Commutative Algebra

Prof Sanjay Amrutiya[1]

Organized Results

complied by

Sarthak[2]

April 2023

[1]samrutiya@iitgn.ac.in
[2]vijaysarthak@iitgn.ac.in

Contents

Chapter I

Commutative rings with identity

1 Exercising Zorn's lemma

January 12, 2023

Theorem 1.1 (Maximal ideals)**.** *Let A be a ring with identity and $\mathfrak{a}$ be a proper ideal. Then there exists a maximal ideal $\mathfrak{m}$ that contains $\mathfrak{a}$.*

Corollary 1.2. *Any ring A is the disjoint union of the sets A^* (the units of A) and*[1] $\bigcup \operatorname{MaxSpec} A$.

Theorem 1.3 (Prime ideals)**.** *Let A be a commutative ring, $\emptyset \neq S \subseteq A$ be multiplicative, and $\mathfrak{a}$ be an ideal such that $\mathfrak{a} \cap S = \emptyset$. Then $\mathfrak{a}$ is contained in some prime ideal that lies outside S.*

Theorem 1.4 (Minimal prime ideals)**.** *Let A be a ring, $\mathfrak{p}$ be a prime ideal and $S \subseteq \mathfrak{p}$. Then there exists a minimal prime ideal $\mathfrak{q}$ such that $X \subseteq \mathfrak{q} \subseteq \mathfrak{p}$.*

2 Simple facts

January 29, 2023

Convention. *Throughout the rest of the document (except of appendices), unless stated otherwise, A will denote a commutative ring with unity, and Fraktur letters will denote the ideals. "$A \neq 0$" will mean that A is a nonzero ring.*

[1] See Definition 3.2.

Proposition 2.1. *Primes are irreducible in an integral domain.*

Proposition 2.2. *Maximal ideals are prime.*

Proposition 2.3 (Characterizing fields)**.** *For $A \neq 0$, the following are equivalent:*

(i) A is a field.

(ii) The only ideals of A are (0) and (1).

(iii) Any homomorphism from A that maps 1 to some nonzero is injective.

Proposition 2.4. *For ideals $\mathfrak{p}$ and $\mathfrak{m}$, the following hold:*

(i) $\mathfrak{p}$ is prime $\iff$ $A/\mathfrak{p}$ is an integral domain.

(ii) $\mathfrak{m}$ is maximal $\iff$ $A/\mathfrak{m}$ is a field.

3 The different radicals

January 12, 2023

Remark. *Most of the results included will use AC, and we'll not bother to explicitly state when it is used.*

Definition 3.1 (Nilradical)**.** We define

$$\operatorname{Nil} A := \{\text{nilpotents in } A\}.$$

Definition 3.2 (Spectra of a ring)**.** We define[2]

$$\begin{aligned} \operatorname{Spec} A &:= \{\text{prime ideals of } A\}, \text{ and} \\ \operatorname{MaxSpec} A &:= \{\text{maximal ideals of } A\}. \end{aligned}$$

Proposition 3.3. *For[3] $A \neq 0$, we have*

$$\operatorname{Nil} A = \bigcap \operatorname{Spec} A = \bigcap \{\textit{minimal prime ideals}\}.$$

Proposition 3.4. *If $A \neq 0$ has no nonzero zero divisors or nilpotents, then there exist more than one minimal prime ideals.*

[2] When "spectrum" is used, we usually see $\operatorname{Spec} A$ under the Zariski topology.

[3] $A \neq 0$ ensures that $\operatorname{Spec} A, \operatorname{MaxSpec} A \neq \emptyset$.

Definition 3.5 (The Jacobson radical)**.** For $A \neq 0$, we define

$$\operatorname{Jac} A := \bigcap \operatorname{MaxSpec} A.$$

Proposition 3.6 (Characterizing Jacobson)**.** *Let $A \neq 0$. Then*

$$\operatorname{Jac} A = \{x \in A : 1 - xy \text{ is a unit for all } y \in A\}.$$

Definition 3.7 (Radical of an ideal)**.** For an ideal $\mathfrak{a}$, we define

$$\operatorname{Rad} \mathfrak{a} := \{x \in A : x^n \in \mathfrak{a} \text{ for some } n \geq 1\}.$$

Proposition 3.8. *For any ring homomorphism, we have*

$$\operatorname{Rad}(\ker \phi) = \phi^{-1}\big(\operatorname{Nil}(\phi(A))\big)$$

Corollary 3.9. *For a proper ideal $\mathfrak{a}$, we have*

$$\operatorname{Rad} \mathfrak{a} = \bigcap \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \supseteq \mathfrak{a}\}.$$

Proposition 3.10.

$$\begin{aligned}
\operatorname{Rad}(\operatorname{Rad} \mathfrak{a}) &= \operatorname{Rad} \mathfrak{a} \\
\operatorname{Rad}(\mathfrak{a} \cdot \mathfrak{b}) &= \operatorname{Rad}(\mathfrak{a} \cap \mathfrak{b}) = \operatorname{Rad} \mathfrak{a} \cap \operatorname{Rad} \mathfrak{b} \\
\operatorname{Rad}(\mathfrak{a} + \mathfrak{b}) &= \operatorname{Rad}(\operatorname{Rad} \mathfrak{a} + \operatorname{Rad} \mathfrak{b}) \\
\operatorname{Rad}(\mathfrak{p}^n) &= \mathfrak{p} \qquad \text{for prime } \mathfrak{p} \text{ and } n \geq 1
\end{aligned}$$

Proposition 3.11 (Characterizing locality)**.** *The following are equivalent:*

(i) A *is local.*

(ii) $A \setminus A^*$ *is an ideal.*

(iii) $1 + \mathfrak{m} \subseteq A^*$ *for some maximal* $\mathfrak{m}$.

(iv) $\{a, 1 - a\}$ *contains a unit for every* $a \in A$.

Definition 3.12 (Coprime)**.** Ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called coprime or comaximal iff $\mathfrak{a} + \mathfrak{b} = (1)$.

Proposition 3.13 (Chinese remainder)**.** *Let $\mathfrak{a}_1, \dots \mathfrak{a}_n$ $(n \geq 1)$ be ideals of A and define $\phi \colon A \to \prod_i A/\mathfrak{a}_i$ by*

$$a \mapsto (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n).$$

Now, the following hold:

(i) ϕ *is surjective* $\iff$ $\mathfrak{a}_i$*'s are pairwise coprime.*

(ii) ϕ *is injective* $\iff$ $\bigcap_i \mathfrak{a}_i = (0)$.

(iii) $\mathfrak{a}_i$*'s are pairwise coprime* $\implies$ $\bigcap_i \mathfrak{a}_i = \odot_i \mathfrak{a}_i$.[4]

[4] This is a generalization of the last part of Proposition 1.4.

Proposition 3.14. *Let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *be prime* ($n \geq 1$) *with* $\mathfrak{a} \subseteq \bigcup_i \mathfrak{p}_i$. *Then* $\mathfrak{a} \subseteq$ *some* $\mathfrak{p}_i$.

Proposition 3.15. *Let* $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i$ ($n \geq 1$) *be prime. Then* $\mathfrak{p} \supseteq$ *some* $\mathfrak{a}_i$.

Further, the above also holds with $\supseteq$ *replaced with* $=$.

Proposition 3.16 (Idempotents decompose the rings)**.** *Let* A *be a commutative ring with identity and* $a \in A$. *Then the following are equivalent:*

(i) a *is idempotent.*

(ii) $1 - a$ *is idempotent.*

(iii) $A = aA \oplus (1-a)A$.[5]

---

[5] See Definition 1.6.

Chapter II

Modules

1 Basics

February 17, 2023

Definition 1.1 (Modules, submodules, module homomorphisms)**.** See Definition 1.1. Submodules are defined obviously. Homomorphisms between two modules over a common ring are defined in the obvious sense.

Remark. *To emphasize that the algebraic object is an A-module, we'll use use "A-module homomorphism" or "A-linear homomorphism".*

Example 1.2.

(i) Any abelian group is a $\mathbb{Z}$-module.

(ii) A is an A-module.

(iii) Submodules of a ring are precisely its ideals.

Lemma 1.3 (Choices for scalar multiplications)**.** *Let M be an abelian group and R be any ring. Then there exists a one-to-one correspondence:*

$$\left\{\begin{matrix} \textit{scalar multiplications } A \times M \to M \\ \textit{that make } M \textit{ an } A\textit{-module} \end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix} \textit{ring homomorphisms} \\ A \to \mathrm{End}(M) \end{matrix}\right\}$$

Proposition 1.4 (Submodules and homomorphisms)**.**

(i) Characterization of submodules (when the ring has identity).

(ii) Transitivity of "being a submodule".

(iii) Sums and intersections of submodules are submodules.

(iv) ker *and* im *of homomorphisms are submodules.*

(v) The injection of a submodule into the parent submodule is a homomorphism.

(vi) Submodules preserved in both directions under homomorphisms.

(vii) For a homomorphism, injectivity $\iff$ $\ker = 0$.

