\} = \{y \in A | x \cdot y \in \mathfrak{q}\} \overset{x \in \mathfrak{q}}{=} A$

2. We define $\mathfrak{r}(\mathfrak{q} : x) = \mathfrak{r}((\mathfrak{q} : x))$. Let's now compute $\mathfrak{r}(\mathfrak{q} : x)$. Starting with $y \in (\mathfrak{q} : x)$, we get $x \cdot y \in \mathfrak{q}$. By assumption $x \notin \mathfrak{q}$, hence $y \in \mathfrak{r}(\mathfrak{q}) = \mathfrak{p}$.

   $\left.\begin{array}{l} \Rightarrow (\mathfrak{q} : x) \subseteq \mathfrak{p} \\ \text{Note} : \mathfrak{q} \subseteq (\mathfrak{q} : x) \end{array}\right\} \Rightarrow \mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$

   Taking radicals yields $\mathfrak{p} = \mathfrak{r}(\mathfrak{q}) \subseteq \mathfrak{r}(\mathfrak{q} : x) \subseteq \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$, i.e. $\Rightarrow \mathfrak{r}(\mathfrak{q} : x) = \mathfrak{p}$.

   Let now be $y \cdot z \in (\mathfrak{q} : x)$ and assume $z \notin \mathfrak{r}(\mathfrak{q} : x) = \mathfrak{p}$. We want to show $y \in (\mathfrak{q} : x)$.

   We have $(x \cdot y) \cdot z = x \cdot (y \cdot z) \in \mathfrak{q}$, but $z \notin \mathfrak{p} = \mathfrak{r}(\mathfrak{q})$.

   Since $\mathfrak{q}$ is primary, $x \cdot y \in \mathfrak{q} \Rightarrow y \in (\mathfrak{q} : x)$.

   $\Rightarrow (\mathfrak{q} : x)$ is primary and, using $\mathfrak{r}(\mathfrak{q} : x) = \mathfrak{p}$, in fact $\mathfrak{p}$-primary.

3. We have that $\mathfrak{q}$ is $\mathfrak{p}$-primary and $x \notin \mathfrak{p}$. We want to show $(\mathfrak{q} : x) = \mathfrak{q}$.

   We already know $\mathfrak{q} \subseteq (\mathfrak{q} : x)$, i.e. we have to show $(\mathfrak{q} : x) \subseteq \mathfrak{q}$.

   Let be $y \in (\mathfrak{q} : x)$, i.e. $x \cdot y \in \mathfrak{q}$.

   $\Rightarrow y \cdot x \in \mathfrak{q}$

   Note that, by assumption, $x \notin \mathfrak{p} = \mathfrak{r}(q)$, i.e. $y \in \mathfrak{q}$.

   $\Rightarrow (\mathfrak{q} : x) \subseteq \mathfrak{q}$

   $\Rightarrow \mathfrak{q} = (\mathfrak{q} : x)$ □

3.2 Uniqueness of a primary decomposition

Definition (primary decomposition)
Let $\mathfrak{a} \subseteq A$ be an ideal. A *primary decomposition* of $\mathfrak{a}$ is given by a *finite* intersection $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ of primary ideals $\mathfrak{q}_1, ..., \mathfrak{q}_n$.
The decomposition is called *minimal* iff the following two conditions are satisfied:

1. All radicals $\mathfrak{r}(\mathfrak{q}_i), i = 1, ..., n$ are pairwise different.
2. For $i = 1, ..., n$ we have $\mathfrak{q}_i \not\supseteq \bigcap_{j=1, j \neq i}^{n} \mathfrak{q}_j$.

Remark
Note that, using Lemma 3, a given primary decomposition can be reduced to a minimal primary decomposition.

Definition
An ideal $\mathfrak{a} \subseteq A$ is called *decomposable*, iff it has a primary decomposition.

Remark
Note, in an arbitrary commutative ring A (with 1), an ideal needs not to be decomposable.

Lemma 3.5. *Let $\mathfrak{a}_1, ..., \mathfrak{a}_n \subseteq A$ be ideals and $\mathfrak{p} \in \mathrm{Spec}(A)$ a prime ideal satisfying $\mathfrak{p} \supseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$. Then, there is $i \in \{1, ..., n\}$ such that $\mathfrak{p} \subseteq \mathfrak{a}_i$.*
Moreover, if $\mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, then there is $i \in \{1, ..., n\}$ such that $\mathfrak{p} = \mathfrak{a}_i$.

Proof:
Argue by contradiction: Assume $\mathfrak{p} \not\subseteq \mathfrak{a}_i$ for all $i = 1, ..., n$.
$\Rightarrow \exists x_i \in \mathfrak{a}_i, x_i \notin \mathfrak{p}, i = 1, ..., n$
$\Rightarrow \prod_{i=1}^n x_i \in \prod_{i=1}^n \mathfrak{a}_i \subseteq \bigcap_{i=1}^n \mathfrak{a}_i$, but $\prod_{i=1}^n x_i \notin \mathfrak{p}$ (since $\mathfrak{p}$ is prime)
$\Rightarrow \mathfrak{p} \not\supseteq \bigcap_{i=1}^n \mathfrak{a}_i$ contradiction

Second part:
Assume: $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$

1. $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i \overset{1.}{\Rightarrow} \exists i \in \{1, ..., n\} : \mathfrak{p} \supseteq \mathfrak{a}_i$
2. $\mathfrak{p} \subseteq \bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{a}_i$ for all $i = 1, ..., n$.

$\Rightarrow \exists i \in \{1, ..., n\} : \mathfrak{p} = \mathfrak{a}_i$ □

Theorem 3.1. ((1) First uniqueness theorem) *Let $\mathfrak{a} \subseteq A$ be a decomposable ideal and let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition. Further, let $\mathfrak{p}_i = \mathfrak{r}(\mathfrak{q}_i), i = 1, ..., n$.*
Then, the $\mathfrak{p}_i$'s are precisely the prime ideals in the set of ideals $\mathfrak{r}(\mathfrak{a} : x)$ with $x \in A$, i.e. we have $\{\mathfrak{r}(\mathfrak{a} : x) | x \in A\} \cap \mathrm{Spec}(A) = \{p_1, ..., p_n\}$. Therefore, the prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are independent on the specific (minimal) primary decomposition of $\mathfrak{a}$.

Proof:
Using the properties of ideal quotients, we compute for any $x \in A$:
$(\mathfrak{a} : x) = (\bigcap_{i=1}^n \mathfrak{q}_i : x) = \bigcap_{i=1}^n (\mathfrak{q}_i : x)$
Taking radicals, we arrive at $\mathfrak{r}(\mathfrak{a} : x) = \mathfrak{r}\left(\bigcap_{i=1}^n (\mathfrak{q}_i : x)\right) = \bigcap_{i=1}^n \mathfrak{r}(\mathfrak{q}_i : x)$.
Now, recall Lemma 4:

1. $x \in \mathfrak{q}_i \Rightarrow (\mathfrak{q}_i : x) = A \Rightarrow \mathfrak{r}(\mathfrak{q}_i : x) = A$
   Therefore, $x \in \mathfrak{q}_i$ does not contribute to the intersection $\bigcap_{i=1}^n \mathfrak{r}(\mathfrak{q}_i : x)$.
2. $x \notin \mathfrak{q}_i \Rightarrow \mathfrak{r}(\mathfrak{q}_i : x) = \mathfrak{p}_i$

$\Rightarrow \mathfrak{r}(\mathfrak{a} : x) = \bigcap_{j=1, x \notin \mathfrak{q}_j}^n \mathfrak{p}_j$
Now, we show $\{\mathfrak{r}(\mathfrak{a} : x) | x \in A\} \cap \mathrm{Spec}(A) \subseteq \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$.
We have

1. $\mathfrak{r}(\mathfrak{a} : x)$ is prime ideal.
2. $\mathfrak{r}(\mathfrak{a} : x) = \bigcap_{j : x \notin \mathfrak{q}_j} \mathfrak{p}_j$

By the previous lemma, there is $j \in \{1, ..., n\}, x \notin \mathfrak{q}_j$ such that $\mathfrak{r}(\mathfrak{a} : x) = \mathfrak{p}_j$.
Next, we show the inclusion $\{p_1, ..., p_n\} \subseteq \{\mathfrak{r}(\mathfrak{a} : x) | x \in A\} \cap \mathrm{Spec}(A)$. Given $\mathfrak{p}_i$ we construct $x_i \in A$ such that $\mathfrak{p}_i = \mathfrak{r}(\mathfrak{a} : x_i) \in \mathrm{Spec}(A)$.
By minimality of the decomposition of $\mathfrak{a}$, we have $\mathfrak{q}_i \not\supseteq \bigcap_{j=1, j \neq i}^n \mathfrak{q}_j$.
$\Rightarrow \exists x_i \in \left(\bigcap_{j=1, j \neq i}^n \mathfrak{q}_j\right) \setminus \mathfrak{q}_i$
$\Rightarrow \mathfrak{r}(\mathfrak{a} : x_i) = \bigcap_{i=1}^n \mathfrak{r}(\mathfrak{q}_j : x_i) = \mathfrak{r}(\mathfrak{q}_i : x_i) \cap \bigcap_{j=1, j \neq i}^n \mathfrak{r}(\mathfrak{q}_j : x_i) \overset{Lemma\ 4}{=} \mathfrak{p}_i \cap \bigcap_{j=1, j \neq i}^n A = \mathfrak{p}_i$ □

Lecture on 2008-01-10

Remark
Let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ a minimal primary decomposition with $\mathfrak{q}_i$ being $\mathfrak{p}_i$-primary $(i = 1, ..., n)$. Choose $x_i \notin \mathfrak{p}_i, x_i \in \bigcap_{i=1, j \neq i}^n \mathfrak{q}_j$.
$\Rightarrow \mathfrak{r}(\mathfrak{a} : x_j) = \mathfrak{r}(\bigcap_{i=1}^n \mathfrak{q}_i : x_j) = \bigcap_{i=1}^n \mathfrak{r}(\mathfrak{q}_i : x_j) = \mathfrak{q}_j$

Definition
Let $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition with $\mathfrak{q}_i$ being $\mathfrak{p}_i$-primary $(i = 1, ..., n)$.

1. The prime ideals $\mathfrak{p}_i$ are called *associated* to the ideal $\mathfrak{a}$.
2. The minimal elements of $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ are called *minimal* or *isolated* ideals associated to $\mathfrak{q}$.
3. The non-minimal elements of $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ are called *embedded* prime ideals (associated to $\mathfrak{a}$).

Remark
In the first uniqueness theorem, the prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are associated primes of $\mathfrak{a}$.

Aim: Second uniqueness theorem
Let be $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ a (minimal) primary decomposition, where the $\mathfrak{q}_i$ are $\mathfrak{p}_i$-primary.
Then, $\mathfrak{q}_i$ is uniquely determined, if $\mathfrak{p}_i$ is minimal.

Proposition 3.1. (2) *Let $\mathfrak{a}$ be decomposable with minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ (all $\mathfrak{q}_i$ are $\mathfrak{p}_i$-primary).*
Then, we have $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\} = \{\mathfrak{p} \in \mathrm{Spec}(A) | \mathfrak{p} \supseteq \mathfrak{a}, \mathfrak{p} \text{ minimal}\}$.

Proof:
By lemma 1 from section 1 the inclusion $\subseteq$ is clear ($\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i \subseteq \mathfrak{q}_i \subseteq \mathfrak{p}_i$).
So, let's prove the inclusion $\supseteq$.
Let be $\mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \supseteq \mathfrak{a}$ minimal.
$\Rightarrow \mathfrak{p} = \mathfrak{r}(\mathfrak{p}) \supseteq \mathfrak{r}(\mathfrak{a}) = \mathfrak{r}(\bigcap_{i=1}^{n} \mathfrak{q}_i) = \bigcap_{i=1}^{n} \mathfrak{r}(\mathfrak{q}_i) = \bigcap_{i=1}^{n} \mathfrak{p}_i$
$\overset{(*)}{\Rightarrow} \exists i \in \{1, ..., n\} : \mathfrak{p} \supseteq \mathfrak{p}_i$
Proof of $(*)$: Assuming $\mathfrak{p} \not\supseteq \mathfrak{p}_i$ for all i, we get $\exists x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$.
$\Rightarrow \prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} \mathfrak{p}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{p}_i$, but $\prod_{i=1}^{n} x_i \notin \mathfrak{p}$ (since $\mathfrak{p}$ is a prime ideal).
This is a contradiction to $\mathfrak{p} \supseteq \bigcap_{i=1}^{n} \mathfrak{p}_i$.
$\Rightarrow \mathfrak{p} \subseteq \mathfrak{a}$ is minimal and contains a minimal prime ideal $\mathfrak{p}_i$ associated to $\mathfrak{a}$.
$\Rightarrow \exists i : \mathfrak{p} = \mathfrak{p}_i$ □

Proposition 3.2. (3) *Let $\mathfrak{a}$ be a decomposible ideal with primary decomposition $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ ($\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary).*
Then, $\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A | (\mathfrak{a} : x) \neq \mathfrak{a}\}$.
In particular, if $\mathfrak{a} = (0)$, then the set of zero divisors $D = \{x \in A | (0 : x) \neq (0)\}$ of A equals the union of the prime ideals, associated to $\mathfrak{a} = (0)$. (We have $(0 : x) = \{0 \neq y \in A | x \cdot y = 0\}$.)

