Algebra I

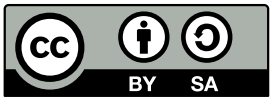
Lecturer
Dr. Gebhard Martin

Assistant

Notes
Maximilian Kessler, Elbrus Meyer

Version
git: 793e38d
compiled: Thursday 10th April, 2025 16:28

This work is licensed under a Creative Commons "Attribution-ShareAlike 4.0 International" license.



Visit the GitLab page for the source code of this document.

Contents

Summary of lectures

Lecture 1
Mo 07 Apr 2025

Orga 0.0.1. First, some organizational remarks:

Lecture The lecture always starts at 15 past. It will be 45 mins, 10 mins of break and then 45 mins again.

eCampus The pasword for the eCampus course is "Hilbert". The lecture notes and sheets will be uploaded there.

Exercises
- Sheet 0 (ring theory basics) will not be handed in.
- Sheet 1 (topology) is due this Friday.
- Further sheets will be uploaded Thursdays and handed in Thursdays the week after
- You will need 50% of the points to be admitted to the exam. Sheets 0 and 1 will not count towards the total (but points earned on sheet 1 will count towards your total, i.e. they are bonus points).

Content We will cover commutative rings and modules in the lecture.

Exam The first exam will be on July 29th.

Goal. *As our first goal of the lecture, we want to motivate that rings can be seen as rings of functions. For this, we will introduce the spectrum of a ring along with its Zariski topology.*

1 The spectrum of a ring

1.1 Rings, ideals and algebras

Definition 1.1 (Ring)**.** A **ring** is a set A together with two operations

- $+\colon A \times A \to A$
- $\cdot\colon A \times A \to A$, often abbreviated as $ab \coloneqq a \cdot b$

such that

(i) $(A, +)$ is an Abelian group. Its neutral element is called 0 ("zero").

(ii) $a(bc) = (ab)c \ \forall a, b, c \in A$, i.e. multiplication is associative.

(iii) $ab = ba \ \forall a, b \in A$, i.e. multiplication is commutative.

(iv) $\exists 1 \in A$ such that $1 \cdot a = a \ \forall a \in A$. 1 is called "one".

(v) $a(b + c) = ab + ac \ a, b, c \in A$, i.e. the distributive law holds

Convention 1.2. All rings are commutative, unless otherwise specified, i.e. we assume that $a \cdot b = b \cdot a$ for all $a, b \in A$.

Definition 1.3. Let A be a ring.

(1) An element $a \in A$ is called a **unit** if there exists $b \in A$ with $a \cdot b = 1$. We write $A^\times$ for the group of units of A.

(2) An element $a \in A$ is called **zero divisor** if there exists $b \neq 0 \in A$ such that $a \cdot b = 0$.

(3) A is called **integral domain** if 0 is its only zero-divisor.

(4) A is called a **field** if $A^\times = A \setminus \{0\}$.

Example 1.4. (1) $\mathbb{Z}$ is an integral domain, but not a field.

(2) $\mathbb{Z}/n\mathbb{Z}$ is a ring. Additionally,

$$n \text{ prime} \iff {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \text{ integral domain} \iff {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \text{ field}$$

We denote $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ if p is a prime.

(3) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ $\mathbb{F}_q$ are fields.

(4) If A is a ring, then $A[X]$, the polynomial ring in 1 variable, is also a ring.

Exercise. *Show that if A is an integral domain, then $A[X]$ is also an integral domain.*

(5) If A is a ring, then

$$A[x, x^{-1}] := \left\{ \sum_{i=-n}^{m} a_i X^i \;\middle|\; a_i \in A \right\}$$

is a ring.

(6) For all sets I and rings A,

$$A[\{X_i\}_{i \in I}],$$

the polynomial ring in the variables X_i, is a ring.

(7) If A is a ring and $B \subseteq A$ is a subset with $1 \in B$ and $\forall a, b \in B \colon a - b, ab \in B$, then B is called a **subring** of A. B is itself a ring.