Convention. *Throughout the document (except in the appendices), M and N will stand for generic A-modules.*

Proposition 1.5 (Quotient of modules)**.** *Let N be a submodule of M. Then the quotient group M/N forms an A-module under the following well-defined operations:*

$$\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$$
$$a\,\overline{m} = \overline{am}$$

Proposition 1.6. *We have the analogues of correspondence and all the three isomorphism theorems.*

Definition 1.7 (Independence, spans, bases, free modules)**.** Defined in the obvious way.

Modules that have a basis are called free.

Proposition 1.8 (Characterizing spanning and independent sets)**.** *Let $S \subseteq M$. Define $\phi \colon A^{[S]} \to M$ via*[1]

$$(a_s) \mapsto \sum_s a_s\, s.$$

Then the following hold:

(i) ϕ is a homomorphism.

(ii) S is independent $\iff$ ϕ is injective.

(iii) S spans M $\iff$ ϕ is surjective.

Definition 1.9 (Direct sums and direct products)**.** Given A-modules $\{M_\lambda\}_{\lambda\in\Lambda}$, the sets

$$\oplus_{\lambda\in\Lambda} M_\lambda \quad \text{and} \quad \prod_{\lambda\in\Lambda} M_\lambda$$

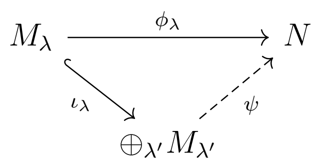
(defined usually) form A-modules via pointwise operations.[2]

[1] Since direct sum, ϕ is well-defined.

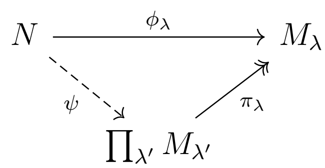
[2] Note that the former is a submodule of the latter.

Proposition 1.10 (The universal property of direct sums and direct products)**.** *Let M_λ's be A-modules for $\lambda \in \Lambda$. Then the following universal properties respectively characterize*[3] $\left(\oplus_\lambda A_\lambda, (\iota_\lambda)\right)$ *and* $\left(\prod_\lambda A_\lambda, (\pi_\lambda)\right)$ *up to (unique) isomorphisms:*

(i) Given any A-module N and homomorphisms $\phi_\lambda \colon M_\lambda \to N$, there exists a unique homomorphism $\psi \colon \oplus_\lambda M_\lambda \to N$ such that each ϕ_λ factors through[4] *ι_λ:*



(ii) Given any A-module N and homomorphisms $\phi_\lambda \colon N \to M_\lambda$, there exists a unique homomorphism $\psi \colon N \to \prod_\lambda M_\lambda$ such that each ϕ_λ factors through π_λ:



Notation. *Sometimes, the unique functions ψ's above are denoted by $\oplus_\lambda \phi_\lambda$ and $\prod_\lambda \phi_\lambda$.*

Definition 1.11 (Ideal times a module)**.** We define[5]

$$\mathfrak{a} \cdot M := \sum_{i \in \mathbb{N}} \mathfrak{a} M.$$

Lemma 1.12. *For any $a \in A$, we have*

$$aM = (a) \cdot M.$$

Definition 1.13 ($(N : L)$ and annihilators)**.** For submodules N, L of M, we define

$$(N : L) := \{a \in A : N \supseteq aL\}.$$

We define

$$\mathrm{Ann}(M) := (0 : M).$$

---

[3] ι_λ is the injection $A_\lambda \hookrightarrow \oplus_\lambda A_\lambda$, and π_λ is the projection $\prod_\lambda A_\lambda \twoheadrightarrow A_\lambda$.
[4] That is, the diagram commutes.
[5] Note how $\mathfrak{a} \cdot \mathfrak{b} = \sum_{i \in \mathbb{N}} \mathfrak{a}\mathfrak{b}$.

Proposition 1.14 (A-module as an $A/\mathfrak{a}$-module)**.** *Let $\mathfrak{a} \subseteq \operatorname{Ann}(M)$. Then M forms an $A/\mathfrak{a}$ with the following well-defined scalar multiplication:*

$$\overline{a}\, m = am.$$

Lemma 1.15. *$A/\mathfrak{a}$ as the "ring over itself" module is the same as the module constructed by these steps:*

$$A \text{ over } A \longrightarrow A/\mathfrak{a} \text{ over } A \longrightarrow A/\mathfrak{a} \text{ over } A/\mathfrak{a}.$$

2 Cayley-Hamilton and Nakayama

February 17, 2023

Theorem 2.1 (Generalized Cayley-Hamilton)**.** *Let $\{m_1, \ldots, m_k\}$ generate the M ($k \geq 1$). Let $\phi\colon M \to M$ be a homomorphism and $P \in A^{k\times k}$ such that*

$$\phi(m_j) = \sum_{i=1}^{k} P_{i,j}\, m_i.$$

Let $\chi \in A[x]$ be the characteristic polynomial of P. Then

$$\chi(\phi) = 0.$$

Corollary 2.2. *Let M be generated by $k \geq 0$ elements and $\phi\colon M \to M$ be a homomorphism such that $\phi(M) \subseteq \mathfrak{a} \cdot M$. Then there exist $a_0, \ldots, a_{k-1} \in \mathfrak{a}$ such that*

$$\phi^k + a_{k-1}\, \phi^{k-1} + \cdots + a_0\, I = 0.$$

Theorem 2.3 (Nakayama's lemma)**.** *Let M be finitely generated.*

Version I *Let $\mathfrak{a} \cdot M = M$. Then there exists an $a \in A$ such that*

$$a \equiv 1_A \pmod{\mathfrak{a}} \quad \text{and} \quad aM = 0.$$

Version II $\mathfrak{a} \subseteq \operatorname{Jac}(A)$ *and* $\mathfrak{a} \cdot M = M \implies M = 0$.

Version III *Let $\mathfrak{a} \subseteq \operatorname{Jac}(A)$ and N be a submodule of M such that $\mathfrak{a} \cdot M + N = M$. Then $N = M$.*[6]

Proposition 2.4 (Pulling a spanning set from the quotient vector space to the module)**.** *Let $\mathfrak{m}$ be maximal in A. Then the following hold:*

(i) *$M/(\mathfrak{m} \cdot M)$ is a vector space over $A/\mathfrak{m}$.*

(ii) *If $(A, \mathfrak{m})$ is local and finitely many $\overline{m_i}$'s ($m_i \in M$) span the vector space $M/(\mathfrak{m} \cdot M)$ (over $A/\mathfrak{m}$), then m_i's span M (over A).*

[6] Version II becomes a special case of Version III by putting $N = 0$.

3 Tensor products of modules

February 20, 2023

Definition 3.1 (Multilinear maps)**.** Let $\{M_\lambda\}$ and N be A-modules. Then a set theoretic function $\mathscr{f} \colon \prod_\lambda M_\lambda \to N$ is called A-multilinear iff for each λ_0 and each $(m_{\lambda \neq \lambda_0}) \in \prod_{\lambda \neq \lambda_0} M_\lambda$, the induced function $M_{\lambda_0} \to N$ given by

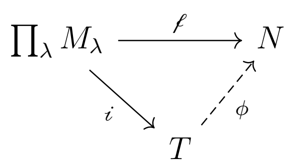
$$\tilde{m} \mapsto \mathscr{f}\left(\begin{smallmatrix} \tilde{m}, & \lambda = \lambda_0 \\ m_\lambda, & \lambda \neq \lambda_0 \end{smallmatrix} \right)$$

is a homomorphism.

Convention. *We'll use calligraphic font for multilinear maps.*

Definition 3.2 (Tensor products)**.** Let $\{M_\lambda\}$ be A-modules. Then an A-module T together with a multilinear map $\mathscr{i} \colon \prod_\lambda M_\lambda \to T$, denoted $(T, \mathscr{i})$ is called a tensor product of M_λ's iff the following universal property holds:

Any multilinear map $\mathscr{f} \colon \prod_\lambda M_\lambda \to N$ (N any A-module) factors through $\mathscr{i}$ via a unique homomorphism $\phi \colon T \to N$.



Remark. *Generally, just T is called the tensor product.*

Proposition 3.3. *Any two tensor products of a family of modules are unique up to a unique isomorphism.*[7]

Notation. *This allows us to denote the (module of the) tensor product (up to (the unique) isomorphism) by $\otimes_i M_i$.*

[7] More precisely, given $(T_1, \mathscr{i}_1)$ and $(T_2, \mathscr{i}_2)$, there exists a unique isomorphism $T_1 \to T_2$.

Lemma 3.4 (Existence of tensor products)**.** *Let $\{M_\lambda\}$ be A-modules. Let P be the submodule of $A^{[\prod_\lambda M_\lambda]}$ generated by the following elements:*

$$e\left(\begin{smallmatrix} n_1, & \lambda=\lambda_0 \\ m_\lambda, & \lambda\neq\lambda_0 \end{smallmatrix}\right) + e\left(\begin{smallmatrix} n_2, & \lambda=\lambda_0 \\ m_\lambda, & \lambda\neq\lambda_0 \end{smallmatrix}\right) - e\left(\begin{smallmatrix} n_1+n_2, & \lambda=\lambda_0 \\ m_\lambda, & \lambda\neq\lambda_0 \end{smallmatrix}\right)$$

$$a\,e\left(\begin{smallmatrix} n, & \lambda=\lambda_0 \\ m_\lambda, & \lambda\neq\lambda_0 \end{smallmatrix}\right) - e\left(\begin{smallmatrix} an, & \lambda=\lambda_0 \\ m_\lambda, & \lambda\neq\lambda_0 \end{smallmatrix}\right)$$

Here, $(m_\lambda) \in \prod_{\lambda\neq\lambda_0} M_\lambda$; $n, n_1, n_2 \in M_{\lambda_0}$; and, $a \in A$.