Proof:

1. Reduction to the case $\mathfrak{a} = (0)$.
   Consider $\pi : A \to A/\mathfrak{a}$ with $\overline{\mathfrak{a}} = \pi(\mathfrak{a})$ and $\overline{\mathfrak{q}_i} = \pi(\mathfrak{q}_i)$.
   Starting with $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ and applying π yields

$$(\overline{0}) = \overline{\mathfrak{a}} = \pi(\mathfrak{a}) = \pi(\bigcap_{i=1}^{n} \mathfrak{q}_i) = \bigcap_{i=1}^{n} \pi(\mathfrak{q}_i) = \bigcap_{i=1}^{n} \overline{\mathfrak{q}_i}$$

   Claim: The ideals $\overline{\mathfrak{q}_i}$ are primary.
   Let be $\overline{x} \cdot \overline{y} \in \overline{\mathfrak{q}_i}, \overline{x} = x + \mathfrak{a}, \overline{y} = y + \mathfrak{a}$. Then, we get $x \cdot y \in \mathfrak{q}_i + \mathfrak{a}$. Since $\mathfrak{a} \subseteq \mathfrak{q}_i$, we get $x \cdot y \in \mathfrak{q}_i$.
   $\Rightarrow x \in \mathfrak{q}_i$ or $y^n \in \mathfrak{q}_i, n \in \mathbb{N}_{>0}$
   $\Rightarrow \overline{x} \in \overline{\mathfrak{q}_i}$ or $\overline{y}^n \in \overline{\mathfrak{q}_i}, n \in \mathbb{N}_{>0}$
   $\Rightarrow (\overline{0}) = \bigcap_{i=1}^{n} \overline{\mathfrak{q}_i}$ is a primary decomposition of $(\overline{0})$.
   Now, it's left to show that

$$\bigcup_{i=1}^{n} \overline{\mathfrak{p}_i} = \{\overline{x} \in A/\mathfrak{a} | (\overline{0} : \overline{x}) \neq (\overline{0})\} \Rightarrow \bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A | (\mathfrak{a} : x) \neq \mathfrak{a}\}$$

So, let be $\bigcup_{i=1}^{n} \overline{\mathfrak{p}_i} = \{\overline{x} \in A/\mathfrak{a} | (\overline{0} : \overline{x}) \neq (\overline{0})\}$.

(a) $\bigcup_{i=1}^{n} \mathfrak{p}_i \supseteq \{x \in A | (\mathfrak{a} : x) \neq \mathfrak{a}\}$
Let be $y \in \{x \in A | (\mathfrak{a} : x) \neq \mathfrak{a}\}$, i.e. $(\mathfrak{a} : y) \neq \mathfrak{a}$.
$\Rightarrow (\overline{0} : \overline{y}) \neq \overline{0}$
$\Rightarrow \overline{y} \in \bigcup_{i=1}^{n} \overline{\mathfrak{p}_i}$
$\Rightarrow y \in \pi^{-1}(\bigcup_{i=1}^{n} \overline{\mathfrak{p}_i}) = \bigcup_{i=1}^{n} \mathfrak{p}_i$

(b) $\bigcup_{i=1}^{n} \mathfrak{p}_i \subseteq \{x \in A | (\mathfrak{a} : x) \neq \mathfrak{a}\}$
This inclusion can be shown analogously.

2. W.l.o.g. we assume that $\mathfrak{a} = (0)$.
Claim: $\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A | (0 : x) \neq (0)\} = D$

(a) $D \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$
Recall: $D = \bigcup_{x \in A, x \neq 0} \mathrm{Ann}(x) = \bigcup_{x \in A, x \neq 0} (0 : x)$
Taking radicals gives

$$D = \mathfrak{r}(D) = \mathfrak{r}(\bigcup_{x \in A, x \neq 0} \mathrm{Ann}(x)) = \bigcup_{0 \neq x \in A} r(\mathrm{Ann}(x)) = \bigcup_{0 \neq x \in A} \mathfrak{r}(0 : x)$$

We recall from the proof of theorem 1 (First uniqueness theorem) $\mathfrak{r}(0 : x) = \bigcap_{j=1, x \notin \mathfrak{p}_j}^{n} \mathfrak{p}_j$.
$\Rightarrow \exists j \in \{1, ..., n\} : \mathfrak{r}(0 : x) \subseteq \mathfrak{p}_j$, since $x \notin \mathfrak{p}_j$.
$\Rightarrow D = \bigcup_{0 \neq x \in A} \mathfrak{r}(0 : x) \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$

(b) $D \supseteq \bigcup_{j=1}^{n} \mathfrak{p}_j$
From theorem 1, we know $\exists 0 \neq x_i \in A : \mathfrak{p}_i = \mathfrak{r}(0 : x_i)$.
$\Rightarrow \bigcup_{i=1}^{n} \mathfrak{p}_i = \bigcup_{i=1}^{n} \mathfrak{r}(0 : x_i) \subseteq \bigcup_{0 \neq x \in A} \mathfrak{r}(0 : x) = D$. □

Definition (extension ideal, contraction ideal)
Let A, B be commutative rings with 1, $f : A \to B$ a ring homomorphism and $\mathfrak{a} \subseteq A, \mathfrak{b} \subseteq B$ ideals. The *extension ideal* $\mathfrak{a}^e \subseteq B$ of $\mathfrak{a} \subseteq A$ is the ideal

$$\mathfrak{a}^e = \langle f(a) | a \in \mathfrak{a} \rangle = \{\sum_{i}^{n} b_i f(a_i) | b_i \in B, a_i \in \mathfrak{a}, n \in \mathbb{N}\}$$

The *contraction ideal* $\mathfrak{b}^c \subseteq A$ of $\mathfrak{b} \subseteq B$ is the ideal $\mathfrak{b}^c = f^{-1}(\mathfrak{b})$.

Remark
We have $(\mathfrak{a}^e)^c \supseteq \mathfrak{a}$.

Proposition 3.3. (4) *Let A be a commutative ring with 1, $S \subseteq A$ be a multiplicatively closed subset, $B = S^{-1}A$ the localization of A at S, $f : A \to B$ given by $a \mapsto \frac{a}{1}$ and $\mathfrak{q} \subset A$ a $\mathfrak{p}$-primary ideal.*
Then, we have

1. *$S \cap \mathfrak{p} \neq \emptyset \Rightarrow S^{-1}\mathfrak{q} = S^{-1}A$*
2. *If $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary. Moreover, $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$.*
   Therefore, one has $\{\mathfrak{q} \subset A | \mathfrak{q}$ is $\mathfrak{p}$-primary, $S \cap \mathfrak{p} = \emptyset\} \overset{1:1}{\longleftrightarrow} \{\mathfrak{q}' \subset S^{-1}A | \mathfrak{q}'$ is primary$\}$.

Proof:

1. $S \cap \mathfrak{p} \neq \emptyset \Rightarrow \exists s \in S \cap \mathfrak{p} \Rightarrow \exists s^n \in S \cap \mathfrak{q}, n \in \mathbb{N}_{>0}$, since $\mathfrak{p} = \mathfrak{r}(\mathfrak{q}) \supseteq \mathfrak{q}$.
   $\Rightarrow \frac{s^n}{1} \in S^{-1}\mathfrak{q}$ (s is a unit.)
   $\Rightarrow \frac{1}{1} \in S^{-1}\mathfrak{q} \Rightarrow S^{-1}\mathfrak{q} = S^{-1}A$

2. Note: Since $S \cap \mathfrak{p} = \emptyset$, we know that $S^{-1}\mathfrak{p} \in \mathrm{Spec}(S^{-1}A)$.
   Let's compute $\mathfrak{r}(S^{-1}\mathfrak{q}) = S^{-1}\mathfrak{r}(\mathfrak{q}) = S^{-1}\mathfrak{p}$. So, if $S^{-1}\mathfrak{q}$ is primary, then S^{-1} is $\mathfrak{p}$-primary.
   Now, we show that $S^{-1}\mathfrak{q}$ is primary:
   Let be $\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st} \in S^{-1}\mathfrak{q}, x, y \in A, s, t \in S$.
   $\Rightarrow xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}, n \in \mathbb{N}_{>0}$
   $\Rightarrow \frac{x}{s} \in S^{-1}\mathfrak{q}$ or $(\frac{y}{t})^n = \frac{y^n}{t^n} \in S^{-1}\mathfrak{q}$
   Next, we show $(\mathfrak{q}^e)^c = (S^{-1}\mathfrak{q})^c = \mathfrak{q}$:
   We already know by the definition $(S^{-1}\mathfrak{q})^c \supseteq \mathfrak{q}$. Let's prove the opposite inclusion, i.e. $(S^{-1}\mathfrak{q})^c \subseteq \mathfrak{q}$.
   Let $a \in (S^{-1}\mathfrak{q})^c$.
   $\Rightarrow f(a) = \frac{a}{1} \in S^{-1}\mathfrak{q} \Rightarrow \exists q \in \mathfrak{q}, s \in S : \frac{a}{1} = \frac{q}{s} \Rightarrow \exists t \in S : (a \cdot s - q \cdot 1) \cdot t = 0$
   $\Rightarrow ast = (st)a = tq \in \mathfrak{q}$
   On the other hand, $s \cdot t \notin \mathfrak{p} = \mathfrak{r}(\mathfrak{q})$, since $S \cap \mathfrak{p} = \emptyset$.
   $\Rightarrow \forall n \in \mathbb{N}_{>0} : (s \cdot t)^n \notin \mathfrak{q} \Rightarrow a \in \mathfrak{q}$, since $a(st) \in \mathfrak{q}$ and $\mathfrak{q}$ is primary.
   $\Rightarrow (S^{-1}\mathfrak{q})^c \subseteq \mathfrak{q}$
   $\Rightarrow (S^{-1}\mathfrak{q})^c = \mathfrak{q}$
   We get the mapping

$$\begin{array}{ccc} \varphi : \{\mathfrak{q} \subset A | \mathfrak{q} \text{ is } \mathfrak{p}\text{-primary}, S \cap \mathfrak{p} = \emptyset\} & \longrightarrow & \{\mathfrak{q}' \subset S^{-1}A | \mathfrak{q}' \text{ is } \mathfrak{p}'\text{-primary}\} \\ & & || \\ & & \{S^{-1}\tilde{\mathfrak{q}} \subset S^{-1}A | S^{-1}\tilde{\mathfrak{q}} \text{ is } S^{-1}\mathfrak{p}\text{-primary}\}, \\ & & \text{where } \tilde{\mathfrak{q}} \subset A, \mathfrak{r}(\tilde{\mathfrak{q}}) = \mathfrak{p} \end{array}$$

   We get $\varphi(\mathfrak{q}) = S^{-1}\mathfrak{q}$. Since $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$, φ is injective.
   φ is also surjective, since we have $\mathfrak{q}' = S^{-1}\tilde{\mathfrak{q}}$. It is left to the reader to check that $\tilde{\mathfrak{q}}$ is primary. □

Remark
In the given situation we have for $\mathfrak{a} \subset A$: $S^{-1}\mathfrak{a} = \mathfrak{a}^e$.

Notation
We use the notation as above. Furthermore let be $\mathfrak{a} \subseteq A$ an ideal.
We define $S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = (\mathfrak{a}^e)^c \supseteq \mathfrak{a}$.
Note: If $\mathfrak{q}$ is primary, then $S(\mathfrak{q}) = \mathfrak{q}$.

Proposition 3.4. (5) *Let $s \subseteq A$ be a multiplicatively closed subset and $\mathfrak{a} \subseteq A$ a decomposable ideal with minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$.*
Assume $\mathfrak{p}_i = \mathfrak{r}(\mathfrak{q}_i), i = 1, ..., n$ and that the indexing is such that $\mathfrak{p}_1, ..., \mathfrak{p}_m$ are disjoint to S while $\mathfrak{p}_{m+1}, ..., \mathfrak{p}_n$ are not.
Then, the primary decompositions (*) $S^{-1}\mathfrak{a} = \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i, S(\mathfrak{a}) = \bigcap_{i=1}^m \mathfrak{q}_i$ are minimal.

Proof:
By proposition 4 (2.), we know that $S^{-1}\mathfrak{q}_i$ are $S^{-1}\mathfrak{p}$-primary for $i = 1, ..., m$. By the properties of localization and proposition 4 (1.), we compute:

$$S^{-1}\mathfrak{a} = S^{-1}(\bigcap_{i=1}^{n} \mathfrak{q}_i) = \bigcap_{i=1}^{n} S^{-1}\mathfrak{q}_i = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \cap \underbrace{\bigcap_{i=m+1}^{n} S^{-1}\mathfrak{q}}_{=S^{-1}A} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i$$

Since $\mathfrak{p}_1, ..., \mathfrak{p}_m$ are pairwise distinct, also $S^{-1}\mathfrak{p}_1, ..., S^{-1}\mathfrak{p}_m$ are pairwise distinct. Therefore, the primary decomposition $S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i$ is also minimal.
To prove the second statement, take the contraction on both sides of (*).
$S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = (\bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m}(S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m} \mathfrak{q}_i$
Evidently, the primary decomposition $S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i$ is minimal, since the original decomposition for $\mathfrak{a}$ was minimal. □

Lecture on 2008-01-17

Example
Let be $A = K[X, Y]$ and $\mathfrak{a} = (X^2, XY)$.
$\Rightarrow \mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ with $\mathfrak{q}_1 = (X)$ and $\mathfrak{q}_2 = (X, Y)^2$.
$\mathfrak{q}_1$ and $\mathfrak{q}_2$ are primary and $\mathfrak{p}_1 = \mathfrak{r}(q_1) = \mathfrak{q}_1 = (X)$, $\mathfrak{p}_2 = \mathfrak{r}(\mathfrak{q}_2) = (X, Y)$. The ideals (X) and (X, Y) are associated to $\mathfrak{a}$. (They are uniquely determined by $\mathfrak{a}$.)
$\mathfrak{p}_1 = (X) \subset (X, Y) = \mathfrak{p}_2$.
$\mathfrak{p}_1$ is minimal and $\mathfrak{p}_2$ is embedded.

Now, let's look at the example geometrically:
$K[X, Y] \longleftrightarrow \mathbb{A}^2_K$
$\mathfrak{a} \longleftrightarrow V(\mathfrak{a}) = \{\binom{x}{y} \in \mathbb{A}^2_K | x = 0\}$
$\mathfrak{p}_1 \longleftrightarrow V(\mathfrak{p}_1) = \{\binom{x}{y} \in \mathbb{A}^2_K | x = 0\}$
$\mathfrak{p}_2 \longleftrightarrow V(\mathfrak{p}_2) = \{x\binom{x}{y} \in \mathbb{A}^2_K | x = y = 0\}$
Note also that besides the minimal primary decomposition $(X^2, XY) = \mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ we have the different minimal decomposition $\mathfrak{a} = \mathfrak{q}'_1 \cap \mathfrak{q}'_2$ with $\mathfrak{q}'_1 = (X)$ and $\mathfrak{q}'_2 = (X^2, Y)$.

Definition (isolated set of prime ideals)
Let $\mathfrak{a} \subseteq A$ be a decomposable ideal and $\Sigma \subseteq \mathrm{Spec}(A)$ a set of prime ideals associated to $\mathfrak{a}$.
Σ is called *isolated*, if it has the following property: If $\mathfrak{p} \in \Sigma$ and $\mathfrak{p}'$ is an associated prime ideal with $\mathfrak{p}' \subseteq \mathfrak{p}$, then $\mathfrak{p}' \in \Sigma$.