Typical examples are $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(8) If X is a topological space, the set $\mathcal{C}^0(X)$ of continuous $\mathbb{R}$-valued functions on X is a ring (with pointwise addition and multiplication of functions).

Definition 1.5 (Ring homomorphism)**.** A map $f\colon A \to B$ between rings is called **ring homomorphism** if

(i) f is a group homomorphism with respect to addition.

(ii) $f(ab) = f(a) \cdot f(b)$ for all $a, b \in A$.

(iii) $f(1) = 1$.

Example 1.6. (1) For all rings A, there is a unique ring homomorphism $f\colon \mathbb{Z} \to A$.

Indeed, $f(1) \overset{\text{(iii)}}{=} 1$, hence

$$f(n) = f\left(\sum_{i=1}^{n} 1\right) \overset{\text{(i)}}{=} \sum_{i=1}^{n} f(1) = \sum_{i=1}^{n} 1_A = :n \cdot 1.$$

(2) The morphism of **Reduction mod n**: The unique morphism $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ as in (1).

(3) Field extensions are ring homomorphisms.

(4) If $g\colon X \to Y$ is a continuous map of topological spaces, then

$$\begin{array}{ccc} \mathcal{C}^0(Y) & \longrightarrow & \mathcal{C}^0(X) \\ f & \longmapsto & f \circ g \end{array}$$

is a ring homomorphism.

Definition 1.7 (Ideal)**.** Let A be a ring.

(1) An **ideal** I of A is a subgroup of the additive group $(A, +)$ such that $ab \in I$ for all $a \in A$ and $b \in I$.

(2) For a subset $S \subseteq A$, the ideal (check!)

$$(S) := \left\{ \sum_{i=1}^{n} \lambda_i a_i \;\middle|\; \lambda_i \in A, a_i \in S \right\}$$

is the **ideal generated by S**.

(3) A **principal ideal** of A is an ideal generated by one element.

(4) An ideal $I \subseteq A$ is called **prime** if $I \neq A$ and for all $a, b \in A$ with $ab \in I$, already $a \in I$ or $b \in I$.

(5) An ideal $I \subseteq A$ is called **maximal** if $I \neq A$ and I is maximal with respect to inclusion, i.e. if $I \subseteq J \neq A$ for another ideal J, then

$I = J$.

Example 1.8. (1) For all rings A, we have the

- **zero ideal**: $(0) = \{0\} \subseteq A$.
- **unit ideal**: $(1) = A \subseteq A$. Also, for $a \in A^\times$, $(a) = (1)$, hence the name.

(2) If $I, J \subseteq A$ are ideals, then their **intersection** $I \cap J$ is an ideal. Infinite intersections also preserve ideals.

(3) If $I, J \subseteq A$ are ideals, there is the **product ideal**

$$I \cdot J := (\{ij \mid \in I, j \in J\}).$$

You can check that $I \cdot J \subseteq I \cap J$.

(4) The ideals of $\mathbb{Z}$ are exactly the principal ideals (n) for $n \in \mathbb{Z}_{\geqslant 0}$.

The ideal (n) is maximal if and only if n is prime.

The zero ideal is a prime ideal, but not maximal.

(5) If K is a field, then

$$(X) \subseteq K[X]$$

is a maximal ideal.

For proofs of the following, see the lecture notes of "Einführung in die Algebra". The lecture notes are available on eCampus.

Recall. *If $N \lhd G$ is a normal subgroup, then G/N is a group.*

Lemma 1.9. Let A be a ring and $I \subseteq A$ an ideal. Then there exists a unique ring structure on A/I that makes

$$\begin{array}{ccc} A & \longrightarrow & A/I \\ a & \longmapsto & \overline{a} := a + I \end{array}$$

into a ring homomorphism.