Write $T := A^{[\prod_\lambda M_\lambda]}$ and let $\imath\colon \prod_\lambda M_\lambda \to T$ be given by[8]

$$(m_\lambda) \mapsto \overline{e_{(m_\lambda)}}.$$

Then $(T, \imath)$ is a tensor product of M_λ's.

Definition 3.5 (Simple tensors)**.** For a given tensor product $(T, \imath)$ of modules M_λ's, we set

$$\otimes_\lambda m_\lambda := \imath((m_\lambda)).$$

Remark. *Strictly speaking, $\imath$ must've been mentioned in the notation.*

Remark. *Sometimes, when modules can be seen as being over several rings, we might specify the ring A over which the tensor product is being taken by writing $\otimes_A$.*

Corollary 3.6. *(i) $m \otimes n = 0 \implies$ every bilinear map on $M \times N$ vanishes at (m, n).*

(ii) $M \otimes N = 0 \implies$ the only bilinear map on $M \times N$ are zero maps.[9]

(iii) If G is an abelian group with each element having finite order, then $G \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Proposition 3.7. *The tensor product is generated by simple tensors.*

Remark. *Not all tensors are simple: Consider $e \otimes e + f \otimes f \in M \otimes M$ where $\{e, f\}$ form a basis of M.*

Proposition 3.8 (Being a basis is preserved by $\_\otimes\_$)**.** *If $\{m_i\}$'s and $\{n_j\}$'s respectively form bases for M and N, Then $\{m_i \otimes n_j\}$'s form a basis for $M \times N$.*

[8] Note that we are using two notations for the same thing: $e\,\square$ and $e_\square$.

[9] Map*s*, not map (since codomain can vary).

Corollary 3.9. *Over A, we have*

$$A^m \otimes A^n \cong A^{m\times n}.$$

Proposition 3.10. *We have*

$$A/\mathfrak{a} \otimes A/\mathfrak{b} \cong A/(\mathfrak{a}+\mathfrak{b})$$

with an isomorphism given by

$$\overline{a} \otimes \overline{b} \mapsto \overline{ab}.$$

Proposition 3.11. *The kernel of the homomorphism $A \mapsto A/\mathfrak{a} \otimes A/\mathfrak{b}$ given by*

$$a \mapsto a(\overline{1} \otimes \overline{1})$$

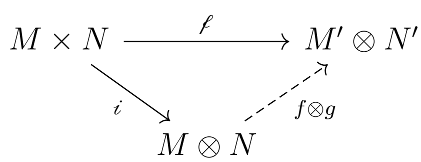
is $\mathfrak{a}+\mathfrak{b}$.

Remark. *Contrast this with the kernel $\mathfrak{a} \cap \mathfrak{b}$ of the map $A \to A/\mathfrak{a} \times A/\mathfrak{b}$ given by $a \mapsto (\overline{a}, \overline{a}) = a(\overline{1}, \overline{1})$.*

Proposition 3.12 ($\_ \otimes \_$ as a covariant bifunctor $\mathsf{Mod}_A \times \mathsf{Mod}_A \to \mathsf{Mod}_A$)**.** *Let $f\colon M \to M'$ and $g\colon N \to N'$ be homomorphisms. Then the function $\not{f}\colon M \times N \to M' \otimes N'$ defined by*

$$(m,n) \mapsto f(m) \otimes g(n)$$

is bilinear and we define $f \otimes g$ to be the unique homomorphism through which $\not{f}$ factors:



$f \otimes g$ is characterized by [10]

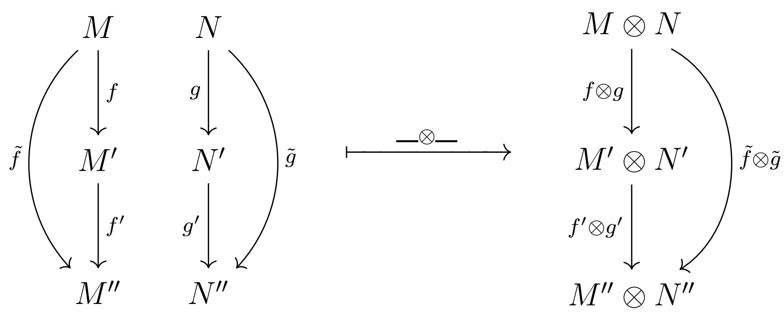
$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

Further, if we also have homomorphisms $f'\colon M' \to M''$ and $g'\colon N' \to N''$, then we have that

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g).$$

[10] Note that $\otimes$ is different in the tensor products on the left- and right-hand-sides.

Diagrammatically, the commutativity of the left-hand-side implies the commutativity of the right-hand-side:



Corollary 3.13. *If $M \cong M'$ and $N \cong N'$, then $M \otimes N \cong M' \otimes N'$.*

Proposition 3.14 (Canonical isomorphisms)**.**

$$M \otimes N \cong N \otimes M \qquad m \otimes n \leftrightarrow n \otimes m$$

$$\begin{aligned} (M \otimes N) \otimes P &\cong M \otimes N \otimes P & (m \otimes n) \otimes p &\leftrightarrow m \otimes n \otimes p \\ &\cong M \otimes (N \otimes P) & &\leftrightarrow m \otimes (n \otimes p) \end{aligned}$$

$$(\oplus_\lambda E_\lambda) \otimes M \cong \oplus_\lambda (E_\lambda \otimes M) \qquad (e_\lambda) \otimes m \leftrightarrow (e_\lambda \otimes m)$$

$$A \otimes M \cong M \qquad a \otimes m \leftrightarrow am$$

Corollary 3.15. *It follows that if A is an integral domain, then*

$$\mathrm{Frac}(A) \otimes_A \mathrm{Frac}(A) \cong \mathrm{Frac}(A).$$

Proposition 3.16 ($M \otimes$ (a free module))**.** *Let F be a free A-module with a basis $\{f_i\}$. Then*

$$M \otimes F \cong \oplus_i M,$$ [11]

and each $t \in M \otimes F$ can uniquely be written as

$$t = \sum_i m_i \otimes f_i.$$

[11] This just says that for any set $\mathcal{B}$, we have $M \otimes A^{[\mathcal{B}]} \cong M^{[\mathcal{B}]}$, which is a generalization of the last part of Proposition 3.14.

Proposition 3.17. *For $k \geq 0$, we have*[12]

$$A[x]^{\otimes k} \cong A[x_1, \ldots, x_k]$$

with

$$p_1(x) \otimes \cdots \otimes p_k(x) \leftrightarrow p_1(x_1) \cdots p_k(x_k).$$

4 Exact and split sequences

February 22, 2023

Definition 4.1 (Exact and short sequences)**.** A sequence (finite or infinite) of modules joined by homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\phi_i} M_i \xrightarrow{\phi_{i+1}} M_{i+1} \longrightarrow \cdots$$

is called exact at M_i iff we have

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

The whole sequence is called exact iff it is exact at all the (non-terminal) modules. A sequence of the form

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

is called a short sequence.

Corollary 4.2.

(i) $0 \longrightarrow M' \xrightarrow{\phi} M$ *is exact* $\iff$ ϕ *is injective.*

(ii) $M \xrightarrow{\psi} M'' \longrightarrow 0$ *is exact* $\iff$ ψ *is surjective.*

Corollary 4.3 (Two ways to generate exact sequences)**.**

(i) If $\phi\colon M \to N$ is injective, then

$$0 \longrightarrow M \xrightarrow{\phi} N \longrightarrow N/\operatorname{im}\phi \longrightarrow 0$$

is exact.

[12] Note that the tensor product of an empty family of modules is the zero module.

(ii) If $\psi\colon M \to N$ is surjective, then

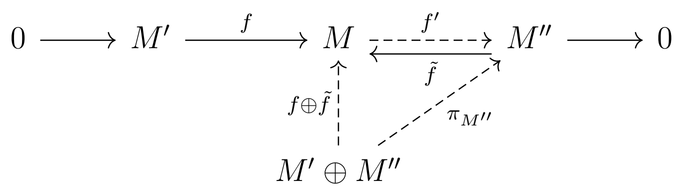
$$0 \longrightarrow \ker\psi \longrightarrow M \xrightarrow{\psi} N \longrightarrow 0$$

is exact.

Theorem 4.4 (Splitting of an injective sequence)**.** *Let the sequence*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{f'} M''$$

be exact. Let $\tilde{f}\colon M'' \to M$ be a homomorphism such that $f' \circ \tilde{f} = \mathrm{Id}_{M''}$. Then, in the diagram[13]



the following hold:

(i) f' is surjective.