Remark
Keep the previous notations. Then, the set $S = A \setminus \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ is multiplicatively closed.
$(a, b \in S \Rightarrow \forall \mathfrak{p} \in \Sigma : a, b \notin \mathfrak{p} \Rightarrow \forall \mathfrak{p} \in \Sigma : a \cdot b \notin \mathfrak{p} \Rightarrow ab \in S)$

Remark
Let $\mathfrak{a}$ be decomposable and $\Sigma \subseteq \mathrm{Spec}(A)$ an isolated set of prime ideals associated to $\mathfrak{a}$.
Then, the set $S = A \setminus \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ is multiplicatively closed.
Furthermore, we note $\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \Rightarrow \mathfrak{p}' \cap S = \emptyset$.
Finally, we have $\mathfrak{p} \notin \Sigma \Rightarrow \mathfrak{p}' \not\subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. **Proof:**

Assume $\mathfrak{p}' \subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Let $\mathfrak{b} \subseteq A$ be an ideal, and $\mathfrak{p}_1, \mathfrak{p}_2$ prime ideals such that $\mathfrak{b} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2$.
$\Rightarrow \mathfrak{b} \subseteq \mathfrak{p}_q$ or $\mathfrak{b} \subseteq \mathfrak{p}_2$ **Proof:**
Assume $\mathfrak{b} \not\subseteq \mathfrak{p}_1, \mathfrak{b} \not\subseteq \mathfrak{p}_2$, but $\mathfrak{b} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2$.
$\Rightarrow \exists x_1 \in \mathfrak{b}, x_1 \in \mathfrak{p}_2 \setminus \mathfrak{p}_1$
$\exists x_2 \in \mathfrak{b}, x_2 \in \mathfrak{p}_1 \setminus \mathfrak{p}_2$
$\Rightarrow x_1 + x_2 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$, but $x_1 + x_2 \in \mathfrak{b}$ (otherwise: $x_1 + x_2 \in \mathfrak{p}_1 \cup \mathfrak{p}_2, x_1 \in \mathfrak{p}_2 \Rightarrow x_2 \in \mathfrak{p}_2 \Rightarrow$ contradiction)
$\Rightarrow$ contradiction

$\Rightarrow \mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$.
$\Rightarrow \mathfrak{p}' \notin \Sigma$, what is a contradiction.

$\Rightarrow \mathfrak{p}' \cap S \neq \emptyset$ □

Theorem 3.2. (Second uniqueness theorem (6)) *Let $\mathfrak{a} \subseteq A$ be a decomposable ideal and $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ a minimal primary decomposition of $\mathfrak{a}$. Further, let $\Sigma = \{\mathfrak{p}_{i_1}, ..., \mathfrak{p}_{i_m}\}$ be an isolated set of associated prime ideals.*
Then, the intersection $\bigcap_{k=1}^m \mathfrak{q}_{i_k}$ is independet of the given primary decomposition of $\mathfrak{a}$, i.e. it is determined solely by $\mathfrak{a}$.

Proof:
Consider the multiplicatively closed set $S = A \setminus \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} = A \setminus (\bigcup_{k=1}^m \mathfrak{p}_{i_k})$.
By the above remark, we know for $\mathfrak{p}' \in \mathrm{Spec}(A)$ associated to $\mathfrak{a}$:
$S \cap \mathfrak{p}' = \emptyset \Leftrightarrow \mathfrak{p}' \in \{\mathfrak{p}_{i_k} | i = 1, ..., m\}$.
By proposition 5, we get $\bigcap_{k=1}^m \mathfrak{q}_{i_k} = (S^{-1}\mathfrak{a})^c = S(\mathfrak{a})$.
Note, since $\mathfrak{p}_{i_1}, ..., \mathfrak{p}_{i_m}$, depend by the first uniqueness theorem solely on $\mathfrak{a}$, hence $S(\mathfrak{a})$ also depends solely on $\mathfrak{a}$. □

Corollary 3.1. (7) *Let $\mathfrak{a} \subseteq A$ be a decomposable ideal with minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$.*
Then, the primary components of $\bigcap_{i=1}^n \mathfrak{q}_i$ are uniquely determined whose radicals are minimal/isolated associated prime ideals of $\mathfrak{a}$.

Proof:
Let be $\mathfrak{p}_i \in \mathrm{Spec}(A)$ be a minimal prime ideal associated to $\mathfrak{a}$. Then, $\Sigma = \{\mathfrak{p}_i\}$ is an isolated set. Applying theorem 6 with this Σ shows that $\mathfrak{q}_i$ is solely determined by $\mathfrak{q}$, hence unique. □

3.3 Existence of primary decompositions in noetherien rings

In this section, we let A be a noetherian ring (and commutativ with 1 as always).

Definition (irreducible ideal)
An ideal $\mathfrak{a} \subseteq A$ is called *irreducible*, if the equality $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ ($\mathfrak{b}, \mathfrak{c} \subseteq A$ ideals) implies $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$. If $\mathfrak{a}$ is not irreducible, then $\mathfrak{a}$ is called *reducible*.

Proposition 3.5. (1) *In the noetherian ring A, an ideal $\mathfrak{a}$ is a finite intersection of irreducible ideals.*

Proof:
Assume, there is an ideal $\mathfrak{a}' \subseteq$, which is not a finite intersection of irreducible ideals. Let $\mathcal{M}$ be the set of all such ideals. By assumption, we get $\mathfrak{a}' \in \mathcal{M}$, i.e. $\mathcal{M} \neq \emptyset$.
Since A is noetherian, $\mathcal{M}$ has a maximal element $\mathfrak{a}$.
By construction, $\mathfrak{a}$ is not irreducible.
$\Rightarrow \exists \mathfrak{b}, \mathfrak{c} \subseteq A$ ideals, $\mathfrak{b} \subset \mathfrak{a}, \mathfrak{c} \supset \mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$
But, since $\mathfrak{a}$ is maximal in $\mathcal{M}$, $\mathfrak{b}, \mathfrak{c}$ do not belong to $\mathcal{M}$. Therefore, $\mathfrak{b}, \mathfrak{c}$ are finite intersections of irreducible ideals, hence $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ is also a finite intersection of irreducible ideals, which contradicts our assumption on $\mathfrak{a}$. □

Proposition 3.6. (2) *In a noetherian ring A every irreducible ideal $\mathfrak{a}$ is primary.*

Proof:
By considering the canonical surjective ring homomorphism $\pi : A \to A/\mathfrak{a}$ it suffices to prove the claim for the zero ideal in A. We are left to show:
If $(0) \subseteq A$ is irreducible, then it is primary.
Let $x \cdot y \in (0)$, i.e. $x \cdot y = 0$. We have to show $y = 0$ or $x^n = 0$ for some $n \in \mathbb{N}_{>0}$ ($\Leftrightarrow x \in \mathfrak{r}(0)$).
Consider the ascending chain of ideals $Ann(x) \subseteq Ann(x^2) \subseteq ....$
Since A is noetherian, this chain becomes stationary, i.e. $\exists n \in \mathbb{N}_{>0} : Ann(x^n) = Ann(x^{n+1}) = ...$
Claim: $(x^n) \cap (y) = (0)$, provided $y \neq 0$.

Let $a \in (x^n) \cap (y)$. We have to show that $a = 0$.
We have $a \in (y)$, i.e. $a = by$, $b \in A$.
$\Rightarrow ax = b(xy) = 0$, since $xy = 0$
Furthermore, we have $a \in (x^n) : a = b'x^n, b' \in A$.
$\Rightarrow b'x^{n+1} = (b'x^n)x = ax = 0$
$\Rightarrow b' \in Ann(x^{n+1}) = Ann(x^n)$
$\Rightarrow a = b'x^n = 0$ □

With $x \cdot y = 0$ and $y \neq 0$, we have to show $x \in \mathfrak{r}(0)$.
Now, we have by our claim $(x^n) \cap (y) = (0) \neq (y)$. By assumption, (0) is irreducible.
$\Rightarrow (x^n) = (0) \Rightarrow x^n \in (0) \Rightarrow x \in \mathfrak{r}(0)$. □

Theorem 3.3. (3) *In a noetherian ring A every ideal $\mathfrak{a} \subset A$ has a primary decomposition.*

Proof:
Use the propositions 1 and 2 in combination. □

Proposition 3.7. (4) *In a noetherian ring A, every ideal $\mathfrak{a}$ contains a power of its radical, i.e. $\exists N \in \mathbb{N}_{>0} : \mathfrak{r}(\mathfrak{a})^N \subseteq \mathfrak{a}$.*

Proof:
The radical $\mathfrak{r}(\mathfrak{a}) \subseteq A$ is finitely generated, let's say by $x_1, ..., x_k$.
$\Rightarrow \exists n_i \in \mathbb{N}_{>0} : x_i^{n_i} \in \mathfrak{a}, i = 1, ..., k$
$m = \sum_{i=1}^{k}(n_i - 1) + 1 \in \mathbb{N}_{>0}$
Now, $\mathfrak{r}(\mathfrak{a})^m$ is generated by $\prod_{i=1}^{k} x_i^{r_i}, r_i \in \mathbb{N}$ with $\sum_{i=1}^{k} r_k = m$.
If $r_i < n_i$ for all $i = 1, ..., k$, then $\sum_{i=1}^{k} r_i \leq \sum_{i=1}^{k}(n_i - 1) < \sum_{i=1}^{k}(n_i - 1) + 1 = m$.
$\Rightarrow \exists i \in \{1, ..., k\} : r_i \geq n_i$
$\Rightarrow \prod_{i=1}^{k} s_i^{r_i} \in \mathfrak{a}$, since $x_i^{r_i} \in \mathfrak{a}$.
$\Rightarrow \prod_{i=1}^{k} s_i^{r_i} \in \mathfrak{a}$ for all $(r_1, ..., r_k) \in \mathbb{N}^k$ and $\sum_{i=1}^{k} r_i = m$.
$\Rightarrow$ Every generator of $\mathfrak{r}(\mathfrak{a})^m$ is contained in $\mathfrak{a}$.
$\Rightarrow \mathfrak{r}(\mathfrak{a})^m \subseteq \mathfrak{a}$ □

Corollary 3.2. (5) *Let A be a noetherian ring, $m \in \mathrm{Max}(A)$ and $\mathfrak{q} \subset A$ an ideal. Then, the following are equivalent:*

1. *$\mathfrak{q}$ is $\mathfrak{m}$-primary.*
2. *$\mathfrak{r}(\mathfrak{q}) = \mathfrak{m}$*
3. *$\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $n \in \mathbb{N}_{>0}$.*

Proof:

1. (1) $\Rightarrow$ (2)
   This is just the definition for $\mathfrak{m}$-primary ideals.
2. (2) $\Rightarrow$ (1)
   See section 1, lemma 2.

3. (2) $\Rightarrow$ (3)

   See preceding proposition 4.

4. (3) $\Rightarrow$ (2)

   Look at $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ and take radicals:

   $\mathfrak{m} = \mathfrak{r}(\mathfrak{m}^n) \subseteq \mathfrak{r}(\mathfrak{q}) \subseteq \mathfrak{r}(\mathfrak{m}) = \mathfrak{m}$

   $\Rightarrow \mathfrak{r}(\mathfrak{q}) = \mathfrak{m}$ $\square$

Chapter 4

Existence and uniqueness of prime ideal decompositions in Dedekind rings

In this section A is assumed to be a noetherian integral domain (with 1).

Definition
The noetherian integral domain A is said to have *dimension* 1, if every prime ideal $\mathfrak{p} \neq (0)$ is maximal.

Proposition 4.1. (1) *Let A be a noetherian integral domain of dimension* 1.
Then, every ideal $(0) \neq \mathfrak{a} \subseteq A$ has a unique decomposition as product of primary ideals of A.

Proof:
By theorem 3, section 3, we have $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ where the $\mathfrak{q}_i$ are $\mathfrak{p}_i$-primary.
Observe: $\mathfrak{p}_i \supseteq \mathfrak{q}_i \supseteq \mathfrak{a} \neq (0)$
$\Rightarrow \mathfrak{p}_i \neq (0)$ for all $i = 1, ..., n$
Since A has dimension 1, every $\mathfrak{p}_i$ is maximal. Since $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are maximal, they are relatively prime to each other i.e. $\forall i \neq j : \mathfrak{p}_i + \mathfrak{p}_j = (1)$.
$\Rightarrow \mathfrak{r}(\mathfrak{q}_i + \mathfrak{q}_j) = \mathfrak{r}(\mathfrak{r}(\mathfrak{q}_i) + \mathfrak{r}(\mathfrak{q}_j)) = \mathfrak{r}(\mathfrak{p}_i + \mathfrak{p}_j) = (1)$
$\Rightarrow \mathfrak{q}_i + \mathfrak{q}_j = (1)$ $(1 \in \mathfrak{r}(\mathfrak{q}_i + \mathfrak{q}_j) \Rightarrow \exists n \in \mathbb{N}_{>0} : 1 = 1^n \in \mathfrak{q}_i + \mathfrak{q}_j \Rightarrow \mathfrak{q}_i + \mathfrak{q}_j = (1))$
$\Rightarrow \mathfrak{q}_1, ..., \mathfrak{q}_n$ are also relatively prime to each other.
$\Rightarrow \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i = \prod_{i=1}^{n} \mathfrak{q}_i$
Uniqueness follows from the second uniqueness theorem, since there are no embedded prime ideals. □

Lecture on 2008-01-24

Definition
A noetherian integral domain A of dimension 1 is called a *Dedekind ring* (or *Dedekind domain*), iff every primary ideal is the power of a prime ideal.

Example
$\mathbb{Z}$ is a Dedekind domain.