Theorem 1.10 (Homomorphism Theorem)**.** Let $f\colon A \to B$ be a ring homomorphism.

1) The **image** $f(A) \subseteq B$ of f is a subring of B.
2) The **kernel**
$$\ker(f) := \{a \in A \mid f(a) = 0\} \subseteq A$$
is an ideal.

3) If $I \subseteq A$ is an ideal, then $f\colon A \to B$ factors through $\pi\colon A \to A/I$ iff $I \subseteq \ker(f)$.

4) There exists a unique $g\colon A/\ker(f) \to B$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/\ker(f) \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & B & \end{array} .$$

Moreover, g is injective, hence $A/\ker(f) \operatorname{im}(f)$.

Lemma 1.11. Let A be a ring and $I \subseteq A$ an ideal. Then

1) I is a prime ideal iff A/I is an integral domain.

2) I is a maximal ideal iff A/I is a field.

The following is a very important corollary:

Corollary 1.12. Let $f\colon A \to B$ be a ring homomorphism and $\mathfrak{p} \subseteq B$ a prime ideal. Then $f^{-1}(\mathfrak{p}) \subseteq A$ is a prime ideal.

Proof. $f^{-1}(\mathfrak{p})$ is the kernel of $A \to B \to {}^{B}\!/_{\mathfrak{p}}$, hence the homomorphism theorem gives an inclusion

$${}^{A}\!/_{f^{-1}(\mathfrak{p})} \hookrightarrow {}^{B}\!/_{\mathfrak{p}}.$$

Since $B/\mathfrak{p}$ is an integral domain by Lemma 1.11, so is $A/f^{-1}(\mathfrak{p})$ as a subring of an integral domain. Thus, $f^{-1}(\mathfrak{p})$ is prime. □

Oral remark 1.12.2. Be aware that the same statement does not hold for maximal ideals. For example, $\mathfrak{m} := (0) \subseteq \mathbb{Q}$ is maximal (since $\mathbb{Q}$ is a field), but $f^{-1}(0) = (0) \subseteq \mathbb{Z}$ is not maximal.

Definition 1.13 (Algebra)**.** Let A be a ring.

(1) An **A-algebra** is a ring B together with a ring homomorphism $A \to B$.

(2) A **homomorphism of A-algebras** is a ring homomorphism $f\colon B \to B'$ of A-algebras such that

$$\begin{array}{ccc} B & \xrightarrow{f} & B' \\ & \nwarrow \quad \nearrow & \\ & A & \end{array}$$

commutes.

Example 1.14. (1) Every ring is a $\mathbb{Z}$-algebra, and every ring homomorphism is a $\mathbb{Z}$-algebra homomorphism.

(2) If A is a ring and I a set,

$$A[\{X_i\}_{i\in I}]$$

is an A-algebra via the morphism

$$\begin{array}{ccc} A & \longrightarrow & A[\{X_i\}_{i\in I}] \\ a & \longmapsto & a. \end{array}$$

(3) If A is a ring, B an A-algebra via $f\colon A \to B$ and $M \subseteq B$ a subset, then there exists a unique A-algebra homomorphism

$$\mathrm{ev}_M : \left| \begin{array}{ccc} A[\{X_m\}_{m\in M}] & \longrightarrow & B \\ X_m & \longmapsto & m, \end{array} \right.$$

called the **evaluation at** M. The image of ev_M is denoted by $A[M] \subseteq B$ and called the A-subalgebra of B generated by M.

(4) In (3), if $M = \{b\}$ for some $b \in B$, we have

$$\mathrm{ev}_b : \left| \begin{array}{ccc} A[X] & \longrightarrow & B \\ P = \sum a_i X^i & \longmapsto & \sum f(a_i) b^i. \end{array} \right.$$

We write $g(b) := \mathrm{ev}_b(g)$.

Definition 1.15. Let A be a ring and B an A-algebra.

