On this lecture

Galois theory = study of single polynomial eqn in one variable over a field

(Primitive Element Theorem: L/K finite field extn.

Then $\exists\, f \in K[T]$ s.th. $L \simeq K[T]/(f)$.)

Commutative algebra = study of systems of polynomial eqns in several variable w/ general coefficients

Historical origins 1) Geometry

$T_1, \dots, T_n$ variables, $f_1, \dots, f_m \in \mathbb{C}[T_1, \dots, T_n]$ polynomial equations.

Can consider $\begin{cases} \text{the ring } A = \mathbb{C}[T_1, \dots, T_n]/(f_1, \dots, f_m) \\ \text{the solution set } X = \{(t_1, \dots, t_n) \in \mathbb{C}^n \mid f_i(\underline{t}) = 0 \text{ for } i = 1, \dots, m.\} \end{cases}$

Then properties of A and X match. Examples:

Dimension of A = $\mathbb{C}$-dimension of X

A is regular $\iff$ X is nonsingular (ie. a manifold)

Only idempotents in A are 0 and 1 $\iff$ X is connected.

2) <u>Number theory</u> Instead of $\mathbb{Q}[T]/(f)$, interested in $\mathbb{Z}[T]/(f)$, $f \in \mathbb{Z}[T]$.

E.g. $\mathbb{Z}[i]$ (Gaussian numbers),

$\mathbb{Z}[\zeta_3]$ (Eisenstein numbers) $\subseteq \mathbb{C}$.

<u>This lecture</u> Commutative rings & modules

+ Examples from 1) & 2).

Follow ups: Alg. Geometry, Alg. Number Theory, Algebra II.

Relations w/: Alg. Topology, Rep. Theory.

<u>Prerequisites</u> Einführung in die Algebra: Basic knowledge of commutative rings. (Most things will be recalled though.)

<u>Main Reference</u> Atiyah - MacDonald Introduction to comm. algebra.

<u>Information</u> math.uni-bonn.de/people/ja/commalg.

ja = Johannes Anschütz (assistent, tutorial organization)

Contact mihatsch@math.uni-bonn.de (lecture)

ja@ ——— (tutorials, exams etc.)

Tutorials Register on eCampus before April 10.

Sheets in pairs, $\geq 50\%$ for exam.

Exams July 31, Sept. 27

Register on Basis.

§1 Rings and Ideals

Ring (in this lecture) $\underset{def}{=}$ commutative ring w/ unit element 1

<u>Def</u> 1) <u>Ideal</u> in ring A $\underset{def}{=}$ abelian subgroup $\mathfrak{a} \subseteq A$ s.th.

$\forall a \in A, x \in \mathfrak{a}$ also $a \cdot x \in \mathfrak{a}$.

2) $S \subseteq A$ a subset. <u>Ideal generated by S</u> $\underset{def}{=}$

$$(S) = \bigcap_{S \subseteq \mathfrak{a} \subseteq A} \mathfrak{a} \qquad \text{(smallest ideal containing } S\text{)}$$

<u>Lem 1</u> $(S) = \left\{ \sum_{s \in S} a_s \cdot s \;\middle|\; a_s \in A, \text{ all but fin many } = 0 \right\}$

<u>Proof</u> Denote RHS by $\mathfrak{b}$. Since $-\sum a_s \cdot s = \sum (-a_s) \cdot s$

& $\sum a_s \cdot s + \sum b_s \cdot s = \sum (a_s + b_s) \cdot s$, $\mathfrak{b}$ is subgrp.

Since $a \cdot \sum a_s \cdot s = \sum (a a_s) \cdot s$, $\mathfrak{b}$ is an ideal.

$\mathfrak{b}$ contains S since $\forall s \in S$, $1 \cdot s \in \mathfrak{b}$. Thus $(S) \subseteq \mathfrak{b}$.