Remark
Let $\mathfrak{q} \subset A$ (A is Dedekind domain) be a $\mathfrak{p}$-primary ideal.
Claim: $\exists m \in \mathbb{N} : \mathfrak{q} = \mathfrak{p}^m$. **Proof:**
By definition, there exist $\mathfrak{p}' \in \mathrm{Spec}(A)$ and $m \in \mathbb{N}$ such that $\mathfrak{q} = \mathfrak{p}'^m$.
Taking radicals yields $\mathfrak{p} = \mathfrak{r}(\mathfrak{q}) = \mathfrak{r}(\mathfrak{p}'^m) = \mathfrak{p}'$.
$\Rightarrow \mathfrak{p}' = \mathfrak{p}$ □

Theorem 4.1. (2) *Let A be a Dedekind ring. Then, every ideal $0 \subset \mathfrak{a} \subset A$ can be uniquely (up to order) represented as a product of powers of prime ideals, i.e. $\mathfrak{a} = \prod_{k=1}^{n} \mathfrak{p}_k^{m_k}$, $\mathfrak{p}_1, ..., \mathfrak{p}_n \in \mathrm{Spec}(A)$.*

Proof:
Use proposition 1 and the remark above. □

Aim
We want to find a more handy characterizations of the notion of Dedekind rings ($\rightarrow$ Section 5).
Motivational example: (See problem set 13)
The ring $A = \mathbb{Z}[\sqrt{-5}]$ turns out to be a Dedekind domain.
Every ideal $0 \subset \mathfrak{a} \subset \mathbb{Z}[\sqrt{-5}]$ is product of powers of prime ideals, but this does not analogously hold for elements, since $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. We have $(6) = (2) \cdot (3) = ((1+\sqrt{-5})) \cdot ((1-\sqrt{-5}))$.

Observation
Let A be a Dedekind ring, $0 \neq \mathfrak{p} \in \mathrm{Spec}()$ and $S = A \setminus \mathfrak{p}$. Look at $s^{-1}A = A_\mathfrak{p}$, the localization of A at $\mathfrak{p}$.
$A_\mathfrak{p}$ is a local ring, i.e. it has only one maximal ideal $\mathfrak{m} = S^{-1}\mathfrak{p}$.

$$\begin{aligned} \{\mathfrak{p}' \in \mathrm{Spec}(A) | \mathfrak{p}' \subseteq \mathfrak{p}\} &\overset{1:1}{\leftrightarrow} \{\mathfrak{p}'' \in \mathrm{Spec}(A_\mathfrak{p})\} \\ \mathfrak{p}' &\mapsto S^{-1}\mathfrak{p}'' \\ (\mathfrak{p}'')^c &\hookleftarrow \mathfrak{p}'' \end{aligned}$$

Note: Since A is a dedekind domain, we get $\{\mathfrak{p}' \in \mathrm{Spec}(A) | \mathfrak{p}' \supseteq \mathfrak{p}\} = \{\mathfrak{p}, (0)\}$.
$\Rightarrow \mathrm{Spec}(A_\mathfrak{p}) = \{(0), \mathfrak{m}\}$
Let $0 \subset \mathfrak{a} \subset A$ be an ideal.
$\Rightarrow \mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{m_i}$
$\Rightarrow S^{-1}\mathfrak{a} = S^{-1}(\prod_{i=1}^{n} \mathfrak{p}_i^{m_i}) = \prod_{i=1}^{n} (S^{-1}\mathfrak{p}_i)^{m_i} = \mathfrak{m}^k$ with $k \in \mathbb{N}$

Definition
Let be $0 \neq x \in A_\mathfrak{p}$. We put $v(x) = k$, where $(x) = \mathfrak{m}^k$ (in the above sense).
Note: $v(x) \in \mathbb{N}$.
Check for $x, y \neq 0$:

1. $x, y \in A_\mathfrak{p} \Rightarrow v(xy) = v(x) + v(y)$
   This follows directly from the definition.
2. $x, y \in A_\mathfrak{p} \Rightarrow v(x+y) \geq \min(v(x), v(y))$

So far, we have a map $v : A_\mathfrak{p}^\times \rightarrow \mathbb{N}$.
Claim: v is surjective.
Proof: We need to find $x \in A_\mathfrak{p}^\times$ such that $v(x) = 1$.
Note: $\mathfrak{m}^{k+1} \neq \mathfrak{m}^k$ for all $k \in \mathbb{N}$.
Assuming the existstance of $k \in \mathbb{N} : \mathfrak{m}^{k+1} = \mathfrak{m}$, we get immediately $\mathfrak{m} \cdot \mathfrak{m}^k = \mathfrak{m}^k$.
Remember:

Nakayama-Lemma:
Let M a finitely generated A-module, $\mathfrak{a} \subseteq A$ and $\mathfrak{a} \subseteq$ Jacobson radical.
$\mathfrak{a}M = M \Rightarrow M = (0)$

Applying the lemma of Nakayama to the ring $A_\mathfrak{p}$, $M = \mathfrak{m}^k$ and $\mathfrak{a} = \mathfrak{m}$, we get $\mathfrak{m}^k = 0$.
$\Rightarrow \mathfrak{m} = 0$, since $A_\mathfrak{p}$ is integral domain.
$\Rightarrow$ contradiction.
Hence, we really have $\forall k \in \mathbb{N} : \mathfrak{m}^{k+1} \neq \mathfrak{m}^k$.
We apply this for $k = 1$ and get $\mathfrak{m}^2 \neq \mathfrak{m} \neq \emptyset$.
$\Rightarrow \exists x \in \mathfrak{m} \setminus \mathfrak{m}^2$
$\Rightarrow (x) = \mathfrak{m}$, i.e. $v(x) = 1$
We extend v to a surjective map $v : \mathrm{Quot}(A_\mathfrak{p}) \setminus \{0\} \to \mathbb{Z}$ by setting $v(x^{-1}) = -v(x)$.
More conseptually: Given a Dedekind domain A, $0 \neq \mathfrak{p} \in \mathrm{Spec}(A)$, we have constructed a surjective homomorphism $v : \mathrm{Quot}(A_\mathfrak{p})^\times \to \mathbb{Z}$. By construction, we have $A_\mathfrak{p}^\times = \{x \in \mathrm{Quot}(A_\mathfrak{p}^\times | v(x) \geq 0\}$.

Definition (discrete valuation)
Let K be a field. *A discrete valuation* on K is given by a surjection homomorphism $v : K^\times \to \mathbb{Z}$ such that

1. $v(xy) = v(x) + v(y)$ for all $x, y \in K^\times$
2. $v(x + y) \geq \min(v(x), v(y))$ for all $x, y, x + y \in K^\times$

holds.
Sometimes, one puts in addition $v(0) = \infty$.
The set $\{x \in K^\times | v(x) \geq 0\} \cup \{0\}$ is a ring, which is called the *discrete valuation ring associated to* v. An integral domain R is called a *discrete valuation ring*, iff it has a discreate valuation v and $R = \{x \in \mathrm{Quot}(R) | v(x) \geq 0\}$.

Example
Let A be a Dedekind domain and $0 \neq \mathfrak{p} \in \mathrm{Spec}(A)$. Then $A_\mathfrak{p}$ is a discrete valuation ring.

4.1 Characterization of Dedekind rings

We start with some preliminaries on integral dependence.

Definition (integral elements, integral closure)
Let A, B be commutative rings with 1 and $B \subseteq A$. An element $x \in B$ is called *integral* over A, if there eixists a monic polynomial $p(X) = X^n + \sum_{k=0}^{n-1} a_k X^k \in A[X]$ with $p(x) = 0$.
The set of all elements $x \in B$, which are integral over A is called the *integral closure* of A in B.

Example
Let be $B = \mathbb{Q}$ and $A = \mathbb{Z}$. In this case, $\mathbb{Z}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$.

Lemma 4.1. (1) *Let A, B be commutative rings with 1 and $B \supseteq A$.*
Then, the following four statements are equivalent:

1. *$x \in B$ is integral over A*
2. *$A[x]$ is a finitely generated A-module.*
3. *$A[x]$ is contained in a subring $C \subseteq B$, which is a finitely generated A-module:*
   $A \subseteq A[x] \subseteq C \subseteq B$
4. *There exists a faithful $A[x]$-module M, which is a finitely generated as an A-module.*
   Recall: A module is called faithful, if $y \cdot M = 0, y \in A[x]$ implies $y = 0$.

Proof:

1. (1) $\Rightarrow$ (2)

   Let be $x \in B$ integral over A.

   $\Rightarrow x^n + \sum_{k=0}^{n-1} a_k x^k = 0$ for some $n \in \mathbb{N}_{>0}, a_0, ..., a_{n-1} \in A$.

   $\Rightarrow x^n = \sum_{k=0}^{n-1} (-a_k) x^k$

   $\Rightarrow x^n$ can be generated (over A), i.e. represented as an A-linear combination, by $1, x, ..., x^{n-1}$, $k \in \mathbb{N}$.

   $\Rightarrow A[x]$ is generated as an A-module by $1, x, ..., x^{n-1}$.

   $\Rightarrow A[x]$ is a finitely generated A-module.

2. (2) $\Rightarrow$ (3)

   Choose $C = A[x]$

   C is a ring: $A \subseteq A[x] = C \subseteq B$.

   C is a finitely generated A module.

3. (3) $\Rightarrow$ (4)

   Choose $M = C$.

   Note: $A[x] \subseteq C$, by (3).

   $\Rightarrow C$ is an $A[x]$-module. C is finitely generated as an A-module, by (3).

   C is a ring, i.e. $1 \in C$.

   Suppose: $y \cdot M = 0$ for some $y \in A[x]$

   $\Rightarrow y \cdot C = 0$ for some $y \in A[x]$

   $\Rightarrow y \cdot 1 = 0$ for some $y \in A[x]$

   $\Rightarrow y = 0$

4. (4) $\Rightarrow$ (1)

   Recall:

   > Let M be a finitely generated A-module, $\mathfrak{a} \subseteq A$ an ideal and $\varphi \in \mathrm{End}_A(M)$ such that $\varphi(M) \subseteq \mathfrak{a} \cdot M$.
   > Then, there exist $a_0, ..., a_{n-1} \in \mathfrak{a}$ such that $\varphi^n + a_{n-1}\varphi^{n-1} + ... + a_0 \mathrm{id}_M = 0_M$.

   Let $\varphi : M \to M$ be given by $m \mapsto x \cdot m$.

   (M is a finitely generated A-module and $\varphi \in \mathrm{End}_A(M)$.)

   $\Rightarrow \exists a_0, ..., a_{n-1} : \varphi^n + \sum_{k=0}^{n-1} a_k \varphi^k = 0 \in \mathrm{End}_A(M)$

   Since M is a faithful $A[x]$-module, we must have $x^n + \sum_{k=}^{n-1} a_k x^k = 0$.

   $\Rightarrow x$ is integral over A. □

Definition (integrally closed)
An integral domain A is called *integrally closed*, if the integral closure of A in $\mathrm{Quot}(A)$ equals A itself.

Lemma 4.2. (2) *Let R be discrete valuation ring.*
Then, R is integrally closed.

Proof:
Let be $K = \mathrm{Quot}(R)$ and $v : K^\times \to (\mathbb{Z}, +)$ our well-known surjective homomorphism.
We have $R = \{x \in K^\times | v(x) \geq 0\} \cup \{0\}$.
We have to show: $x \in K$ (integral over R)$\Rightarrow x \in R$.
Let be $0 \neq x \in K$ integral over R.
$\Rightarrow \exists n \in \mathbb{N}_{>0}, a_0, ..., a_{n-1} \in R : x^n + \sum_{k=0}^{n-1} a_k x^k = 0$

(Note, $x \in K^\times = \left\{ \begin{array}{l} v(x) \geq 0 \ \Rightarrow \ x \in R \\ v(x) < 0 \ \Rightarrow \ x^{-1} \in R \end{array} \right.$)
If $x \in R$, then we are done.
If $x^{-1} \in R$, we divide $x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$ by x^{n-1}.
$\Rightarrow x = -a_{n-1} \cdot 1 - a_{n-2}x^{-1} - ... - a_1(x^{-1})^{n-2} - a_0(x^{-1})^{n-1} \in R$ □

Characterization
We now come to the characterization of discrete valuation ring. For this, we let R be a

- local
- noetherian integral domain
- of dimension 1

Notation
Let be $\mathfrak{m}$ be the unique maximal ideal of R and $K = R/\mathfrak{m}$ the residue field of R.

Remark

1. Let $(0) \subset \mathfrak{a} \subset R$ be primary.
   $\Rightarrow \mathfrak{r}(\mathfrak{a}) = \mathfrak{m}$
   $\Rightarrow \exists n \in \mathbb{N}_{>0} : \mathfrak{m}^n \subseteq \mathfrak{a}$
2. By Nakayama's lemma, we recall $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all $n \in \mathbb{N}$, i.e. $\forall n \in \mathbb{N} : \mathfrak{m}^n \supset \mathfrak{m}^{n+1}$.

Theorem 4.2. (3) *Let R be a local, noetherial integral domain of dimension 1 with maximal ideal $\mathfrak{m}$ and residue field $K = R/\mathfrak{m}$. Then, the following are equivalent:*

1. *R is a discrete valuation ring.*
2. *R is integrally closed*
3. *$\mathfrak{m}$ is principal ideal*
4. *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$*
5. *Every non-zero ideal of R is a power of $\mathfrak{m}$.*
6. *Every (non-zero) ideal of R is of the form (x^n) for some $x \in R, n \in \mathbb{N}$.*

Proof:

1. (1) $\Rightarrow$ (2)
   This is just Lemma 2.
2. (2) $\Rightarrow$ (3)
   $\mathfrak{m} \neq 0 \Rightarrow \exists a \in \mathfrak{m}, a \neq 0$
   By the second remark above, we find $n \in \mathbb{N} : \mathfrak{m}^n \subseteq (a), \mathfrak{m}^{n-1} \not\subseteq (a)$.
   $\Rightarrow \exists b \in \mathfrak{m}^{n-1} \setminus (a)$
   We define $x = \frac{a}{b} = a \cdot b^{-1} \in K = \text{Quot}(R)$.
   We want to show $\mathfrak{m} = (x)$.
   Note: $x^{-1} \notin R$, since $x^{-1} = \frac{b}{a} \in R \Rightarrow b \in (a)$
   Since R is integrally closed by (2), we have that x^{-1} is not integral over R.
   $\Rightarrow x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$

Assume $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$
$\Rightarrow \mathfrak{m}$ is an $R[x^{-1}]$-module and faithful.
$\Rightarrow$ (Lemma 1, part 4) x^{-1} is integral over R.

By our construction: $b \cdot \mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$

$\Rightarrow x^{-1}\mathfrak{m} = \frac{b}{a} \cdot \mathfrak{m} \subseteq R$

$\Rightarrow x^{-1}\mathfrak{m} = R$ (since $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$)

$\Rightarrow \mathfrak{m} = x \cdot R = (x)$

3. (3) $\Rightarrow$ (4)

   Let be $\mathfrak{m} = (x)$ for some $x \in R$.

   $\Rightarrow \mathfrak{m}/\mathfrak{m}^2$ is generated by $x + \mathfrak{m}^2$ as a K-vector space.