(1) A subset $M \subseteq B$ is said to **generate** B as an A-algebra if $B = A[M]$.

(2) B is called **finitely generated** as an A-algebra, if it can be generated by finitely many elements.

Corollary 1.16. Let A be a ring and B an A-algebra. Then B is finitely generated as an A-algebra iff there is an $n \geqslant 0$ and an ideal $I \subseteq A[x_1, \ldots, x_n]$ and an A-algebra isomorphism

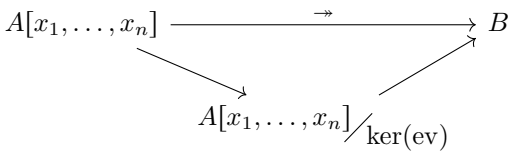
$$A[x_1, \ldots, x_n]/I \xrightarrow{\cong} B.$$

Proof. Pick generators $b_1, \ldots, b_n \in B$ of B as an A-algebra. Looking at the evaluation map

$$\mathrm{ev}_{b_1,\ldots,b_n}\colon A[x_1, \ldots, x_n] \twoheadrightarrow B,$$

it is surjective (because B was generated by the b_i). By the Homomorphism

Theorem, this map factors as



and setting $I := \ker(\mathrm{ev})$, we get the desired isomorphism. □

Orga 1.16.3. Today (april 14th) 7pm, registration for tutorials will open on eCampus. Please only register if you plan to take par in the exercises (which is mandatory for exam admission).

Lecture 2
Do 10 Apr 2025

2 Hilbert's Nullstellenstz v1

Let us represent some facts from an introductory course on algebra.

Definition 2.1 (Irreducible and prime elements of rings)**.** Let A be an integral domain. Then

1) An element $a \in A$ is called **irreducible** if $a \notin A^\times, a \neq 0$ and if $a = bc$, then $b \in A^\times$ or $c \in A^\times$.
2) For $a, b \in A$ we say that a **divides** b and write $a \mid b$ if there exists a $c \in A$ such that $ac = b$.
3) An element $a \in A$ is called **prime** if $a \neq 0, a \notin A^\times$ and if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Example 2.2. (1) In $\mathbb{Z}$, prime elements and irreducible elements are the same.

(2) $a \in A$ is prime if and only if $(a) \neq (0)$ and (a) is a prime ideal.

Lemma 2.3. Let A be an integral domain and $a \in A$. If a is prime, then a is also irreducible.

Definition 2.4. Let A be an integral domain.

(i) A is called **principal ideal domain** (PID) if every ideal I in A is principal.

(ii) A **unique factorization domain** (UFD) if every $a \in A$, $a \neq 0$,

$a \notin A^\times$ can be written as a product of prime elements uniquely up to units and permutation.

Lemma 2.5. Let A be a principal ideal domain. Then A is a unique factorization domain.

Example 2.6. The following are principal ideal domains:

(1) $\mathbb{Z}$.

(2) $k[X]$, where k is a field.

(3) $k[X, Y]$ is not a principal ideal domain.

In fact, (1) and (2) are Euclidean rings, i.e. they have a division with remainder. Generally, Euclidean domains are principal ideal domains.

Theorem 2.7. If A is a unique factorization domain, then $A[X]$ is also a unique factorization domain.

In particular, $k[x_1, \ldots, x_n]$ is a unique factorization domain.

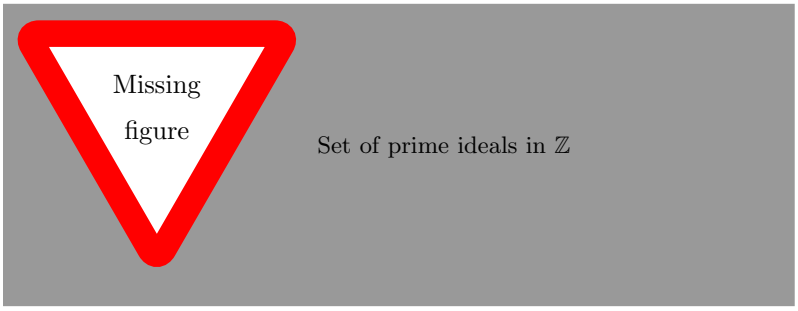
Lemma 2.8. In a unique factorization domain, elements are prime if and only if they are irreducible.