Conversely, if $\mathfrak{a} \subseteq A$ is an ideal w/ $S \subseteq \mathfrak{a}$, then $\mathfrak{a}$ contains all elements $a \cdot s$, $a \in A$, $s \in S$ (ideal property), hence all finite sums $\sum a_s s$. So $\mathfrak{b} \subseteq (S)$ and equality is shown. $\square$

How to construct rings? (Generators and relations principle.)

1) Have known rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ etc....

2) Form polynomial rings: A any ring, T variable (= a symbol)

Defn

$$A[T] := \bigoplus_{i=0}^{\infty} A \cdot T^i = \left\{ \sum_{i=0}^{n} a_i T^i \;\middle|\; \begin{array}{l} n \geq 0, \; a_i \in A \\ a_n \neq 0 \end{array} \right\}$$

$$\sum_{i=0}^{n} a_i T^i = \sum_{i=0}^{m} b_i T^i \iff n = m \quad \left(\begin{array}{c}\text{assume} \\ a_n, b_m \neq 0\end{array}\right)$$

and $a_i = b_i \;\; \forall i = 0, \dots, n$

If $T_1, \dots, T_n$ several variables, can define iteratively

$$A[T_1, \dots, T_n] := A[T_1, \dots, T_{n-1}][T_n]$$

If I any set, $(T_i, \, i \in I)$ variables indexed by I, can define

$$A[T_i, \, i \in I] := \bigcup_{\substack{J \subseteq I \\ \text{finite subset}}} A[T_j, \, j \in J]$$

3) Pass to quotient ring: A ring, $\mathfrak{a} \subseteq A$ ideal.

$A/\mathfrak{a}$:= quotient abelian group w/ multiplication

$$(a+\mathfrak{a}) \cdot (b+\mathfrak{a}) := ab + \mathfrak{a}$$

[This is well-defined: Let $x, y \in \mathfrak{a}$. Then

$$(a+x+\mathfrak{a})(b+y+\mathfrak{a}) = ab + \underbrace{ay + bx}_{\in \mathfrak{a} \text{ by ideal property}} + \mathfrak{a}$$

$$= ab + \mathfrak{a}. \qquad \square.$$
]

Then $A/\mathfrak{a}$ is again a ring.

Common Notation: $a, b \in A$, $\mathfrak{a} \subseteq A$ ideal

•) $a \equiv b \mod \mathfrak{a} \overset{}{\underset{\text{def}}{\Longleftrightarrow}} a - b \in \mathfrak{a}$

•) $\bar{a}, \bar{b} \in A/\mathfrak{a}$:= residue classes $a+\mathfrak{a}, b+\mathfrak{a}$

<u>Some further notions</u> Let A, B be rings.

1) $\varphi: A \to B$ <u>ring map</u> $\overset{=}{\text{def}}$ $\begin{cases} \varphi(a+b) = \varphi(a) + \varphi(b) \\ \varphi(ab) = \varphi(a)\varphi(b) \\ \varphi(1) = 1 \end{cases}$

2) Then $\varphi(A)$ is a <u>subring</u> of B

and $\ker(\varphi) \subset A$ an ideal.

Moreover, $A/\ker(\varphi) \xrightarrow{\sim} \varphi(A)$.

3) Universal property of the polynomial ring:

A ring, I set, $\varphi: A \to B$ ring map.

For every $I \to B$, $i \mapsto b_i$, there is a unique

ring map $\psi_{(b_i)}: A[T_i, i \in I] \longrightarrow B$

s.th. $A \ni a \mapsto \varphi(a)$,

$T_i \mapsto b_i$.

It is called <u>evaluating the T_i at the b_i</u>.