   $\Rightarrow \dim_K(\mathfrak{m}/\mathfrak{m}^2) \leq 1$

   On the other hand, by the second remark, $\mathfrak{m} \neq \mathfrak{m}^2$, hence $\mathfrak{m}/\mathfrak{m}^2 \neq 0$.

   $\Rightarrow \dim_K(\mathfrak{m}/\mathfrak{m}^2) = 1$

Lecture on 2008-01-31

4. (4) $\Rightarrow$ (5) Since $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 1$, we have $\mathfrak{m} = (x)$ for some $x \in R$.

   Assume $\mathfrak{a} \neq (0), R$.

   So $\mathfrak{a}$ is primary with $\mathfrak{r}(\mathfrak{a}) = \mathfrak{m}$. Using corollary 5 of section 3 yields $\exists n_0 \in \mathbb{N} : \mathfrak{m}^{n_0} \subseteq \mathfrak{a}$. (W.l.o.g. we assume $\mathfrak{m}^{n_0} \subset \mathfrak{a}$ and $n_0 \geq 1$ (otherwise $\mathfrak{m} \subseteq \mathfrak{a} \subseteq \mathfrak{m}$).)

   Consider $\pi : R \to \overline{R} = R/\mathfrak{m}^{n_0}$, where $\mathfrak{a} \mapsto \overline{\mathfrak{a}}$. W.l.o.g.: $\overline{\mathfrak{a}} \neq (\overline{0})$ (otherwise $\mathfrak{a} = \mathfrak{m}^{n_0}$).

   Let be $\mathfrak{n}_{\overline{R}}$ the nilradical of $\overline{R}$.

   $\Rightarrow \pi^{-1}(\mathfrak{n}_{\overline{R}}) = \mathfrak{r}(\mathfrak{m}^{n_0}) = \mathfrak{r}(\mathfrak{m}) = \mathfrak{m}$

   $\Rightarrow \overline{\mathfrak{m}} = \pi(\mathfrak{m}) = \pi(\pi^{-1}(\mathfrak{n}_{\overline{R}})) = \mathfrak{n}_{\overline{R}}$

   $\Rightarrow \overline{x} \in (\overline{x}) = \overline{(x)} = \overline{\mathfrak{m}} = \mathfrak{n}_{\overline{R}}$ is nilpotent.

   $\Rightarrow \exists n_1 \in \mathbb{N} : \overline{\mathfrak{m}}^{n_1} = (\overline{0})$

   $\Rightarrow \exists n_2 \in \mathbb{N} : \overline{\mathfrak{a}} \subseteq \overline{\mathfrak{m}}^{n_2}$, but $\overline{\mathfrak{a}} \not\subseteq \overline{\mathfrak{m}}^{n_2+1}$.

   We want to show $\overline{\mathfrak{a}} \supseteq \overline{\mathfrak{m}}^{n_2}$ ($\Rightarrow \overline{\mathfrak{a}} = \overline{\mathfrak{m}}^{n_2}$).

   Let be $\overline{y} \in \overline{\mathfrak{m}}$.

   $\Rightarrow \overline{y} = \overline{a} \cdot \overline{x}^{n_2}, \overline{a} \in \overline{R}$ (note: $\mathfrak{m} = (x) \Rightarrow \overline{\mathfrak{m}} = (\overline{x})$) with $\overline{a} \notin \overline{\mathfrak{m}} \Rightarrow \overline{a} \in \overline{R}^\times$

   $\Rightarrow \overline{\mathfrak{m}}^{n_2} = (\overline{x}^{n_2}) = (\overline{y}) \subseteq \overline{\mathfrak{a}}$

   $\Rightarrow \overline{\mathfrak{a}} = \overline{\mathfrak{m}}^{n_2}$

   Lifting this equation up to R yields:

   $\mathfrak{a} + \mathfrak{m}^{n_0} = \mathfrak{m}^{n_2} + \mathfrak{m}^{n_0}$

   Let n_0 be large enoug such that $\mathfrak{m}^{n_2} \supseteq \mathfrak{m}^{n_0}$.

   $\Rightarrow \mathfrak{a} = \mathfrak{m}^{n_2}$

5. (5) $\Rightarrow$ (6)

   By Nakayama's Lemma, we have $\mathfrak{m} \neq \mathfrak{m}^2$.

   $\Rightarrow \mathfrak{m}^2 \subset \mathfrak{m}$

   $\Rightarrow \exists x \in \mathfrak{m} \setminus \mathfrak{m}^2$

   By assumption, applied to $\mathfrak{a} = (x)$, we have $(x) = \mathfrak{m}^k$ for some $k \in \mathbb{N}$.

   Since $(x) \not\subseteq \mathfrak{m}^2$, we must have $k = 1$, hence $\mathfrak{m} = (x)$.

   Let $(0) \neq \mathfrak{a} \subseteq R$. By assumption, there ist $n \in \mathbb{N}$ such that $\mathfrak{a} = \mathfrak{m}^n = (x)^n = (x^n)$.

6. (6) $\Rightarrow$ (1)

   Let be $K = \mathrm{Quot}(R)$.

   We have to construct a discrete valuation v on $K^\times$ such that $R^\times = \{r \in R | v(r) \geq 0\}$.

   We have, in particular, by assumption $\mathfrak{m} = (x)$ for some $x \in R$. By Nakayama, we note $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ which shows that $(x^n) \neq (x^{n+1})$.

   This shows, that (given $0 \neq a \in R$) there is a unique $n \in \mathbb{N}$ such that $(a) = (x^n)$. We define $v(a) = n \in \mathbb{N}$ and extend this definition to $K^\times$ as follows:

   Any element in $K^\times$ is of the form $\frac{a}{b}$ with $a, b \in R^\times$. We set $v(\frac{a}{b}) = v(a) - v(b)$.

   $\Rightarrow v(K^\times) = \mathbb{Z}$

   By the very construction, v is a homomorphism, i.e. $v(y_1 \cdot y_2) = v(y_1) \cdot v(y_2)$, for all $y_1, y_2 \in K^\times$.

   By inspection you find $v(y_1 + y_2) \geq \min(v(y_1), v(y_2))$ for all $y_1, y_2 \in K^\times$.

   By construction, we also get $R^\times = \{y \in K^\times | v(y) \geq 0\}$. $\square$

Proposition 4.2. (4) *Let $B \supseteq A$ be commutative rings with 1.*
Then, the following holds true:

1. *The integral closure of A in B is a ring containing A.*
2. *Let $C \supseteq B$ be a third commutative ring with 1.*

   If C is integral over B and B is integral over A, then C is integral over A.
3. *Let B be integral over A, $\mathfrak{b} \subseteq B$ an ideal and $\mathfrak{a} = A \cap \mathfrak{b}$.*

   Then, $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.
4. *Let B be integral over A and $S \subseteq A$ a multiplicatively closed set.*

   $\Rightarrow S^{-1}B$ is integral over $S^{-1}A$.

Proof:

1. See Problem-Set 13, Problem 1.

   Note: If x, y are integral over A, then $A[x, y]$ is finitelay generated over A.

   $\Rightarrow A[x + y]$ is finitely generated over A.

   $\Rightarrow x \pm y$ is integral over A.
2. See Problem-Set 13, Problem 2.

   Let be $x \in C$ integral over B.

   $\Rightarrow x^n + \sum_{k=0}^{n-1} b_k x^k = 0, b_0, ..., b_{n-1} \in B$

   $b_0, ..., b_{n-1}$ are ingegral over A.

   $\Rightarrow B' = A[b_0, ..., b_{n-1}] \subseteq B$ is a finitely generated A-module.

   Look at $B'[x]$. This is a faithful $A[x]$-module and finitely generated over A, i.e. x is integral over A.
3. Let $x \in B$ and $\overline{x} \in B/\mathfrak{b}$.

   x is integral over A.

   $\Rightarrow x^n + \sum_{k=0}^{n-1} a_k x^k = 0, a_0, ..., a_{n-1} \in A$

   $\Rightarrow \overline{x}^n + \sum_{k=0}^{n-1} \overline{a}_k \overline{x}^k = 0$

   $\Rightarrow \overline{x} \in B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.

4. Let be $\frac{x}{s} \in S^{-1}B$, i.e. $x \in B, s \in S$. Furthermore, let x be integral over A.

   $\Rightarrow x^n + \sum_{k=0}^{n-1} a_k x^k = 0, a_0, ..., a_{n-1} \in A$

   We localize the equation by s^n:

   $\Rightarrow (\frac{x}{s})^n + \sum_{k=0}^{n-1} \frac{a_k}{s^{n-k}} (\frac{x}{s})^k = 0$

   $\Rightarrow \frac{x}{s}$ is integral over $S^{-1}A$.

Lemma 4.3. (5) *Let $B \supseteq A$ be commutative rings with 1 and C the integral closure of A in B. Let $S \subseteq A$ be a multiplicatively closed subset.*
Then, the integral closure of $S^{-1}A$ in $S^{-1}B$ is $S^{-1}C$.

Proof:
Let C^0 be the integral closure of $S^{-1}A$ in $S^{-1}B$. By Proposition 4 (4.), we have $S^{-1}C \subseteq C^0$.
We show the oppositie inclusion, i.e. $C^0 \subseteq S^{-1}C$. Let be $\frac{b}{s} \in C^0 \subseteq S^{-1}B$ with $b \in B, s \in S$. Since $\frac{b}{s} \in C^0$, $\frac{b}{s}$ is integral over $S^{-1}A$, i.e. $(\frac{b}{s})^n + \sum_{k=0}^{n-1} \frac{a_k}{s_k} (\frac{b}{s})^k = 0$ where $a_0, ..., a_{n-1} \in A$, $s_0, ..., s_{n-1} \in S$. Put $t = \prod_{k=0}^{n-1} s_k \in S$. Multiplying the equation by t gives $(\frac{b}{s})^n t + \sum_{k=0}^{n-1} a_k \frac{t}{s_k} (\frac{b}{s})^k = 0$. Multiplying this by s^n yields $b^n t + a_{n-1} \cdot (s_{n-2} \cdot ... \cdot s_0) \cdot s b^{n-1} + ... + a_0 (s_{n-1} \cdot ... \cdot s_1) s^n = 0$. Finally, we multiply by t^{n-1} and get $(bt)^n a_{n-1} (s_{n-2} \cdot ... \cdot s_0) \cdot s(bt)n - 1 + ... + a_0 \cdot (s_{n-1} \cdot ... \cdot s_1) s^n t^{n-1} = 0$.
$\Rightarrow bt$ is integral over A.
$\Rightarrow bt \in C$.
$\frac{b}{s} = \frac{bt}{st} \in S^{-1}C \Rightarrow C^0 \subseteq S^{-1}C$
$\Rightarrow C^0 = S^{-1}C$ □

Proposition 4.3. (6) *Let A be an integral domain (with quotient field $K = \mathrm{Quot}(A)$).*
Then the following statements are equivalent:

1. *A is integrally closed.*
2. *$A_\mathfrak{p}$ is integrally closed for all $\mathfrak{p} \in \mathrm{Spec}(A)$.*
3. *$A_\mathfrak{m}$ is integrally closed for all $\mathfrak{m} \in \mathrm{Max}(A)$.*

Proof:

1. (1) $\Leftrightarrow$ (2)

   Let be C the integral closure of A in K.

   (Note: If A is integrally closed, then $A = C$.)

   Finally, let be $f : A \to C$ the natural inclusion.

   Now, we have the equivalences:

   A is integrally closed $\Leftrightarrow f : A \hookrightarrow C$ is surjective.
   $\Leftrightarrow f_\mathfrak{p} : A_\mathfrak{p} \hookrightarrow C_\mathfrak{p}$ is surjective for all $\mathfrak{p} \in \mathrm{Spec}(A)$.
   By Lemma 5, $C_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in K.
   $\Leftrightarrow A_\mathfrak{p}$ is integrally closed for all $\mathfrak{p} \in \mathrm{Spec}(A)$

2. (1) $\Leftrightarrow$ (3)

   This equivalence is established in an analogours way, observing the fact that $f : A \to C$ is injective/surcjective, iff $f_\mathfrak{m} : A_\mathfrak{m} \to C_\mathfrak{m}$ is injective/surjective for all $\mathfrak{m} \in \mathrm{Max}(A)$. □

Theorem 4.3. (Characterization of Dedekind domains (7)) *Let A be a notherian integral domain of dimension 1. Then, the following statements are equivalent.*

1. *A is integrally closed.*

2. *Every primary ideal is the power of a prime ideal.*

3. *Every localization* $A_{\mathfrak{p}}, (0) \neq \mathfrak{p} \in \mathrm{Spec}(A)$ *is a discrete valuation ring.*

Proof:

1. (1) $\Leftrightarrow$ (3)

   By proposition 6, we have the equivalence:

   A is integrally closed $\Leftrightarrow f : A \hookrightarrow C$ is surjective.
   $\Leftrightarrow f_{\mathfrak{p}} : A_{\mathfrak{p}} \hookrightarrow C_{\mathfrak{p}}$ is surjective for all $\mathfrak{p} \in \mathrm{Spec}(A)$.
   Note: The case $\mathfrak{p} = (0)$ is trivial: $A_{(0)} = K$.

   Applying theorem 3 to the local, noetherian integral domain $R = A_{\mathfrak{p}}, (0) \neq \mathfrak{p} \in \mathrm{Spec}(A)$ of dimesion 1, shows the equivalence (1) $\Leftrightarrow$ (3).

2. (2) $\Rightarrow$ (3)

   Assume: Every non-zero primary ideal of A is a power of some $(0) \neq \mathfrak{p} \in \mathrm{Spec}(A)$.

   Let now $(0) \neq \mathfrak{a} \subseteq A_{\mathfrak{p}}$ be an ideal and $\mathfrak{m} = \mathfrak{p}_{\mathfrak{p}}$ the maximal ideal of $A_{\mathfrak{p}}$. Since $A_{\mathfrak{p}}$ is noetherian, $(0) \neq \mathfrak{a}$ is $\mathfrak{m}$-primary.

   Since A has dimension 1, by noetherian property, the ideal $\mathfrak{a}$, which is obtained by localization of an ideal of A, has to be a power of $\mathfrak{m}$. (Since the ideal in question reduces to one primary component which is a power of $\mathfrak{p}$.)

   Again, applying theorem 3 to $R = A_{\mathfrak{p}}$ (the implication (1) $\Leftarrow$ (5)), shows (2) $\Rightarrow$ (3).