Lemma 2.9. Let A be a principal ideal domain and $a \in A$. Then, the ideal (a) is maximal if and only if a is irreducible.

Corollary 2.10. Let A be a principal ideal domain and $\mathfrak{p} \subseteq A$ a non-zero prime ideal. Then, $\mathfrak{p}$ is maximal.

Example 2.11. By Corollary 2.10 and Lemma 2.9, we get:

1) The maximal ideals in $\mathbb{Z}$ are the ideals (p) with p prime. The only non-maximal prime ideal is (0).



2) If k is a field, and $0 \neq f \in k[x]$. Then

$$f \in k[x]^\times \iff \deg(f) = 0.$$

If $\deg(f) = 1$, then f is irreducible.

3) We can even fully describe the maximal ideals of $k[x]$ in special cases:

Recall. *A field k is **algebraically closed** iff all non-constant polynomials have a root.*

Thus, if k is algebraically closed, then

$$k[x] \text{ irreducible} \iff \deg(f) = 1.$$

4) Consider $x^2 + 1 \in \mathbb{R}[x]$, which is irreducible. Hence, $(x^2 + 1)$ is a non-zero prime (and maximal) ideal.

Question 2.11.4. What happens in polynomial rings with more variables?

Lemma 2.12. Let k be a field and take a point $P = (a_1, \ldots, a_n) \in k^n$. Then,

$$\mathfrak{m}_P = (x_1 - a_1, \ldots, x_n - a_n) \subseteq k[x_1, \ldots, x_n]$$

is a maximal ideal.

Proof. For $f \in k[x_1, \ldots, x_n]$, we have

$$\overline{f} = \overline{f(a_1, \ldots, a_n)} \mod \mathfrak{m}_P$$

and the composition $k \hookrightarrow k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/\mathfrak{m}_P$ is injective.

Thus, $f \in \mathfrak{m}$ iff $f \in \ker(\varphi)$ where $\varphi = \text{ev}_{a_1,\ldots,a_n}$. Note that φ is also surjective (by evaluating at constants), hence by the homomorphism theorem

$$k[x_1, \ldots, x_n]/\mathfrak{m}_P \cong k$$

and by Lemma 1.11, $\mathfrak{m}_P$ is maximal. □

Goal. *We would like to show that if k is algebraically closed, then every maximal ideal in $k[x_1, \dots, x_n]$ is of the form $\mathfrak{m}_P$ for some point $P \in k^n$.*

We have just seen this for $n = 1$, but not generally.

Definition 2.13. Let k be a field and A a k-algebra.

1) An element $a \in A$ is called **algebraic over k** if there exists $f \neq 0 \in k[x]$ with $f(a) = 0$.
2) A is called **algebraic over k** if all $a \in A$ are algebraic over k.
3) A finite subset $\{a_1, \dots, a_n\} \subseteq A$ is called **algebraically independent** if $\mathrm{ev}_{a_1,\dots,a_n} : k[x_1, \dots, x_n] \to A$ is injective.

   A set $M \subseteq A$ is called algebraically independent if all finite subsets of M are algebraically independent.
4) If A is a field, a **transcendence basis** for A over k is an algebraically independent subset $M \subseteq A$ such that A is algebraic over $k(M)$.

Example† 2.13.5. $x^n \in k(x)$ is a transcendence basis of $k(x)$ over k for all $n \geqslant 1$.

Theorem 2.14 (Existence of transcendence basis)**.** Let L/K be a field extension.