4) Universal property of the quotient ring:

$\varphi : A \to B$ ring map, $\mathfrak{a} \subseteq \ker(\varphi)$ an ideal. Then $\exists!$ factorization

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d] \arrow[dr, phantom, "="] & B \\ A/\mathfrak{a} \arrow[ur, dotted, "\exists!"'] & \end{tikzcd} \qquad \begin{tikzcd} a \arrow[r, mapsto] \arrow[d, mapsto] & \varphi(a) \\ a+\mathfrak{a} \arrow[ur, mapsto] & \end{tikzcd}$$

§2 Examples

1) K a field, $K[T]$ polynomial ring,

$$f = \sum_{i=0}^{n} a_i T^i \in K[T], \quad n \neq 0.$$

Then for $m \geq n$, we have

$$T^m = \underbrace{a_n^{-1} T^{m-n} \cdot f}_{\in (f)} - a_n^{-1} \sum_{i=0}^{n-1} a_i T^{m-n+i}$$

i.e. $T^m \equiv -a_n^{-1}\left(a_{n-1}T^{m-1} + a_{n-2}T^{m-2} + \cdots + a_0 T^{m-n}\right)$

mod (f).

Apply iteratively

$\Longrightarrow$ Every residue class in $K[T]/(f)$ has a representative $g + (f)$ w/ $\deg(g) \leq n-1$.

<u>Exercise</u> This "minimal" representative g is <u>unique</u>.

Write $t := \overline{T} = T + (f)$ in following.

The above shows that $A = K[T]/(f)$ is an n-dimensional K-vsp with basis

$$1, t, \ldots, t^{n-1}.$$

Multiplication in this ring:

$$t \cdot t^i = \begin{cases} t^{i+1} & i < n-1 \\ -a_n^{-1}(a_{n-1}t^{n-1} + \cdots + a_1 t + a_0) & i = n-1. \end{cases}$$

This can be done for any base ring assuming that a_n is invertible:

A ring, $f = \sum_{i=0}^{n} a_i T^i$ w/ $a_n \in A^\times$.

$t := T + (f) \in A[T]/(f)$ as before.

Then $A[T]/(f) \cong \bigoplus_{i=0}^{n-1} A \cdot t^i$ as abelian group

with multiplication as before.

2) Consider $\mathbb{Z}[X,Y]$ and its ideal (XY)

Note that $(XY) = \{ f \in \mathbb{Z}[X,Y] \mid XY | f \}$

Every $f \in \mathbb{Z}[X,Y]$ can be written as

$$f = c + \sum_{i=1}^{n} a_i X^i + \sum_{j=1}^{m} b_j Y^j + \underbrace{g \cdot XY}_{\in (XY)}$$

w/ unique c, a_i, b_i, g. In other words,

every class in $\mathbb{Z}[X,Y]/(XY)$ has a <u>unique</u>

representative of the form

$$c + \sum_{i=1}^{n} a_i X^i + \sum_{j=1}^{m} b_j Y^j$$

Put $x := X + (XY)$, $y := Y + (XY)$.

This shows

$$\mathbb{Z}[X,Y]/(XY) \cong \mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} (\mathbb{Z} \cdot x^i \oplus \mathbb{Z} \cdot y^i)$$

(as abelian group)

with multiplication $x^i x^j = x^{i+j}$, $y^i \cdot y^j = y^{i+j}$

$xy = 0$.

§3 Basic properties

Defn Let A be a ring.

1) $x \in A$ nilpotent $\underset{def}{=}$ $x^n = 0$ for some $n \geq 0$

A reduced $\underset{def}{=}$ 0 is the only nilpotent element

2) $x \in A$ zero divisor $\underset{def}{=}$ $\exists\, 0 \neq y \in A$ s.th. $x \cdot y = 0$.

A integral domain or domain $\underset{def}{=}$ $A \neq 0$ and 0 is the only zero divisor.

$x \in A$ regular $\underset{def}{=}$ x not zero divisor.

3) $x \in A$ unit $\underset{def}{=}$ $\exists\, y \in A$ s.th. $x \cdot y = 1$.

$A^\times \underset{def}{=}$ units of A. Form group under multiplication.