3. (3) $\Rightarrow$ (2)

   Assume: $A_{\mathfrak{p}}$ are discrete valuation rings for all $\mathfrak{p} \in \mathrm{Spec}(A), \mathfrak{p} \neq (0)$.

   Now, we apply theorem 3, with $R = A_{\mathfrak{p}}$ (implication (1) $\Rightarrow$ (5)).

   Hence, every $(0) \neq \mathfrak{a} \subset A_{\mathfrak{p}}$ is a power of $\mathfrak{m} = \mathfrak{p}_{\mathfrak{p}}$, i.e. $\mathfrak{a} = \mathfrak{m}^n$ for some $n \in \mathbb{N}_{>0}$, i.e. $\mathfrak{a}$ is $\mathfrak{m}$-primary. By contraction of $\mathfrak{a}$, we get a primary ideal of A such that $\mathfrak{a} \cap A = \mathfrak{p}^n$.

   Since (3) holds for all $\mathfrak{p} \in \mathrm{Spec}(A)$, we cover all primary ideals of A in this way and recognize them as powers of prime ideals. □

4.2 The fundamental theorem of arithmetic

Definition
Let $K/\mathbb{Q}$ be a finite algebraic extension. The integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called the ring of integers of K.
$\mathcal{O}_K$ is also called *maximal order* in K.
$\mathbb{Z}[\sqrt{-5}]$ is a ring of integers of $\mathbb{Q}(\sqrt{-5})$.
The fundamental theorem fails here: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Theorem 4.4. (1) *The ring of integers* $\mathcal{O}_K$ *of a finite algebraic extension* $K/\mathbb{Q}$ *is a Dedekind domain.*

Proof:
We show that $\mathcal{O}_K$ is a noetherian integral domain of dimension 1 and that all primary ideals are powers of prime ideals.

1. $\mathcal{O}_K$ is an integral domain:

   This is clear, since $\mathcal{O}_K \hookrightarrow K$.

   Note: $K = \mathrm{Quot}(\mathcal{O}_K)$.

2. $\mathcal{O}_K$ is integrally closed:

   Let C be the integral closure of $\mathcal{O}_K$ in K.

   $\Rightarrow C$ is integral over $\mathcal{O}_K$ and $\mathcal{O}_K$ is integral over $\mathbb{Z}$.

   $\Rightarrow C$ is integral over $\mathbb{Z}$.

   $\Rightarrow C = \mathcal{O}_K$ by the definition of $\mathcal{O}_K$.

3. $\mathcal{O}_K$ is noetherian: Wie show: $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. ($\Rightarrow$ every ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is also a finitely generated $\mathbb{Z}$-module, hence a finitely generated ideal.)

   We take a basis $\{\alpha_1, ..., \alpha_n\}$ of $K/\mathbb{Q}$. W.l.o.g. $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$.

   Let be $x \in \mathcal{O}_K$.

   $\Rightarrow x \in K$

   $\Rightarrow \exists x_1, ..., x_n \in \mathbb{Q} : x = \sum_{j=1}^n x_j \alpha_j$

   Multipliying x by α_k yields $K \ni x \cdot \alpha_k = \sum_{j=1}^n x_j (\alpha_j \alpha_k), k = 1, ..., n$.

   $\mathbb{Z} \ni \mathrm{tr}_{K/\mathbb{Q}}(x \cdot \alpha_k) = \sum_{j=1}^n x_j \underbrace{\mathrm{tr}_{K/\mathbb{Q}}(\alpha_j \alpha_k)}_{\in \mathbb{Z}}$

   This is a system of linear equations for $x_1, ..., x_n$. Let $D = \det(\mathrm{tr}_{K/\mathbb{Q}}(\alpha_j \alpha_k)) \in \mathbb{Z}$.

   $D \neq 0$ by general reasons (or, use $K = \mathbb{Q}(\vartheta), \alpha_1 = \vartheta^0, ..., \alpha_n = \vartheta^{n-1}$ and note that D is the Vandermonde determinant which is non-zero).

   $\Rightarrow x_j \in D^{-1}\mathbb{Z}, j = 1, ..., n$

   $\Rightarrow \mathcal{O}_K \subseteq D^{-1} \sum_{j=1}^n \mathbb{Z} \cdot \alpha_j$ is a finitely generated $\mathbb{Z}$-module.

   $\Rightarrow \mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module (as a $\mathbb{Z}$-submodule of $D^{-1} \sum_{j=1}^n \mathbb{Z} \cdot \alpha_j$).

4. $\mathcal{O}_K$ has dimension 1:

   Let $(0) \neq \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$

   Proposition 4: $\mathcal{O}_K/\mathfrak{p}$ is integral over $\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} = \mathbb{F}_p$.

   Show: $\mathcal{O}_K/\mathfrak{p}$ is a field.

   $x \in \mathcal{O}_K/\mathfrak{p}, x \neq 0$

   $\Rightarrow x^n + \sum_{k=0}^n a_k x^k = 0$ with $a_0, ..., a_{n-1} \in \mathbb{Z}/(p)$

   $x^{-1} = -a_0^{-1}(x^{n-1} + \sum_{k=1}^{n-1} a_k x^{k-1}) \in \mathcal{O}_K/\mathfrak{p}$

Lecture on 2008-02-07

Chapter 5

Structure Theorems for Algebras

5.1 Basics

In this chapter, K denotes a field.

Definition (K-algebra)
A ring A is called K-*algebra*, if A has a K-vector space structure, with $\lambda\cdot(a\cdot b) = (\lambda\cdot a)\cdot b = a\cdot(\lambda\cdot b)$, $\lambda \in K$, $a, b \in A$ and whose addition coincides with that of the ring structure.

Definition
The *dimension* $\dim_K A$ of a K-algebra A is the dimension of A as a K-vector space.

Example
Let be $M_n(K)$ the set of $n \times n$-matrices with entries in K, i.e. $M_n(K) = \{(a_{j,k})_{1\leq j,k\leq n} | a_{j,k} \in K\}$. We have $\dim_K(M_n(K)) = n^2$. $M_n(K)$ is a K-algebra and non-commutative, if $n > 1$.

Definition (skew-field)
A K-algebra A is called a *skew-field* (Ⓓ: Schiefkörper) or *division algebra* over K, if for each $0 \neq a \in A$, there exists $a^{-1} \in A$ satisfying $a^{-1} \cdot a = 1 = a \cdot a^{-1}$.

Example (Hamiltonians)
Let be $K = \mathbb{R}$. We define $\mathbb{H} = \{a \cdot 1 + b \cdot i + c \cdot j + d \cdot k | a, b, c, d \in \mathbb{R}\}$ subject to the following conditions:
$i^2 = j^2 = k^2 = -1$
$i \cdot j = -j\dot{i} = k$ (analogously for cyclically permuted i, j and k)
We get $\dim_{\mathbb{R}} \mathbb{H} = 4$.
$\Rightarrow \mathbb{H}$ is a non-commutative $\mathbb{R}$-algebra.
Let be $0 \neq \alpha \in \mathbb{H}, \alpha = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$. We definie $\overline{\alpha} = a \cdot 1 - b \cdot i - c \cdot j - d \cdot k$.
$\Rightarrow N(\alpha) = \alpha \cdot \overline{\alpha} = a^2 + b^2 + c^2 + d^2 \neq 0$, since $\alpha \neq 0$
$\Rightarrow \alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}$
$\Rightarrow \mathbb{H}$ is a division algebra over $\mathbb{R}$.

Definition
Let A, B be K-algebras. A map $f : A \to B$ is called K-*algebra homomorphism*, if f is

1. K-liniear
2. ring homomorphism

Example
Take $A = \mathbb{H}, B = M_2(\mathbb{C})$.
We definie $f : \mathbb{H} \to M_2(\mathbb{C})$ by $f(a \cdot 1 + b \cdot i + c \cdot j + d \cdot k) = \begin{pmatrix} a+ib & c+id \\ -(c-id) & a-ib \end{pmatrix}$. This is an (injective) $\mathbb{R}$-algebra homomorphism.

Definition
Let A be a K-agebra. An additive subgroup $\mathfrak{a} \subseteq A$ is called *left ideal* (resp. *right-ideal*) in A, if $a \cdot x \in \mathfrak{a}$ for all $a \in A, x \in \mathfrak{a}$ (resp. $x \cdot a$). The subgroup $\mathfrak{a} \subseteq A$ is called a *two-sided ideal*, if it is at the same time left- and right-ideal.

Example
Let A be a K-algebra and $x \in A$.

1. $\mathfrak{a} = A \cdot x = \{a \cdot x | a \in A\}$ is a left-ideal.
2. $\mathfrak{b} = x \cdot A = \{x \cdot a | a \in A\}$ is a right-ideal.
3. $\mathfrak{c} = A \cdot x \cdot A = \{\sum a_j x b_j | a_j, b_j \in A\}$ is a 2-sided-ideal.

Definition
Let A be a K-algebra. A right ideal $\mathfrak{a} \subseteq A$ is called *minimal* if $\mathfrak{a}$ does not contain any other right ideals apart from (0) and $\mathfrak{a}$ itself.
A corresponding definition holds for left-ideals.

Definition
Let A be a K-algebra with 1. An abelian group P together with a map $P \times A \to P$, given by $(x, a) \mapsto x \cdot a$, is called an *A-right module*, if the following are satisfied

1. $x \cdot (a + b) = x \cdot a + x \cdot b$
2. $(x + y) \cdot a = x \cdot a + y \cdot a$
3. $(x \cdot a) \cdot b = x \cdot (a \cdot b)$
4. $x \cdot 1 = x$

for all $a, b \in A$ and $x, y \in P$.
Analogously, one defines *A-left modules*.

Definition
Let P, Q be A-right modules.
A map $f : P \to Q$ is called *A-right linear*, if it satisfies $f(x+y) = f(x)+f(y)$ and $f(x \cdot a) = f(x) \cdot a$ for all $x, y \in P, a \in A$.

Remark (Example)
Let A be a K-algebra and P an A-right module. We set $\mathrm{End}_A(P) = \{f : P \to P | f$ is right linear$\}$. For $f, g \in \mathrm{End}_A(P)$ and $\lambda \in K$ we have $(f + g)(x) = f(x) + g(x), (\lambda f)(x) = \lambda f(x)$ and $(f \circ g)(x) = f(g(x))$. This is obviously a K-algebra.

Theorem 5.1. (1) *Let A be a K-algebra.*
Then, the following holds:

1. *For any A-right module P and any natural number $n \in \mathbb{N}_{>0}$, we have the A-algebra isomorphism $M_n(\mathrm{End}_A(P)) \cong \mathrm{End}_A(P^n) = \mathrm{End}_A(\bigoplus_{k=1}^n P)$.*
2. *Let $(0) \neq \mathfrak{a} \subseteq A$ be a minimal right ideal. Then, $D = \mathrm{End}_A(\mathfrak{a})$ is a division algebra over K.*

3. *The map $\eta : A \to \mathrm{End}_A(A)$, given by $a \mapsto \eta(a), \eta(a)(x) = x \cdot a$ $(a, x \in A)$ is an isomorphism of K-algebras.*

Proof:

1. General remark: Let $P_1, ..., P_n$ be A-right modules. Then, one has the obvious A-right linear maps $i_j : P_j \to \bigoplus_{k=1}^n P_k$, defined by $x \mapsto (0, ..., 0, x, 0, ..., 0)$, and $p_k : \bigoplus_{r=1}^n P_r \to P_k$, defined by $(x_1, ..., x_n) \mapsto x_k$.

   One easily checks

   (a) $p_k \circ i_j = 0$ for $j \neq k$ and $p_j \circ i_j = \mathrm{id}_{P_j}$

   (b) $\sum_{j=1}^n i_j \circ p_j = \mathrm{id}_{\bigoplus_{k=1}^n P_k}$

   Let now be $P_1 = P_2 = ... = P_n = P$.

   We define $\alpha : \mathrm{End}_A(P^n) \to N_n(\mathrm{End}_A(P))$ by $f \mapsto (p_j \circ f \circ i_k)_{1 \leq j,k \leq n}$.

   $$P \xrightarrow{i_k} P^n \xrightarrow{f} P^n \xrightarrow{p_j} P \qquad (\alpha : P^n \to P^n)$$

   It is easy to see that α is K-linear. It remains to show that α is multiplicative.

   Let be $f, g \in \mathrm{End}_A(P^n)$.

   We have

   $$\begin{aligned}\alpha(f \circ g) &= (p_j \circ (f \circ g) \circ i_k)_{1 \leq j,k \leq n} = (p_j \circ f \circ (\textstyle\sum_{l=1}^n i_l \circ p_l) \circ g \circ i_k)_{1 \leq j,k \leq n} \\ &= (\textstyle\sum_{l=1}^n (p_j \circ f \circ i_l) \circ (p_l \circ g \circ i_k))_{1 \leq j,k \leq n} = \alpha(f) \cdot \alpha(g)\end{aligned}$$

   So α is a K-algebra homomorphism. Consider next $\beta : M_n(\mathrm{End}_A(P)) \to \mathrm{End}_A(P^n)$, defined by $(f_j, k)_{1 \leq j,k \leq n} \mapsto \sum_{j=1}^n \sum_{k=1}^n i_j \circ f_{j,k} \circ g_k$.

   We show that β is the inverse of α (i.e. $\alpha \circ \beta = \mathrm{id}_{M_n(\mathrm{End}_A(P))}$), hence α (and β) are K-algebra isomorphisms

   $$\begin{aligned}(\alpha \circ \beta)(f_{j,k}) &= \alpha(\textstyle\sum_j \sum_k i_j \circ f_{j,k} \circ p_k) = p_l \circ (\sum_j \sum_k i_j \circ f_{j,k} \circ p_k) \circ i_m \\ &= \textstyle\sum_j \sum_k (p_l \circ i_j) \circ f_{j,k} \circ (p_k \circ i_m) = (f_{j,k})\end{aligned}$$

   Now, we show that $\beta \circ \alpha = \mathrm{id}_{\mathrm{End}_A(P^n)}$:

   $(\beta \circ \alpha)(f) = \beta(p_j \circ f \circ i_k) = \sum_j \sum_k i_j \circ p_j \circ f \circ i_k \circ p_k = id_{P^n} \circ f \circ id_{P^n} = f$

2. Let be $0 \neq f \in D = \mathrm{End}_A(\mathfrak{a})$.

   ($f : \mathfrak{a} \to \mathfrak{a}$, non-trivial, A-right linear)

   $\ker(f), \mathrm{im}(f)$ are A-right ideals, contained in A.