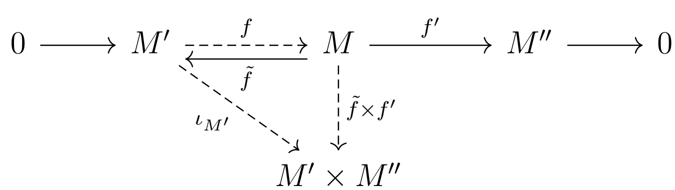
(ii) The dashed arrows commute.

(iii) $f \oplus \tilde{f}$ is an isomorphism.

Theorem 4.5 (Splitting of a surjective sequence)**.** *Let the sequence*

$$M' \xrightarrow{f} M \xrightarrow{f'} M'' \longrightarrow 0$$

be exact. Let $\tilde{f}\colon M \to M'$ be a homomorphism such that $\tilde{f} \circ f = \mathrm{Id}_{M'}$. Then, in the diagram[14]



the following hold:

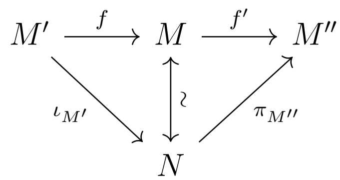
(i) f is injective.

[13]The diagram is *not* commutative for $\tilde{f} \circ \pi_{M''} \neq f \oplus \tilde{f}$ in general.
[14]Again, the diagram is non-commutative in general.

(ii) The dashed arrows commute.

(iii) $\tilde{f} \times f'$ *is an isomorphism.*

Lemma 4.6 ("Converse" to Theorems 4.4 and 4.5)**.** *Write* $N := M' \times M'' = M' \otimes M''$ *and let the following diagram commute with* $M \cong N$*:*



Then there exist homomorphisms $\tilde{f}\colon M \to M'$ *and* $\tilde{f}'\colon M'' \to M$ *such that* $\tilde{f} \circ f = \mathrm{Id}_{M'}$ *and* $\tilde{f}' \circ f' = \mathrm{Id}_{M''}$*.*

5 The Hom functors

February 21, 2023

Remark. *For us,* Hom *will mean* $\mathrm{Hom}_{\mathsf{Mod}_A}$ *and hence we'll omit the subscript.*

Remark. *Note that if* $M, N \in \mathsf{Mod}_A$*, then* $\mathrm{Hom}(M, N) \in \mathsf{Mod}_A$ *as well. This is* not *true of general categories.*

Proposition 5.1 ($\mathrm{Hom}(\_,\_)$ as a covariant functor $\mathsf{Mod}_A^{\mathrm{op}} \times \mathsf{Mod_A} \to \mathsf{Mod}_A$)**.** *Let* $f\colon M' \to M$ *and* $g\colon N \to N'$ *be homomorphisms. Then*

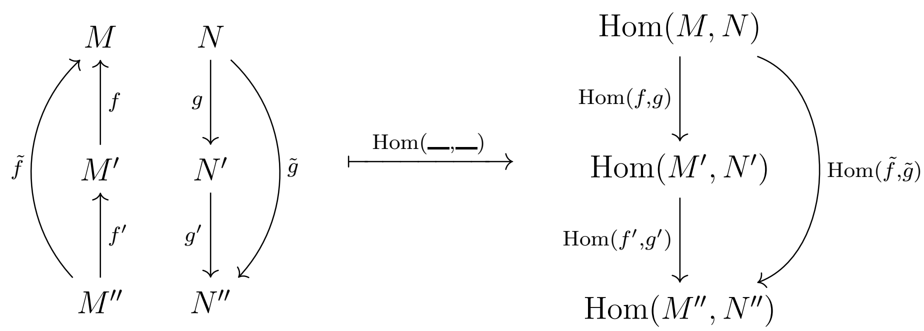
$$\mathrm{Hom}(f, g)\colon \phi \mapsto g \circ \phi \circ f$$

defines a homomorphism $\mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N')$*.*

Further, if we also have homomorphisms $f'\colon M'' \to M'$ *and* $g'\colon N' \to N''$*, then*

$$\mathrm{Hom}(f \circ f', g' \circ g) = \mathrm{Hom}(f', g') \circ \mathrm{Hom}(f, g).$$

Diagrammatically, the commutativity of the left-hand-side implies the commutativity *of the right-hand-side:*



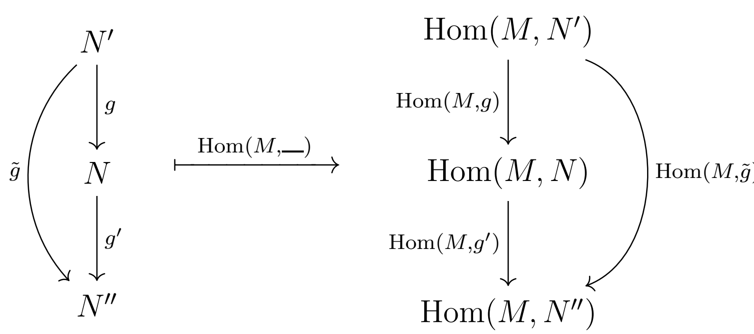
Proposition 5.2 (Hom(M, _) on $\mathsf{Mod}_A \to \mathsf{Mod}_A$ as a covariant left-exact functor)**.** *Fix a module M. Let $g\colon N' \to N$ be a homomorphism. Then we have a homomorphism* $\mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N)$ *given by*

$$\mathrm{Hom}(M, g)\colon \phi \mapsto g \circ \phi.$$

Further, if we also have a homomorphism $g'\colon N \to N''$, then we have

$$\mathrm{Hom}(M, g' \circ g) = \mathrm{Hom}(M, g') \circ \mathrm{Hom}(M, g).$$

Diagrammatically, the commutativity of the left-hand-side implies that of the right-hand-side:



Further, the following are equivalent:[15]

(i) $0 \to N' \to N \to N''$ *is exact.*

(ii) $0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$ *is exact.*

[15]This required AC.

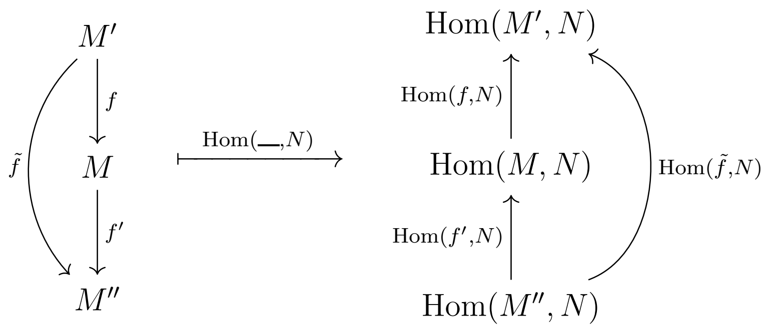
Proposition 5.3 ($\mathrm{Hom}(\_, N)$ on $\mathsf{Mod}_A \to \mathsf{Mod}_A$ as a contravariant left-exact[16] functor)**.** *Fix a module N. Let $f\colon M' \to M$ be a homomorphism. Then we have a homomorphism* $\mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N)$ *given by*

$$\mathrm{Hom}(f, N)\colon \phi \mapsto \phi \circ f.$$

Further, if we also have a homomorphism $f'\colon M \to M''$, then we have

$$\mathrm{Hom}(f' \circ f, N) = \mathrm{Hom}(N, f) \circ \mathrm{Hom}(N, f').$$

Diagrammatically, the commutativity of the left-hand-side implies that of the right-hand-side:



Further, the following are equivalent:

(i) $M' \to M \to M'' \to 0$ *is exact.*

(ii) $\mathrm{Hom}(M', N) \leftarrow \mathrm{Hom}(M, N) \leftarrow \mathrm{Hom}(M'', N) \leftarrow 0$ *is exact.*

6 The $\_ \otimes N$ functor

Notation. *We'll denote by $\mathrm{Bil}(M \times N, P)$ the set of all bilinear maps $M \times N \to P$. This in turn also forms an A-module under pointwise operations.*

Proposition 6.1. *We have*

$$\mathrm{Hom}(M, \mathrm{Hom}(N, P)) \cong \mathrm{Bil}(M \times N, P) \cong \mathrm{Hom}(M \otimes N, P).$$

[16]Yea, calling it "left-exact" here *is* confusing.

Lemma 6.2 (Exactness of isomorphic sequences)**.** *Consider the following:*

$$\begin{array}{ccccc} M' & \xrightarrow{f} & M & \xrightarrow{f'} & M'' \\ \updownarrow \wr & & \updownarrow \wr & & \updownarrow \wr \\ N' & \dashrightarrow & N & \dashrightarrow & N'' \end{array}$$

Let dashed arrows be the induced homomorphisms. Then the exactness at M is equivalent to exactness at N.

Proposition 6.3 ($\_ \otimes N$ is a right-exact covariant functor on $\mathsf{Mod}_A \to \mathsf{Mod}_A$)**.** *Let $M' \xrightarrow{f} M \xrightarrow{f'} M'' \to 0$ be exact. Then*

$$M' \otimes N \xrightarrow{f \otimes \mathrm{Id}_N} M \otimes N \xrightarrow{f' \otimes \mathrm{Id}_N} M'' \otimes N \longrightarrow 0$$

is exact as well.[17]

7 Projective and injective modules

February 21, 2023

Definition 7.1 (Projective and injective modules)**.** We call M *projective* iff $\mathrm{Hom}(M, \_)$ is exact, *i.e.*, it preserves short exact sequences. We call N *injective* iff $\mathrm{Hom}(\_, N)$ is exact.