1) $M \subseteq L$ is a transcendence basis for L/K iff M is maximally algebraically independent.
2) If $M' \subseteq L$ is algebraically independent and $M'' \subseteq L$ is such that $L/K(M'')$ is algebraic, then there exists a transcendence basis with $M' \subseteq M \subseteq M' \cup M''$.

In particular, transcendence bases exist.

Recall. *If A is an integral domain, the **field of fractions** $\mathrm{Frac}(A)$ of A is the set of equivalence classes of $\frac{a}{b}$ with $a \in A, b \neq 0 \in A$ under the relation $\frac{ac}{bc} = \frac{a}{b}$.*

Lemma 2.15 (Universal property of the field of fractions)**.** Let A be an integral domain and $f\colon A \to B$ a ring homomorphism. Then, f factors through

$$\begin{array}{ccc} A & \longrightarrow & \mathrm{Frac}(A) \\ a & \longmapsto & \frac{a}{1} \end{array}$$

if and only if $f(A \setminus \{0\}) \subseteq B^\times$.

Lemma 2.16. Let A be an algebra over a field k.

1) If A is an integral domain and algebraic over k, then A is a field.
2) If A is a field and contained in a finitely generated k-algebra, then A is algebraic over k.

Oral remark 2.16.6. One might be tempted to deduce 2) from 1) by arguing that A is itself finitely generated over k since it is contained in a finitely generated k-algebra. However, this is not true in general, as the following example shows.

Example† **2.16.7.** Let k be a field and consider the finitely generated k-algebra. However, the subalgebra $B = k[x, xy, xy^2, xy^3, \dots]$ is not finitely generated.

Corollary 2.17 (Zariski's Lemma)**.** Let L/K be a field extension. If L is finitely generated as a K-algebra, then L/K is finite.

Note. *The notions of being finitely generated as a k-algebra and being finitely generated as a field extension over k are not the same.*

For example, $k(x)/k$ is finitely generated as a field extension, but not as a k-algebra.

Corollary 2.18. Let k be a field and let $A \to B$ be a morphism of k-algebras. Let $\mathfrak{m} \subseteq B$ be a maximal ideal.

If B is finitely generated as a k-algebra, then $f^{-1}(\mathfrak{m})$ is maximal.

Proof. As in Corollary 1.12, by the homomorphism theorem we get a commutative diagram

$$\begin{array}{ccccc} & & A & \longrightarrow & B \\ & & \downarrow & & \downarrow \\ k & \longrightarrow & A/f^{-1}(\mathfrak{m}) & \hookrightarrow & B/\mathfrak{m} \end{array}$$

Since B is finitely generated as a k-algebra, so is $B/\mathfrak{m}$. Since $B/\mathfrak{m}$ is also a field, by Corollary 2.17 it is algebraic over k.

Hence, also $A/f^{-1}(\mathfrak{m})$ is algebraic over k. Since $A/f^{-1}(\mathfrak{m})$ is an integral domain, by Lemma 2.16, $f^{-1}(\mathfrak{m})$ is in fact maximal. □

Corollary 2.19. Let k be an algebraically closed field and $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$

a maximal ideal. Then, there exists a point $P \in k^n$ such that $\mathfrak{m} = \mathfrak{m}_P$.

Corollary 2.20 (Hilbert's Nullstellensatz v1)**.** Let k be an algebraically closed field and $I \subsetneq k[x_1, \ldots, x_n]$ a proper ideal. Then, there exists $P \in k^n$ such that $f(P) = 0$ for all $f \in I$.

Proof. By Zorn's lemma, there is some maximal ideal $\mathfrak{m}$ with $I \subseteq \mathfrak{m}$. By Corollary 2.19, $\mathfrak{m} = \mathfrak{m}_P = \ker(\mathrm{ev}_P)$ for some point $P \in k^n$. Hence, for all $f \in I$, $f(P) = \mathrm{ev}_P(f) = 0$. □