   By minimality of $\mathfrak{a}$, we have $\ker(f) \in \{(0), \mathfrak{a}\}$. Since $f \neq 0$, we have $\ker(f) \neq \mathfrak{a}$.

   $\Rightarrow \ker(f) = (0) \Rightarrow f$ is injective.

   Analogously, $\mathrm{im}(f) \in \{(0), \mathfrak{a}\}$.

   $\Rightarrow f$ is surjective, since $f \neq 0$

   $\Rightarrow f$ is bijective.

   $\Rightarrow \exists f^{-1}$

3. We consider the map $\eta : A \to \mathrm{End}_A(A)$, defined by $\eta(a)(x) = x \cdot a$.

   Furthermore, we define $\vartheta : \mathrm{End}_A(A) \to A$ by $f \mapsto f(1)$.

   $\Rightarrow (\vartheta \circ \eta)(a) = \vartheta(\eta(a)) = \eta(a)(1) = 1 \cdot a = a, a \in A$

   $(\eta \circ \vartheta)(f) = \eta(f(1)) = f$, since $\eta(f(1))(a) = f(1) \cdot a = f(a)$ $\square$

5.2 Structure theorem for simple algebras

Definition
A K-algebra A is called simple, if the only two-sided ideals are (0) and A.

Goal
Let A be a simple K-algebra.
Then, there exists a division algebra D over K and $n \in \mathbb{N}_{>0}$ such that $A \cong M_n(D)$.

Lemma 5.1. (1) *Let D be a division algebra over K and $n \in \mathbb{N}_{>0}$. Then, the K-algebra $M_n(D)$ is simple.*

Proof:
Let $E_{j,k} \in M_n(D)$ be the elementary matrix having a 1 at the jth row in the kth column an 0s everywhere else. Let $M = (a_{j,k})_{1 \leq j,k \leq n} \in M_n(D)$ be any matrix.
Then, one easily computes: $E_{j,k} \cdot M \cdot E_{k,l} = a_{j,k} \cdot E_{l,l}$. (*)
Now, let $(0) \neq \mathfrak{a} \subseteq M_n(D)$ be a two-sided ideal. We have to show that $\mathfrak{a} = M_n(D)$.
Since $\mathfrak{a} \neq (0)$, there exists $M \in M_n(D), M \neq 0$, i.e. $M = (a_{j,k})_{1 \leq j,k \leq n}$ with some (j,k) such that $a_{j,k} \neq 0$.
If $a_{j,k} \in D$, wie have $a_{j,k}^{-1} \in D$, since D is a division algebra.
By (*), we have $E_{l,l} = \underbrace{a_{j,k}^{-1} \cdot E_{l,j}}_{\in M_n(D)} \cdot \underbrace{M}_{\in \mathfrak{a}} \cdot \underbrace{E_{k,l}}_{\in M_n(D)} \in \mathfrak{a}$.
$\Rightarrow 1 = E_{1,1} + ... + E_{n,n} \in \mathfrak{a} \Rightarrow \mathfrak{a} = M_n(D)$
$\Rightarrow M_n(D)$ is simple. □

Lemma 5.2. (2) *Let A be a simple, finite dimensional K-algebra and P a non-trivial A-right module with $\dim_K(P) < \infty$. Further, let $\mathfrak{a} \subseteq A$ be any minimal right-ideal, $\mathfrak{a} \neq (0)$.*
Then, there exists $n \in \mathbb{N}_{>0}$ such that $P \cong \bigoplus_{k=1}^n \mathfrak{a}$. (The isomorphism $\cong$ is a bijective, bilinear map.)

Proof:
Consider $A \cdot \mathfrak{a} = \{\sum_{\text{i, finite}} a_i x_i | a_i \in A, x_i \in \mathfrak{a}\}$. $A \cdot \mathfrak{a}$ is a two-sided ideal in the simple algebra A. Since $\mathfrak{a}$ is not trivial and A is simple, the two-sided ideal $A\mathfrak{a} \supseteq \mathfrak{a} \neq (0)$ is the whole algebra, i.e. $A\mathfrak{a} = A$.
$\Rightarrow P = PA = P(A\mathfrak{a}) = P\mathfrak{a}$
Since $\dim_K P < \infty$, we can choose a K-basis $\{v_1, ..., v_m\}$ for P such that
$P = \sum_{k=1}^m v_k K = (\sum_{k=1}^m v_k K)\mathfrak{a} = \sum_{k=1}^m v_k \mathfrak{a}$.
Now, choose a minimal set of elements $w_1, ..., w_n \in P$ such that $P = \sum_{k=1}^n w_k \mathfrak{a}$. In this way, we get a A-right linear map $\varphi : \bigoplus_{k=1}^n \mathfrak{a} \to P$, defined by $(x_1, ..., x_n) \mapsto \sum_{j=1}^n w_j x_j \in P$. By construction, φ is surjective. It remains to show that φ is also injective.
Let $(x_1, ..., x_n) \in \bigoplus_{k=1}^n \mathfrak{a}$ such that $\varphi(x_1, ..., x_n) = 0 \in P$, i.e. $\sum_{k=1}^n w_k x_k = 0$.
We have to show $x_1 = ... = x_n = 0$.
Assume that there exists $0 \neq x_i \in \mathfrak{a}$ for some i. W.l.o.g. let be $i = 1$.
$\Rightarrow 0 \neq x_1 \cdot A$ is a non-zero right-ideal in $\mathfrak{a}$.
Since $\mathfrak{a}$ is minimal, we must have $x_1 \cdot A = \mathfrak{a}$.
$\Rightarrow w_1 \cdot \mathfrak{a} = w_1 x_1 \cdot A \subseteq \sum_{k=2}^n w_k x_k A$, taking into account that $w_1 x_1 = -\sum_{k=2}^n w_k x_k$.
Since $x_k \cdot A \subseteq \mathfrak{a}$ for $k = 2, ..., n$, we get $w_1 \mathfrak{a} \subseteq \sum_{k=2}^n w_k \mathfrak{a}$. This contradicts the minimality of $w_1, ..., w_n$. □

Corollary 5.1. (3) *In a simple, finite dimensional K-algebra A all minimal A-right ideals $\mathfrak{a} \neq (0)$ are isomorphic.*

Proof:
Let $(0) \neq \mathfrak{a} \subseteq A$ and $(0) \neq \mathfrak{a}' \subseteq A$ be two minimal A-right ideals. We will show that $\mathfrak{a} \cong \mathfrak{a}'$.
By lemma 2, there is $n \in \mathbb{N}_{>0}$ and an A-right linear isomorphism $\varphi : \mathfrak{a}^n = \bigoplus_{k=1}^n \mathfrak{a} \to \mathfrak{a}'$. We are left to show that $n = 1$.

Let $\psi : \mathfrak{a} \to \mathfrak{a}^n$ (defined by $x \mapsto (x, 0, ..., 0)$ be the natural, injective A-right linear map. By composition, we get $\varphi \circ \psi : \mathfrak{a} \to \mathfrak{a}'$. Since $\mathfrak{a} \neq (0)$, we get $\psi(\mathfrak{a}) \subseteq \mathfrak{a}^n$ is non trivial.
$\Rightarrow (0) \neq \varphi(\psi(\mathfrak{a})) \subseteq \mathfrak{a}'$
Note: $\varphi(\psi(\mathfrak{a}))$ is a A-right ideal. By minimality of $\mathfrak{a}'$, we get $\varphi(\psi(\mathfrak{a})) = \mathfrak{a}'$.
We assume $n > 1$ and lead it to a contradiction. Obviously, for $n > 1$, we have $\psi(\mathfrak{a}) \neq \mathfrak{a}^n$. Now, we have the two equalities $\varphi(\psi(\mathfrak{a})) = \mathfrak{a}'$ and $\varphi(\mathfrak{a}^n) = \mathfrak{a}'$. This is a contradiction, since φ is injective.
$\Rightarrow n = 1 \Rightarrow \varphi : \mathfrak{a} \xrightarrow{\cong} \mathfrak{a}'$ □

Theorem 5.2. (4) *Let A be a simple, finite dimensional K-algebra. Then, there is exactly one $n \in \mathbb{N}_{>0}$ and, up to isomorphism of K-algebras, exactly one division algebra D over K such that $A \cong M_n(D)$ as K-algebras.*

Proof:

1. Existence

   Let $0 \neq \mathfrak{a} \subseteq A$ be any minimal A right ideal. By lemma 2, we have $n \in \mathbb{N}_{>0}$ and an (A-right linear) isomorphism $A \cong \mathfrak{a}^n$.

   Now, apply theorem 1 (from the previous subsection), parts 1 and 3, to get:

   $A \cong \mathrm{End}_A(A) \cong \mathrm{End}_A(\mathfrak{a}^n) \cong M_n(\mathrm{End}_A(\mathfrak{a}))$

   Now, since $\mathfrak{a} \neq (0)$ and $\mathfrak{a}$ is a minimal A-right ideal, theorem 1 shows that $D = \mathrm{End}_A(\mathfrak{a})$ is a division algebra over K.

2. Uniqueness

   Intermediate consideration
   Assume: $A = M_n(D), e = E_{1,1}$
   $\Rightarrow D \cong e \cdot A \cdot e \qquad (d \mapsto d \cdot e = e \cdot d \cdot e)$

   Claim 1: $e \cdot A \cdot e \cong \mathrm{End}_A(e \cdot A)$
   Proof:
   Let be $\varphi : e \cdot A \cdot e \to \mathrm{End}_A(e \cdot A)$ defined by $e \cdot a \cdot e \mapsto (x \mapsto e \cdot a \cdot e \cdot x)$. The images of φ, are obiviously A-right linear maps.
   φ is a K-algebra homomorphism: It's clear that φ is K-linear. Furthermore, we have $\varphi((e \cdot a \cdot e) \cdot (e \cdot b \cdot e))(x) = e \cdot a \cdot e \cdot e \cdot b \cdot e \cdot x = (\varphi(e \cdot a \cdot e) \circ \varphi(e \cdot b \cdot e))(x)$.
   Wie define $\psi : \mathrm{End}_A(e \cdot A) \to e \cdot A \cdot e$ by $f \mapsto f(e) = f(e^2) = f(e) \cdot e$ (we have $e = e^2$). Obviously, ψ is a K-algebra homomorphism.
   Finally, it's left to check that φ and ψ are inverses of each other.
   $\psi(\varphi(e \cdot a \cdot e)) = \psi(e \cdot a \cdot e \cdot \_) = e \cdot a \cdot e \cdot e = e \cdot a \cdot e$
   $\Rightarrow \psi \circ \varphi = \mathrm{id}_{e \cdot A \cdot e}$
   $\varphi(\psi(f))(x) = \varphi(f(e) \cdot e)(x) = f(e) \cdot e \cdot x = f(x)$
   $\Rightarrow \varphi \circ \psi = \mathrm{id}_{\mathrm{End}_A(e \cdot A)}$
   $\Rightarrow \varphi : e \cdot A \cdot e \xrightarrow{\cong} \mathrm{End}_A(e \cdot A)$

   Claim 2: A is a minimal A-right ideal.
   Proof:
   Let $(0) \neq \mathfrak{a} \subseteq A$ be some minimal A right ideal.
   We know by lemma 2: $e \cdot A \cong \mathfrak{a}^m$.
   $D \cong e \cdot A \cdot e \cong \mathrm{End}_A(e \cdot A) \cong \mathrm{End}_A(\mathfrak{a}^m) \cong M_m(\mathrm{End}_A(\mathfrak{a}))$
   Since D is division algebra, we have $m = 1$, i.e. $e \cdot A$ is minimal.

   Let's now prove the uniqueness as follows: Let $A = M_n(D)$ and $A' = M_{n'}(D')$ where $n, n' \in \mathbb{N}_{>0}$ and D, D' are division algebras over K. We show $A \cong A' \Rightarrow D = D' \wedge n = n'$.

   Let $\alpha : A \xrightarrow{\cong} A'$ denote the K-algebra isomorphism between A and A'.

   $\Rightarrow D \cong a \cdot A \cdot e \cong \mathrm{End}_A(e \cdot A) \cong \mathrm{End}_{A'}(\alpha(e \cdot A))$ where $\alpha(e \cdot A)$ is a minimal A'-right ideal.

$\Rightarrow D \cong \mathrm{End}_{A'}(\alpha(e \cdot A)) \cong \mathrm{End}_{A'}(e \cdot A') \cong a \cdot A' \cdot e \cong D'$

$\Rightarrow D \cong D'$

$\Rightarrow M_n(D) = A \cong A' = M_{n'}(D') \cong M_{n'}(D)$

By dimension reasons, we get $n = n'$. □

Lecture on 2008-02-14

5.3 Structure theorem for semi-simple K-algebras

Definition
Let K be a field and A a finite dimensional K-algebra. The radical $\mathcal{R}$ of A is defined as the union of all nilpotent, two-sided A-ideals.
Recall: $\mathfrak{a}$ is nilpotent, if there exists $n \in \mathbb{N}$ such that $\mathfrak{a}^n = (0)$.

Lemma 5.3. (1) *Let A be a finite dimensional K-algebra. Then, every nilpotent right ideal is contained in a nilpotent 2-sided ideal.*

Proof:
Remark: Let $\mathfrak{a}, \mathfrak{b}$ be two nilpotent right ideals, w.l.o.g. $\mathfrak{a}^n = (0) = \mathfrak{b}^n$ for some $n \in \mathbb{N}$. Then, the sum $\Rightarrow \mathfrak{a} + \mathfrak{b}$ is also a nilpotent right ideal. (We just consider $(\mathfrak{a} + \mathfrak{b})^{2n}$. This power is a sum of products of $\mathfrak{a}$ and $\mathfrak{b}$. Since $\mathfrak{a}$ or $\mathfrak{b}$ occur at least n times, every summand is (0), i.e. $(\mathfrak{a}+\mathfrak{b})^{2n} = (0)$.)
Claim: $A \cdot \mathfrak{a}$ is a left ideal, which is nilpotent.
We have $(A \cdot \mathfrak{a})^n = \prod_{k=1}^{n}(A \cdot \mathfrak{a}) = A \cdot \prod_{k=1}^{n-1}(a \cdot A) \cdot \mathfrak{a} = A \cdot \mathfrak{a}^{n-1} \cdot \mathfrak{a} = A \cdot \mathfrak{a}^n = A \cdot (0) = (0)$.
Consider finally the two-sided ideal $\mathfrak{a}' = \mathfrak{a} + A \cdot \mathfrak{a}$.
By the initial remark, $\mathfrak{a}'$ is also nilpotent and $\mathfrak{a}' \subseteq \mathfrak{a}$. □

Corollary 5.2. *Let A be a finite dimensional K-algebra.*
Then, the radical $\mathcal{R}$ of A is given by the union of all nilpotent right-ideals of A.