Corollary 7.2.

(i) M is projective $\iff$ every $M \to N''$ factors through each surjection $N \twoheadrightarrow N''$:

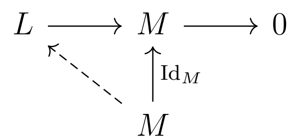
$$\begin{array}{ccccc} N & \longrightarrow & N'' & \longrightarrow & 0 \\ & \nwarrow & \uparrow & & \\ & & M & & \end{array}$$

(ii) N is injective $\iff$ every $M' \to N$ factors through each injection $M' \hookrightarrow M$:

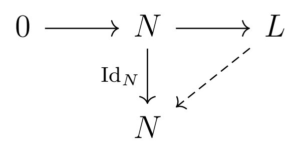
$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow & \swarrow & \\ & & N & & \end{array}$$

[17]That $\_ \otimes N$ is a covariant functor follows straight away from Proposition 3.12.

Definition 7.3 (Splitting of surjective and injective homomorphisms)**.** The exact sequence $L \to M \to 0$ is said to split iff there exists a commutative diagram like so:



Similarly, an exact sequence $0 \to N \to L$ is said to split iff there exists a commutative diagram of the following kind:



Corollary 7.4.

(i) If M is projective, then each exact $L \to M \to 0$ splits.

(ii) If N is injective, then each exact $0 \to N \to L$ splits.

Corollary 7.5. *Let N be a submodule of M such that either N is injective or M/N is projective. Then*

$$M \cong N \oplus M/N.$$

Example 7.6. $\mathbb{Z}$ (over $\mathbb{Z}$) is not injective and $\mathbb{Q}/\mathbb{Z}$ (over $\mathbb{Z}$) is not projective.

Lemma 7.7. *Free modules are projective.*[18]

Theorem 7.8 (Characterizing projective modules)**.** *M is projective $\iff$ it is the direct summand of a free module.*

Lemma 7.9. *A free module over an integral domain can't have nonzero torsion elements.*

Corollary 7.10. *In particular, if G is an abelian group with a non-zero torsion element, then G as a $\mathbb{Z}$-module is not projective.*

Corollary 7.11. *$\oplus_\lambda M_\lambda$ is projective $\iff$ each M_λ is projective.*

[18] This is one of the results that uses AC.

8 Flat modules

February 22, 2023

Definition 8.1 (Flat modules)**.** N is said to be flat iff $\_ \otimes N$ is exact.

Proposition 8.2. $\oplus_\lambda M_\lambda$ *is flat* $\iff$ *each* M_λ *is flat.*

Chapter III

Noether, Zariski, and Hilbert

1 On Noetherian-ness

April 22, 2023

Lemma 1.1 (Chain condition). *For a poset Σ, the following are equivalent:*

(i) Σ satisfies the ascending chain condition.

(ii) Every nonempty subset of Σ has a maximal element.

Corollary 1.2. *A is Noetherian $\iff$ A is Noetherian as an A-module.*

Proposition 1.3.

(i) A is Noetherian $\iff$ each ideal of A is finitely generated.

(ii) M is Noetherian $\iff$ each submodule is finitely generated.

Corollary 1.4. *Submodules of Noetherian modules are Noetherian.*

Remark. *Subrings of Noetherian subrings needn't be Noetherian (although their ideals will be, as A-modules). For instance $K[x_1, x_2, \ldots]$ a non-Noetherian subring of the field $K(x_1, x_2, \ldots)$, where K is a field.*

Theorem 1.5 (Exactness and Noetherian-ness).

(i) Let M', M'' be Noetherian and the composition $M' \to M \to M''$ be zero. Then M is Noetherian as well.

(ii) Let M be Noetherian, and $0 \to M' \to M$ (respectively $M \to M'' \to 0$) be exact. Then M' (respectively M'') is Noetherian as well.

Corollary 1.6.

(i) *Submodules and quotients of Noetherian modules are Noetherian.*

(ii) *Let N be a Noetherian submodule of M with M/N also Noetherian. Then M is Noetherian as well.*

(iii) *Homomorphic image of a Noetherian module is Noetherian.*

(iv) *If M, N are Noetherian, then $M \oplus N$ is Noetherian as well.*

(v) *If A is Noetherian, then $A/\mathfrak{a}$ is Noetherian (as a ring) as well.*

(vi) *If A is Noetherian and M over A is finitely generated, then M is Noetherian as well.*

Theorem 1.7 (Hilbert's basis[1] theorem)**.** *If A is Noetherian, then $A[x]$ is Noetherian as well.*

2 On algebras

April 24, 2023

Convention. *Throughout the rest of the document, we'll also reserve B, C for commutative rings with identity.*

Definition 2.1 (Algebra)**.** B together with a nice ring homomorphism $\phi\colon A \to B$ is called an A-algebra.

Remark.

(i) *We'll work with this definition rather than the more general Definition 1.4.*

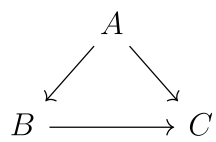
(ii) *If clear from the context, we'll just write B as the A-algebra, omitting ϕ.*

(iii) *The A-algebra B above also is an A-module with the scalar multiplication given by $(a, b) \mapsto \phi(a)\, b$. When we call an A-algebra an A-module, this is the module that we'll mean, unless stated otherwise.*

Corollary 2.2. *A is a $\mathbb{Z}$-algebra via the nice homomorphism $n \mapsto n1_A$.*

[1] The set of generators of an ideal was earlier called a "basis" of the ideal.

Definition 2.3 (Algebra homomorphisms)**.** Let B, C be A-algebras. Then an A-algebra homomorphism from B to C is a nice ring homomorphism $B \to C$ such that the following diagram commutes:



Proposition 2.4 (Alternate definition of algebra homomorphisms)**.** *Let B, C be A-algebras. Then a nice ring homomorphism $B \to C$ is an A-algebra homomorphism $\iff$ it is an A-module homomorphism.*

Proposition 2.5 (Finitely generated algebras)**.** *Let B be an A-algebra via $\phi\colon A \to B$. Then the following are equivalent:*

(i) There exists a $b \in B^n$ such that the evaluation $A[x_1, \ldots, x_n] \to B$ at b via ϕ is surjective.

(ii) There exists a surjective A-algebra homomorphism $A[x_1, \ldots, x_n] \to B$.[2]

Definition 2.6 (Finitely generated algebras)**.** An A-algebra satisfying either of the (equivalent) conditions in Proposition 2.5 is called a finitely generated A-algebra.

Lemma 2.7. *Homomorphic image of a Noetherian ring is Noetherian.*

Proposition 2.8. *A finitely generated algebra over a Noetherian ring is Noetherian as a ring.*

3 Towards the Nullstellensatz[3]

April 24, 2023

Theorem 3.1 (Artin-Tate)**.** *Let nice ring homomorphisms*

$$A \xrightarrow{\phi} B \xrightarrow{\psi} C$$

be given such that

(i) ψ is injective;

[2] Note that $A[x_1, \ldots, x_n]$ is an A-algebra via the usual inclusion.

[3] In German, *null* is zero, *stellen* is place, and *satz* is sentence.

(ii) C is finitely generated as B-module (via ψ); and,

(iii) C is finitely generated also as A-algebra (via $\psi \circ \phi$).

Then B is finitely generated as A-algebra (via ϕ).

Convention. *Let's reserve k, E, F, K to denote generic fields in the remainder of this document.*

Theorem 3.2 (Zariski's lemma)**.** *Let $\phi\colon k \to E$ be a field extension such that E is finitely generated as k-algebra. Then ϕ is an algebraic extension of finite degree.*

Corollary 3.3 (Field theory version of the Nullstellensatz)**.** *Let A be a finitely generated k-algebra and $\mathfrak{m}$ be maximal in A. Then $A/\mathfrak{m}$ is an algebraic extension of k of finite degree.*

Definition 3.4 (The sets $Z(T)$ and $I(X)$)**.** Let $n \geq 0$. Then for any $T \subseteq k[x_1, \ldots, x_n]$, we define

$$Z(T) := \{\text{common zeroes of the polynomials in } T\}$$

and for any $X \subseteq k^n$, we define

$$I(X) := \{\text{polynomials that vanish on } X\}.$$

Result 3.5 (The Zariski topology)**.** Let $n \geq 0$ and set $A := k[x_1, \ldots, x_n]$. Then the following hold:

(i) $Z(A) = \emptyset$.

(ii) $Z(0) = k^n$.

(iii) $Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a} \cdot \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$ for ideals $\mathfrak{a}$, $\mathfrak{b}$ of A.

(iv) $Z\big(\sum_i \mathfrak{a}_i\big) = \bigcap_i Z(\mathfrak{a}_i)$.