Proof:
By Lemma 1, we have the inclusion
$\bigcup_{\mathfrak{a} \text{ right ideal, nilpotent}} \mathfrak{a} \subseteq \bigcup_{\mathfrak{a}' \text{ 2-sided, nilpotent}} \mathfrak{a}' \subseteq \bigcup_{\mathfrak{a}'' \text{right iceal, nilpotent}} \mathfrak{a}''$
(All inclusionas are in fact equalities.) □

Definition
A finite dimensional K-algebra A is called semi-simple, if the radical $\mathcal{R}$ of A is simple, i.e. $\mathcal{R} = (0)$.

Remark
Let A be a simple algebra. Then, we have $\mathcal{R} = (0)$, hence A is semi-simple.
We will see that, in general, the converse is not true.

Remark
Let A be a finite dimensional K-algebra and $\mathcal{R}$ its radical. Then, one easily checks thet $\mathcal{R}$ is a 2-sided ideal. Hence, one can consider the factor algebra $A/\mathcal{R}$, which is a K-algebra.

Claim
The K-algebra $A/\mathcal{R}$ is semisimple. **Proof:**
Let $\overline{\mathfrak{a}} \subseteq A/\mathcal{R}$ be two-sided and nilpotent, i.e. $\overline{\mathfrak{a}}^n = (\overline{0})$.
$\Rightarrow \mathfrak{a}^n \subseteq \mathcal{R}$
$\Rightarrow \mathfrak{a}^n$ is two-sided and nilpotent.
$\Rightarrow \mathfrak{a}$ is 2-sided and nilpotent.
$\Rightarrow \mathfrak{a} \subseteq \mathcal{R}$
$\Rightarrow \overline{\mathfrak{a}} = (\overline{0})$ □

Classification perspective

0. A is a finite dimensional K-algebra
1. Take the radical $\mathcal{R}$ of A
2. $A_1 = A/\mathcal{R}$ is a semi-simple K-algebra
3. Classify semi-simple K-algebra in terms of simple K-algebras
4. Apply theorem 4 above

Definition (idempotent elements)
An element e satisfying $e^2 = e$ is called *idempotent*.

Lemma 5.4. (3) *Let A be a finite dimensional, semi-simpel K-algebra and $\mathfrak{a} \neq (0)$ a minimal right-ideal in A.*
Then, there is an element $e \in \mathfrak{a}$ such that $e^2 = e$ (i.e. e is idempotent) and $\mathfrak{a} = e \cdot A$.

Proof:
We have $\exists a \in \mathfrak{a} : a \cdot \mathfrak{a} \neq (0)$. (Otherwise we had $\mathfrak{a}^2 = (0)$, i.e. $\mathfrak{a}$ is nilpotent. Then, $\mathfrak{a} + A\mathfrak{a}$ would be a non-trivial, two-sided, nilpotent ideal in A, what contradicted the semi-simplicity of A.)
Now, consider the set $a \cdot \mathfrak{a} = \{a \cdot x | x \in \mathfrak{a}\} \subseteq \mathfrak{a} \cdot A = \mathfrak{a}$. Obviously, $a \cdot \mathfrak{a}$ is an A-right ideal. Since $a \cdot \mathfrak{a} \neq (0)$ and $\mathfrak{a}$ is minimal, we must have $a \cdot \mathfrak{a} = \mathfrak{a}$.
$\Rightarrow \exists e \neq 0 \in \mathfrak{a} : a \cdot e = a$
$\Rightarrow (a \cdot (e^2 - e) = \underbrace{(a \cdot e - a)}_{=0} \cdot e = 0$
$\Rightarrow e^2 - e \in \mathfrak{b} = \{x \in \mathfrak{a} | a \cdot x = 0\}$
$\Rightarrow \mathfrak{b}$ is an A-right ideal and $\mathfrak{b} \subseteq \mathfrak{a}$.
$\Rightarrow \mathfrak{b} = (0)$ or $\mathfrak{b} = \mathfrak{a}$
$\Rightarrow \mathfrak{b} = (0)$, since $\mathfrak{b} \neq \mathfrak{a}$ (we have $e \notin \mathfrak{b}$).
$\Rightarrow e^2 - e \in \mathfrak{b} = (0) \Rightarrow e^2 - e = 0 \Rightarrow e^2 = e$
Finally, note:
$a \cdot e = a \neq 0 \Rightarrow e \cdot A \subseteq \mathfrak{a}$ is a right ideal and can not be trivial, since $e \cdot A \ni a \neq 0$.
$\Rightarrow a \cdot A = \mathfrak{a}$, since $\mathfrak{a}$ is minimal. □

Lemma 5.5. (4) *Let A be finite dimensional, semi-simple K-algebra, $(0) \neq \mathfrak{a}$ a right ideal in A and $0 \neq e \in \mathfrak{a}$ idempotent, i.e. $e^2 = e$.*
Then, $\mathfrak{a} = e \cdot A \oplus \mathrm{Ann}_{\mathfrak{a}}(e)$, where $\mathrm{Ann}_{\mathfrak{a}}(e) = \{x \in \mathfrak{a} | e \cdot x = 0\}$.

Proof:
We have to show $\mathfrak{a} = e \cdot A + \mathrm{Ann}_{\mathfrak{a}}(e)$ and $e \cdot A \cap \mathrm{Ann}_{\mathfrak{a}}(e) = \{0\}$.

1. $\mathfrak{a} = e \cdot A + \mathrm{Ann}_{\mathfrak{a}}(e)$:

   Let be $a \in \mathfrak{a}$.

   $\Rightarrow e \cdot (a - e \cdot a) = e \cdot a - e^2 \cdot a = e \cdot a - e \cdot a = 0$

   $\Rightarrow a - e \cdot a \in \mathrm{Ann}_{\mathfrak{a}}(e)$

   $a = \underbrace{e \cdot a}_{\in e \cdot A} + \underbrace{(a - e \cdot a)}_{\in \mathrm{Ann}_{\mathfrak{a}}(e)}$

   $\Rightarrow \mathfrak{a} \subseteq e \cdot A + \mathrm{Ann}_{\mathfrak{a}}(e) \subseteq \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$

   $\Rightarrow \mathfrak{a} = e \cdot A + \mathrm{Ann}_{\mathfrak{a}}(e)$

2. $e \cdot A \cap \mathrm{Ann}_{\mathfrak{a}}(e) = \{0\}$:

   Let be $x \in e \cdot A \cap \mathrm{Ann}_{\mathfrak{a}}(e)$. We want to show that $x = 0$.

   $x \in e \cdot A \Rightarrow x = e \cdot a, a \in A$

   $x \in \mathrm{Ann}_{\mathfrak{a}}(A) \Rightarrow e \cdot x = 0$

   $\Rightarrow 0 = e \cdot x = e(e \cdot a) = e^2 \cdot a = e \cdot a = x$

   $\Rightarrow x = 0 \Rightarrow e \cdot A \cap \mathrm{Ann}_{\mathfrak{a}}(e) = \{0\}$

$\Rightarrow \mathfrak{a} = e \cdot A \oplus \mathrm{Ann}_{\mathfrak{a}}(e)$ □

Proposition 5.1. (5) *Let be A a finite dimensional, semi-simple K-algebra and $(0) \neq \mathfrak{a}$ a right ideal in A.*
Then, we have $\mathfrak{a} = \bigoplus_{j=1}^{n} \mathfrak{a}_j$, where all $\mathfrak{a}_j \neq (0)$ are minimal right ideals in A.

Proof:
Since A is finite dimensional, the subvectorspace $\mathfrak{a}$ is also finite dimensional over K, hence there exists a minimal, non-trivial right ideal $\mathfrak{a}_1 \subseteq \mathfrak{a}$.
Applying lemma 3 to $\mathfrak{a}_1$ gives $0 \neq e_1 \in \mathfrak{a}_1 : e_1^2 = e_1$ and $\mathfrak{a}_1 = e_1 \cdot A$.
Applying Lemma 4 to $\mathfrak{a}$, we get $\mathfrak{a} = \underbrace{e_1 \cdot A}_{=\mathfrak{a}_1} \oplus \underbrace{\mathrm{Ann}_{\mathfrak{a}}(e_1)}_{=\mathfrak{b}_1}$, where $\mathfrak{b}_1 \subseteq \mathfrak{a}$ is a right ideal.
$\Rightarrow \mathfrak{a} = \mathfrak{a}_1 \oplus \mathfrak{b}_1$ where $\mathfrak{a}_1 \neq (0)$ is a minimal right ideal.
Now, there are two possibilities:

1. $\mathfrak{b}_1 = (0)$

   In this case, we are done.

2. $\mathfrak{b}_1 \neq (0)$

   If $\mathfrak{b}_1$ is minimal, we are done, too.

   Let's consider the case that $\mathfrak{b}_1$ is not minimal.

   We handle $\mathfrak{b}_1$ as $\mathfrak{a}$ at the beginning.

   $\Rightarrow \mathfrak{b}_1 = \mathfrak{a}_2 \oplus \mathfrak{b}_2$, where $(0) \neq \mathfrak{a}_2$ is minimal right ideal in A and $\mathfrak{b}_2$ is a right ideal in A.

   We continue this way and get a sequence $\mathfrak{a}_1, \mathfrak{a}_2, ...$ Since the dimension of $\mathfrak{b}_j$ is strictly decreasing, the process has eventually to stop because of dimension reasons.

$\Rightarrow \mathfrak{a} = \bigoplus_{j=1}^{n} \mathfrak{a}_j$, where $\mathfrak{a}_j \neq (0)$ and $\mathfrak{a}_j$ is a minimal right-ideal. □

Theorem 5.3. (6) *Let A be a finite dimensional, semi-simple K-algebra.*
Then, A is a direct sum of (finite dimensional) simple K-algebras, i.e. $A = \bigoplus_{j=1}^{s} A_j$ where the A_j are finite dimensional, simple K-algebras.

Proof:
Apply proposition 5 to $\mathfrak{a} = A$ to get $A \cong \bigoplus_{j=1}^{s} \mathfrak{a}_j^{n_j}$, where $\mathfrak{a}_1, ..., \mathfrak{a}_s$ are pairwise non-isomorphic, non-trivial, minimal right ideals in A and $n_1, ..., n_s \in \mathbb{N}_{>0}$.
Note: Since the $\mathfrak{a}_j$ are minimal, for the set of right linear maps holds $\mathrm{Hom}_A(\mathfrak{a}_j, \mathfrak{a}_k) = \{0\}$ for $j \neq k$.
We put $P_j = \mathfrak{a}_j^{n_j}$, which is an A-right-module.
Claim: $\mathrm{End}_A(\bigoplus_{j=1}^{s} P_j) \cong \bigoplus_{j=1}^{s} \mathrm{End}_A(P_j)$
Assume this for the moment.
We get

$$A \cong \mathrm{End}_A(A) \cong \mathrm{End}_A(\bigoplus_{j=1}^{s} P_j) \cong \bigoplus_{j=1}^{s} \mathrm{End}_A(P_j) \cong \bigoplus_{j=1}^{s} \mathrm{End}_A(\mathfrak{a}_j^{n_j}) \cong \bigoplus_{j=1}^{s} M_{n_j}(\mathrm{End}_A(\mathfrak{a}_j))$$

Now, let's show the claim:

We define a K-linear map

$$\alpha : \mathrm{End}_A(\bigoplus_{j=1}^{s} P_j) \to \bigoplus_{j=1}^{s} \mathrm{End}_A(P_j)$$

given by

$$f \mapsto (p_1 \circ f \circ i_1, ..., p_s \circ f \circ i_s)$$

Remember the maps

$$i_j : P_j \to \bigoplus_{r=1} sP_r \quad (p \mapsto (0, ..., p, ..., 0))$$

and

$$p_k : \bigoplus_{r=1} sP_r \to P_k \quad ((p_1, ..., p_s) \mapsto p_k)$$

We show $\alpha(f \circ g) = \alpha(f) \circ \alpha(g)$.
For this note $g \circ i_j = \sum_{k=1}^{s} i_k \circ p_k \circ g \circ i_j = \sum_{k=1}^{s} i_k \circ (\underbrace{p_k \circ g \circ i_j}_{=0, \text{ if } k \neq j}) = i_j \circ p_j \circ g \circ i_j$. Furthermore, we have $p_j \circ (f \circ g) \circ i_j = p_j \circ f \circ (g \circ i_j) = (p_j \circ f \circ i_j) \circ (p_j \circ g \circ i_j)$. This shows that α is a K-algebra homomorphism.
Now, we construct the potential inverse map $\beta : \bigoplus_{j=1}^{s} \mathrm{End}_A(P_j) \to \mathrm{End}_A(\bigoplus_{j=1}^{s} P_j)$, which is given by $(f_1, ..., f_s) \mapsto \sum_{k=1}^{s} i_k \circ f_k \circ p_k$. β is K-linear and well-defined.
We check easily that $\alpha \circ \beta = \mathrm{id}$. Finally, it's left to show that $\beta \circ \alpha = \mathrm{id}$.
We have
$\beta(\alpha(f)) = \beta(p_1 \circ f \circ i_1, ..., p_s \circ f \circ i_s) = \sum_{k=1}^{s} i_k \circ (p_k \circ f \circ i_k) \circ p_k$
$= (\sum_{k=1}^{s} i_k \circ p_k) \circ f \circ (\sum_{k=1}^{s} i_k \circ p_k) = f$
$\Rightarrow \alpha$ and β are inverse to each other. □

Classification program
Let A be a finite dimensional K-algebra. We take $A' = A/\mathcal{R}$ as a finite dimensional, semi-simple K-algebra.
$\Rightarrow A' = \bigoplus_{j=1}^{s} A_j$ where the A_j are finite dimensional, simple K-algebras.
$\Rightarrow A_j \cong M_{n_j}(D_j)$ where the D_j are division algebras over K and $n_j \in \mathbb{N}_{>0}$.
$\Rightarrow A/\mathcal{R} \cong \bigoplus_{j=1}^{s} M_{n_j}(D_j)$

Index