Consequently, $Z(\mathfrak{a})$'s for ideals $\mathfrak{a}$ of A form closed sets of a topology on k^n.
For $n = 1$ and k algebraically closed, we recover the cofinite topology.

Proposition 3.6 (The weak Nullstellensatz)**.** *Let k be algebraically closed. Then the following equivalent statements hold:*

(i) For any $n \geq 0$, we have that

$$\operatorname{MaxSpec}(F[x_1, \ldots, x_n]) = \big\{(x_1 - \alpha_1, \ldots, x_n - \alpha_n) : \alpha_i \in k\big\}.$$

(ii) For any ideal $\mathfrak{a}$ *of* $k[x_1, \ldots, x_n]$ *for* $n \geq 0$*, we have that*

$$Z(\mathfrak{a}) = \emptyset \iff \mathfrak{a} = A.$$

Theorem 3.7 (The strong Nullstellensatz)**.** *Let* k *be algebraically closed and* $\mathfrak{a}$ *be an ideal of* $k[x_a, \ldots, x_n]$ *for* $n \geq 0$*. Then*

$$I(Z(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a}).$$

Chapter IV

Rings and modules of fractions

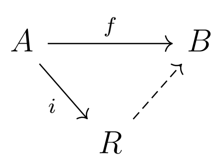
Convention. *Throughout this chapter, S will denote a multiplicative subset of A containing 1_A.*

1 Rings of fractions

1.1 Definition and construction

April 26, 2023

Definition 1.1 (Rings of fractions)**.** A commutative ring with identity R together with a homomorphism $i\colon A \to R$ with $i(S) \subseteq R^*$ is called a ring of fractions of A with respect to S iff any homomorphism $f\colon A \to B$ with $f(S) \subseteq B^*$ factors uniquely through R via i:



Remark. *As with tensor products, we'll usually mean just the ring R when we say a ring of fractions.*

Proposition 1.2 (Properties derivable directly from the universal property)**.** *Let (R, i) be a ring of fractions of A with respect to S. Then the following hold:*

(i) *Any other ring of fractions of A with respect to S is isomorphic to R via a unique isomorphism.*[1]

(ii) *The fractions generate the whole of R, i.e.,*

$$R = \{i(a)\, i(s)^{-1} : a \in A, s \in S\}.$$

(iii) *For $a, b \in A$ and $s, t, u \in S$,*

$$(at - bs)u = 0 \implies i(a)\, i(s)^{-1} = i(b)\, i(t)^{-1}.$$

Remark. *(i) allows us to denote ("up to unique isomorphisms") a generic ring of fractions of A with respect to S, using $S^{-1}A$ and i_A^S.*

(ii) allows us to denote the elements of $S^{-1}A$ by a/s.

Proposition 1.3 (Existence of $S^{-1}A$)**.** *The following is an equivalence relation on $A \times S$:*

$$(a, s) \sim (b, t) \quad \text{iff} \quad (at - bs)u = 0 \text{ for some } u \in S$$

Denoting the set of equivalence classes by R and the equivalence classes as $a/s := [(a, s)]$, we have addition and multiplication on R that satisfy

$$a/s + b/t = (at + bs)/(st), \text{ and}$$
$$(a/s)\,(b/s) = (ab)/(st).$$

Then R together with the map $i\colon A \to R$ given by

$$a \mapsto a/1_A$$

forms a ring of fractions of A with respect to S.

Remark. *i is not in general injective.*

Proposition 1.4 (A property derived via the construction)**.** *If (R, i) is a ring of fractions of A with respect to S, then for $a \in A$, we have*

$$i(a) = 0 \implies as = 0 \text{ for some } s \in S.$$

Proposition 1.5 ("Converse" of the derived properties)**.** *Let $i\colon A \to R$ be a homomorphism such that the following hold:*

(i) $i(A) \subseteq R^*$.

(ii) $i(a) = 0 \implies as = 0$ *for some* $s \in S$.

(iii) $R = \{i(a)\, i(s)^{-1} : a \in A, s \in S\}$.

Then (R, i) is a ring of fractions of A with respect to S.

[1] See Footnote 7.

1.2 Properties of $S^{-1}A$

April 28, 2023

Theorem 1.6 ($A_a \cong A[1/a]$)**.** *Let $a \in A$. Set $A_a := \{a^0, a^1, \ldots\}^{-1}A$. Then*

$$A_a \cong A[x]/(ax - 1_A).$$

Proposition 1.7 (Extension and contraction of ideals)**.** *Let $\mathfrak{a}$ be an ideal of A, and $\mathfrak{b}$ be an ideal of $S^{-1}A$. Then we define the following:*

$$\mathfrak{a}^e := (i_A^S(\mathfrak{a}))$$
$$\mathfrak{b}^c := (i_A^S)^{-1}(\mathfrak{b})$$

We also define

$$S^{-1}\mathfrak{a} := \{a/s : a \in \mathfrak{a}, s \in S\}.$$

Remark. *Of course, these notations are not robust, but we'll rely on context.*

Proposition 1.8. *Let $\mathfrak{a}$ be an ideal of A and $\mathfrak{b}$ an ideal of $S^{-1}A$. Then the following hold:*

$$S^{-1}\mathfrak{a} = \mathfrak{a}^e$$
$$(\mathfrak{b}^c)^e = \mathfrak{b}$$
$$(\mathfrak{a}^e)^c = \bigcup_{s \in S}(\mathfrak{a} : \{s\})$$

Proposition 1.9. *For an ideal $\mathfrak{a}$ of A, we have*

$$S^{-1}\mathfrak{a} = S^{-1}A \iff \mathfrak{a} \cap S \neq \emptyset.$$

Lemma 1.10. *Inverse images of prime ideals under ring homomorphisms are prime.*[2]

Proposition 1.11. *We have the following correspondence given by extension and contraction:*

$$\operatorname{Spec}(S^{-1}A) \quad \longleftrightarrow \quad \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$$

[2] True for general rings.

Proposition 1.12. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals of A. Then the following hold:*

$$\begin{aligned}
S^{-1}(\mathfrak{a}+\mathfrak{b}) &= (S^{-1}\mathfrak{a}) + (S^{-1}\mathfrak{b}) \\
S^{-1}(\mathfrak{a}\cap\mathfrak{b}) &= (S^{-1}\mathfrak{a}) \cap (S^{-1}\mathfrak{b}) \\
S^{-1}(\mathfrak{a}\cdot\mathfrak{b}) &= (S^{-1}\mathfrak{a}) \cdot (S^{-1}\mathfrak{b}) \\
S^{-1}(\operatorname{Rad}\mathfrak{a}) &= \operatorname{Rad}(S^{-1}\mathfrak{a}) \\
S^{-1}(\operatorname{Nil}\mathfrak{a}) &= \operatorname{Nil}(S^{-1}\mathfrak{a})
\end{aligned}$$

Proposition 1.13 (Localization)**.** *Let $\mathfrak{p}$ be a prime ideal of A. The the ring of fractions $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$ is a local ring with the maximal ideal being $\mathfrak{p}^e$.*

2 Modules of fractions

April 28, 2023

Remark. *We'll not define the modules of fractions categorically, rather, we will work with an explicit construction.*

Proposition 2.1 (When can M be an $S^{-1}A$-module as well?)**.** *If for each scalar $s \in S$, the endomorphism $\mu_s\colon m \mapsto sm$ is a bijection, then M forms an $S^{-1}A$-module with the scalar multiplication satisfying*

$$(a/s)m = a(m/s)$$

where m/s denotes the pre-image of m under μ_s.

Proposition 2.2 (Constructing $S^{-1}M$)**.** *The following defines an equivalence relation on $M \times S$:*

$$(m, s) \sim (n, t) \quad \textit{iff} \quad u(tm - sn) = 0 \textit{ for some } u \in S$$

Denoting the equivalence classes $[(m, s)]$ by m/t, the set $S^{-1}M$ of these equivalence classes forms an $S^{-1}A$ module with addition and scalar multiplication satisfying the following:

$$\begin{aligned}
m/s + n/t &= (tm + sn)/(st) \\
(a/s)\,(m/t) &= (am)/(st)
\end{aligned}$$

Proposition 2.3. *$S^{-1}\_\colon \mathsf{Mod}_A \to \mathsf{Mod}_{S^{-1}A}$ is a covariant exact functor.*

2.1 Local properties

April 28, 2023

Notation. *For a prime ideal $\mathfrak{p}$, we'll use $\square_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}\square$.*

Proposition 2.4 ("Zeroness")**.** *The following are equivalent:*

(i) $M = 0$.

(ii) $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p}$.

(iii) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* A.

Proposition 2.5 (Surjectivity or injectivity of A-module homomorphisms)**.** *Let* $\phi\colon M \to N$ *be an* A*-module homomorphism. Then the following are equivalent:*

(i) $\phi\colon M \to N$ *is injective.*

(ii) $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective for all prime ideals* $\mathfrak{p}$.

(iii) $\phi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective for all maximal ideals* $\mathfrak{m}$ *of* A.

The above also holds if "injective" is replaced by "surjective" throughout.

Appendix A

Algebras and polynomials

1 Modules and algebras

January 9, 2023

Definition 1.1 (R-modules)**.** Let R be a ring. Then a (left-)module over R is an abelian additive group M along with a scalar multiplication $R \times M \to M$ such that the following hold:

(i) $(r + s)m = rm + sm$.

(ii) $r(m + n) = rm + rn$.

(iii) $(rs)m = r(sm)$.

(iv) If R has an identity, then $1_R m = m$.

Remark. *Unless stated otherwise, a module will be a left-module.*

Definition 1.2 (R-algebras)**.** An R-algebra A is an R-module over a ring R along with a bilinear multiplication on $\times$ on M, *i.e.*, the following hold:

(i) $a \times (b + c) = a \times b + a \times c$;

(ii) $(a + b) \times c = a \times c + b \times c$; and,

(iii) $(ra) \times (sb) = (rs)(a \times b)$.

A is said to be associative, commutative, or to have an identity according to the operation $\times$.

Definition 1.3 (Nice homomorphisms)**.** A ring homomorphism $R \to S$ is said to be nice iff the image of the identity of R, if existent, is the identity in S.

Definition 1.4 (Homomorphism algebras)**.** A nice ring homomorphism $R \to S$ is called an algebra iff the image of R is central in S.

We call it commutative or to be having an identity according to the ring S.

Theorem 1.5 (Interplay of Definitions 1.2 and 1.4)**.**

(i) Let R be a ring with identity and A be an associative R-algebra with identity. Then the map $R \to A$ given by

$$r \mapsto r1_A$$

is an algebra with identity.

(ii) Let $\phi\colon R \to S$ be a nice ring homomorphism. Then the scalar multiplication $R \times S \to S$ defined by

$$(r, s) \mapsto \phi(r)s.$$

makes S an R-module, which is further an associative R-algebra if $\phi(R)$ is central in S.

Proposition 1.6. *Rings form $\mathbb{Z}$-algebras.*

Definition 1.7 (Module homomorphisms)**.** Let M, N be modules over a ring R. Then a function $\phi\colon M \to N$ is called an R-linear map iff the following hold:

(i) $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$.

(ii) $\phi(rm) = r\phi(m)$.

Proposition 1.8 (Algebra of endomorphisms)**.** *Let M be an R-module and define*

$$\mathcal{L}(M) := \{\textit{linear } R\textit{-maps on } M\}.$$

Then we can define the following operations on $\mathcal{L}(M)$:

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

Under these operations, $\mathcal{L}(M)$ forms a ring with identity.

Further, if R is commutative, then we can also define $R \times \mathcal{L}(M) \to \mathcal{L}(M)$ via

$$(r\phi)(m) := r\phi(m),$$

and under these operations $\mathcal{L}(M)$ forms an associative R-algebra with identity.

2 Polynomial rings

January 9, 2023

Definition 2.1 (Multi-index notation)**.** Let $n \in \mathbb{N}$. Then on the set $\mathbb{N}^n$, we define the following:

$$(\alpha + \beta)_i := \alpha_i + \beta_i$$
$$0_i := 0$$
$$(n\alpha)_i := n\alpha_i$$

Proposition 2.2 ("Infinite-polynomial" rings with commuting indeterminates)**.** *Let R be a ring and $n \in \mathbb{N}$. The the addition and multiplication on $R^{\mathbb{N}^n}$ defined by*

$$(f+g)_\alpha := f_\alpha + g_\alpha, \text{ and}$$
$$(fg)_\alpha := \sum_{\mu+\nu=\alpha} f_\mu \, g_\nu$$

make $R^{\mathbb{N}^n}$ a ring which is commutative (respectively, has identity) $\iff$ R is commutative (respectively, has identity).

Notation. *For monomials: We set*[1]

$$(ax^\alpha)_\beta := \begin{cases} a, & \beta = \alpha \\ 0, & \beta \neq \alpha \end{cases}.$$

Remark. *Only when R has identity can we view ax^α as a (more precisely, ax^0) times the monomial x^α (which is $1_R x^\alpha$).*

Proposition 2.3 (Algebra of monomials)**.** *In $R^{\mathbb{N}^n}$, the following hold:*

$$ax^\alpha + bx^\alpha = (a+b)x^\alpha$$
$$(ax^\alpha)(bx^\beta) = ab\, x^{\alpha+\beta}$$

Proposition 2.4 ($R \hookrightarrow R^{\mathbb{N}^n}$)**.** *Let R be a ring and $n \in \mathbb{N}$. Then $\phi\colon R \to R^{\mathbb{N}^n}$ defined by*

$$(\phi(a))_\alpha := \begin{cases} a, & \alpha = 0 \\ 0, & \alpha \neq 0 \end{cases}.$$

is a nice embedding, rendering $R^{\mathbb{N}^n}$ an R-module too. If R is commutative, then ϕ becomes a commutative algebra.

[1] We shouldn't use Kronecker delta since R needn't have identity.

Proposition 2.5 (Sufficient to study $R^{\mathbb{N}^n}$'s)**.** *Let R be a ring and $m, n \in \mathbb{N}$. Then as rings,*

$$(R^{\mathbb{N}^m})^{\mathbb{N}^n} \cong R^{\mathbb{N}^{m+n}}.$$

In particular, the function $\psi\colon R^{\mathbb{N}^{n+1}} \to (R^{\mathbb{N}^n})^{\mathbb{N}}$ given by[2]

$$(\psi(f)_i)_\alpha := f_{(\alpha,i)}$$

is a ring isomorphism.

Corollary 2.6 ($R^{\mathbb{N}^n}$'s nest)**.** *Let R be a ring, then we have the following embeddings:*

$$R \hookrightarrow R^{\mathbb{N}} \hookrightarrow R^{\mathbb{N}^2} \hookrightarrow \cdots$$

Proposition 2.7 ((Finite-)polynomial rings with commuting coefficients)**.** *Let R be a ring and $n \in \mathbb{N}$. Then*

$$\mathcal{P}(R,n) := \left\{p \in R^{\mathbb{N}^n} : p^{-1}(R \setminus \{0\}) \text{ is finite}\right\}$$

is a subring of $R^{\mathbb{N}^n}$ which is commutative (respectively, has identity) $\iff$ R is commutative (respectively, has identity).

Also, we have that

$$\mathcal{P}(R,n) = \Big\{\sum_{\alpha \in S} a_\alpha\, x^\alpha : S \subseteq \mathbb{N}^n \text{ is finite and } \alpha\colon S \to R\Big\}.$$

Proposition 2.8. *Analogues of Propositions 2.4 and 2.5 hold: ϕ can be restricted to be on $R \to \mathcal{P}(R,n)$, and ψ to be on $\mathcal{P}(R,n+1) \to \mathcal{P}(\mathcal{P}(R,n),1)$.*

Under ψ, we have

$$\sum_{|\alpha| \leq k} a_\alpha\, x^\alpha \mapsto \sum_{i=0}^{k} \Big(\sum_{|\beta| \leq k-i} a_{(\beta,i)} x^\beta\Big) x_{n+1}^i.$$

We also have analogue of Corollary 2.6.

Lemma 2.9. *Let R, S be rings. Then $f\colon \mathcal{P}(R,1) \to S$ is a homomorphism $\iff$ the following hold:*

(i) $\phi(0) = 0$.

(ii) $\phi(p + ax^i) = \phi(p) + \phi(ax^i)$.

---

[2] $\alpha \in \mathbb{N}^n$, $i \in \mathbb{N}$ and $(\alpha, i) \in \mathbb{N}^{n+1}$.

(iii) $\phi(ax^i\, bx^j) = \phi(ax^i)\,\phi(bx^j)$.

Proposition 2.10 (Evaluations of polynomials)**.** *Let $\phi\colon R \to S$ be a function between rings with $\phi(0_R) = 0_S$. Let $s \in S^n$ for $n \geq 0$. Then there exists a unique function $\mathcal{P}(R, n) \to S$ such that*[3]

$$\sum_{|\alpha|\leq k} a_\alpha x^\alpha \mapsto \sum_{|\alpha|\leq k} \phi(a_\alpha) s^\alpha$$

which is further a nice homomorphism if ϕ is an algebra.

Definition 2.11 (Image of evaluation)**.** We denote the image of the evaluation defined in Proposition 2.10 by $\phi(R)[s]$, or by $\phi(R)[s_1, \ldots, s_n]$ if $s = (s_1, \ldots, s_n)$.

Remark. *Note that $\phi(R)$ is in "hold-form" in the notation, but sometimes, it gets abused.*

Proposition 2.12 (Extending $R \to S$ to $R[x] \to S[x]$)**.** *Let $\phi\colon R \to S$ be a function between rings such that $\phi(0_R) = 0_S$. Let $n \in \mathbb{N}$. Then there exists a unique function $\mathcal{P}(R, n) \to \mathcal{P}(S, n)$ such that*

$$\sum_{|\alpha|\leq n} a_\alpha\, x^\alpha \mapsto \sum_{|\alpha|\leq n} \phi(a_\alpha) x^\alpha$$

which is further a (nice) homomorphism if ϕ is a (nice) homomorphism.

Remark. *Proposition 2.12 has an immediate generalization to $R^{\mathbb{N}} \to S^{\mathbb{N}}$.*

3 Field of rational functions

April 7, 2023

Definition 3.1 (Rational functions in n variables)**.** Let R be an integral domain and $n \geq 0$. Then $\mathcal{P}(R, n)$ is also an integral domain, and we define

$$\mathcal{R}(R, n) := \mathrm{Frac}\big(\mathcal{P}(R, n)\big).$$

[3]The monomials of the right-hand-side are well-defined, even if some $\alpha_i = 0$, by considering $\phi(a_\alpha)s^\alpha$ as a "single term", and not as the product of several terms, like we did for monomials. If S contains identity, then we can also interpret this as product of terms.

Proposition 3.2. *For any integral domain R and $n \geq 0$, we have that*

$$\mathcal{R}(R, n) \cong \mathcal{R}(\mathrm{Frac}(R), n).$$

Remark. *This is just saying that: It doesn't matter whether the coefficients come from R or $\mathrm{Frac}(R)$. Thus, we can just assume R to be a field rather than an integral domain.*

Definition 3.3 (Evaluations at rational functions)**.** Let $\phi\colon F \to K$ be a field homomorphism.[4] Then for $\alpha \in K^n$ ($n \geq 0$), we define[5]

$$\phi(F)(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathcal{P}(F, n) \text{ with } g(\alpha) \neq 0 \right\}.$$

Remark. *We also denote $\phi(F)(\alpha)$ by $\phi(F)(\alpha_1, \ldots, \alpha_n)$ if $\alpha = (\alpha_1, \ldots, \alpha_n)$.*
Again, $\phi(F)$ must be "held".

Proposition 3.4. *Continuing Definition 3.3, we have that that $\phi(F)(\alpha)$ is a subfield of K.*

4 Adjoining elements to rings and fields

April 7, 2023

Definition 4.1 (Adjoining elements)**.**

(i) Let $\phi\colon R \to S$ be a ring homomorphism and $T \subseteq S$. Then by $\phi(R)[T]$, we denote the smallest subring of S containing $\phi(R)$ as well as T.

(ii) Let $\psi\colon F \to K$ be a field homomorphism and $T \subseteq K$. Then we denote the smallest subfield of K containing $\psi(F)$ as well as T, by $\psi(F)(T)$.

Remark. *Again, $\phi(R)$, $\psi(F)$, strictly speaking, are in "hold-form" in the notation, but this is sometimes abused.*

[4] That is, a nice ring homomorphism.

[5] "$f(\alpha)$" and "$g(\alpha)$" denote the images of f, g under the evaluation at α.

Corollary 4.2. *Continuing Definition 4.1, we have*

$$\phi(R)[T] = \bigcup_{\substack{T' \subseteq T \\ |T'| < \infty}} \phi(R)[T'], \text{ and}$$
$$\psi(F)(T) = \bigcup_{\substack{T' \subseteq T \\ |T'| < \infty}} \psi(F)(T').$$

Also, if $s_1, \dots, s_n \in S$ *and* $\alpha_1, \dots, \alpha_n \in K$ *for* $n \geq 0$*, then we have*

$$\begin{aligned} \phi(R)[\{s_1, \dots, s_n\}] &= \phi(R)[s_1, \dots, s_n], \text{ and} \\ \psi(F)(\{\alpha_1, \dots, \alpha_n\}) &= \psi(F)(\alpha_1, \dots, \alpha_n) \\ &\cong \operatorname{Frac}\big(\psi(F)[\alpha_1, \dots \alpha_n]\big). \end{aligned}$$

Appendix B

Basic facts about rings

1 General

January 12, 2023

Proposition 1.1 (Prime ideals via multiplicative set)**.** *In a ring A a proper ideal $\mathfrak{p}$ is prime $\iff$ $A \setminus \mathfrak{p}$ is multiplicative.*[1]

Proposition 1.2. *The correspondence of ideals in $A/\ker\phi$ and $\phi(A)$ preserves maximality and primality.*

Proposition 1.3 (Operations on ideals)**.** *In a ring A, the following hold:*

$$\begin{aligned} \mathfrak{a}+\mathfrak{b} &= \mathfrak{b}+\mathfrak{a} & \mathfrak{a}\cap\mathfrak{b} &= \mathfrak{b}\cap\mathfrak{a} \\ (\mathfrak{a}+\mathfrak{b})+\mathfrak{c} &= \mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) & (\mathfrak{a}\cap\mathfrak{b})\cap\mathfrak{c} &= \mathfrak{a}\cap(\mathfrak{b}\cap\mathfrak{c}) \\ \mathfrak{a}+(0) &= \mathfrak{a} & \mathfrak{a}\cap A &= \mathfrak{a} \end{aligned}$$

$$\begin{aligned} \mathfrak{a}\cdot\mathfrak{b} &= \mathfrak{b}\cdot\mathfrak{a} && \text{if } A \text{ is commutative} \\ (\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c} &= \mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c}) \\ \mathfrak{a}\cdot(1) &= \mathfrak{a} && \text{if } 1\in A \end{aligned}$$

We also have

$$\sum_{i=1}^{n}\mathfrak{a}_i = \{a_1+\cdots+a_n : a_i\in\mathfrak{a}_i\}, \text{ and}$$
$$\bigodot_{i=1}^{n}\mathfrak{a}_i = \{\text{finite sums of terms of the form } a_1\cdots a_n \text{ where } a_i\in\mathfrak{a}_i\}.$$

[1] That is, closed under the ring multiplication.

The former motivates to define arbitrary sums of ideals as

$$\sum_{i \in I} \mathfrak{a}_i := \{\textit{finite sums of elements from } \mathfrak{a}_i\textit{'s}\}$$

which is indeed an ideal.

Proposition 1.4. *For ideals, the following hold:*

$$\begin{aligned} \mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) &= \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c} \\ (\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) &\subseteq \mathfrak{a} \cdot \mathfrak{b} \\ \mathfrak{a} \cap \mathfrak{b} &= \mathfrak{a} \cdot \mathfrak{b} \textit{ if } 1 \in A \textit{ and } \mathfrak{a} + \mathfrak{b} = (1) \end{aligned}$$

Proposition 1.5. *Let A be a ring and R, S be its additive subgroups. Then the following are equivalent:*

(i) *Every $x \in R + S$ has a unique decomposition.*

(ii) $R \cap S = \{0\}$.

(iii) *0 has a unique decomposition.*

Definition 1.6 (Independence of additive subgroups)**.** We call such subgroups as R, S above as independent. Further, if $A = R + S$, then we also write

$$A = R \oplus S.$$

Appendix C

Ideas from field theory

Convention. *In this appendix, F, K, L will denote generic fields.*

1 Algebraic independence

April 24, 2023

Definition 1.1 (Algebraic independence)**.** Let $\phi\colon F \to K$ be an extension. Then a subset $S \subseteq K$ is called algebraically independent with respect to ϕ iff for all $\beta_1, \ldots, \beta_n \in K$ for $n \geq 0$, we have that the kernel of the evaluation $F[x_1, \ldots, x_n] \to K$ at $(\beta_1, \ldots, \beta_n)$ via ϕ is 0.[1]

Corollary 1.2.

(i) We have the obvious characterization of algebraically independence if S is finite.

(ii) Subsets of algebraically independent sets are algebraically independent.

Lemma 1.3 (Extending an algebraically independent set by one element)**.** *Let $\phi\colon F \to K$ be an extension and $S \subseteq K$ be algebraically independent. Let $\beta \in K$ be transcendental with respect to the inclusion $\phi(F)(S) \hookrightarrow K$. Then $S \cup \{\beta\}$ is algebraically independent with respect to ϕ.*

Proposition 1.4 (Maximal algebraically independent subset)**.** *Let $\phi\colon F \to K$ be an extension and $S \subseteq K$. Then there exists a maximal subset $\tilde{S} \subseteq S$ such that*

(i) $\tilde{S}$ is algebraically independent with respect to ϕ; and,

(ii) each element of $S \setminus \tilde{S}$ is algebraic with respect to $\phi(F)(\tilde{S}) \hookrightarrow K$.

[1] That is, $F[x_1, \ldots, x_n] \to \phi(F)[\beta_1, \ldots, \beta_n]$ is an isomorphism.

2 Algebraically closed fields

April 24, 2023

Definition 2.1 (Algebraically closed fields)**.** A field F is called so iff every nonconstant polynomial in $F[x]$ has a root in F.

Corollary 2.2. *The following are equivalent:*

(i) *F is algebraically closed.*

(ii) *The irreducibles of $F[x]$ are precisely $x - \alpha$ for $\alpha \in F$.*

(iii) $\operatorname{MaxSpec}(F[x]) = \big\{(x - \alpha) : \alpha \in F\big\}$.[2]

Lemma 2.3. *Let $\phi\colon F \to K$ be a field extension with F being algebraically closed. Then $\phi(F)$ is an algebraically closed subfield of K.*

Proposition 2.4 (No proper algebraic extensions of algebraically closed fields possible)**.** *Let $\phi\colon F \to K$ be a field extension with F being algebraically closed. Then ϕ is an isomorphism.*

[2] We have unit in F, so we can use x for $1_F\, x^1$.