Equivalent characterization Consider $\phi : A \longrightarrow A$, $a \longmapsto x \cdot a$

Then ϕ not injective $\Longleftrightarrow$ x zero divisor

ϕ injective $\Longleftrightarrow$ x regular

ϕ surjective $\Longleftrightarrow$ ϕ bijective $\Longleftrightarrow$ $x \in A^\times$

Note: $\mathrm{Im}(\phi) = A \cdot x = (x)$ is ideal generated by x.

<u>Example</u> Let $n \in \mathbb{Z}$, put $A_n = \mathbb{Z}[T]/(T^2-n)$

Put $t = T + (T^2-n)$ as before.

·) If $n = 0$, $t^2 = 0$ in this ring. But $t \neq 0$, so it

is a <u>nilpotent</u> element. $\Longrightarrow$ A_0 not reduced

·) If $n = m^2$ is a square, then

$$(m+t)(m-t) = m^2 - t^2 = n - n = 0.$$

So $(m+t)$, $(m-t)$ are <u>zero divisors</u>.

<u>Exercise</u>: Show $\mathbb{Z}[T]/_{T^2-n}$ reduced if $n \neq 0$.

$\Longrightarrow$ A_{m^2} reduced, but not integral domain.

·) If n not a square, $A_n \cong \mathbb{Z}[\sqrt{n}] \subset \mathbb{Q}(\sqrt{n})$

$$t \longmapsto \sqrt{n}$$

can be embedded as subring of field $\mathbb{Q}(\sqrt{n})$. In ptic,

A_n is an integral domain

Prop 2 Consider a polynomial ring $B = A[T_i\ ,\ i \in I]$.

If A is a domain (resp. reduced), then B is so as well.

Proof First assume I is finite. Since $A[T_1, \dots, T_n] = A[T_1, \dots, T_{n-1}][T_n]$,

we can proceed by induction and assume $B = A[T]$. Then we

can look at leading coefficient: Let

$f = a_n T^n + \dots + a_0, \quad g = b_m T^m + \dots + b_0, \quad a_n, b_m \quad 0.$

Then $f \cdot g = a_n \cdot b_m T^{n+m}$ + lower terms

$f^r = a_n^r T^{r \cdot n}$ + lower terms

A domain $\Rightarrow a_n \cdot b_m \neq 0 \Rightarrow f \cdot g \neq 0$

A reduced $\Rightarrow a_n^r \neq 0 \ \forall r \Rightarrow f^r \neq 0 \ \forall r$ $\square$ I finite.

In general, given f resp. f and g, there is a finite subset $J \subseteq I$ s.th. $f, g \in A[T_j, j \in J] \subseteq B$

Then we may show $f \cdot g \neq 0$ or $f^r \neq 0 \ \forall r$ in there

because $A[T_j\ ,\ j \in J] \hookrightarrow A[T_i\ ,\ i \in I]$

is injective. $\square$

Prop 3 1) For A ring, put $\mathrm{nil}(A) = \{x \in A \mid x \text{ nilpotent}\}$.

Then $\mathrm{nil}(A)$ is an ideal, called the nilradic of A.

2) The quotient $\bar{A} = A/\mathrm{nil}(A)$ is reduced.

3) If B is reduced, then any ring map $\varphi : A \to B$ factors uniquely through $\bar{A}$.

Proof 1) If $x^n = 0$, then $(ax)^n = a^n x^n = 0$ $\forall a \in A$.

Thus $x \in \mathcal{N} := \mathrm{nil}(A) \Rightarrow ax \in \mathcal{N}$.

If $x^n = y^m = 0$, then $(x+y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^{n+m-1-i} y^i = 0$

because always ($n+m-1-i \geq n$ or $i \geq m$)

Thus $\mathcal{N}$ is an ideal.

2) Let $\bar{x} \in \bar{A}$ be image of $x \in A$ and assume $\bar{x}^n = 0$.

This means $x^n \in \mathcal{N}$, i.e. $(x^n)^k = x^{nk} = 0$ for $k \gg 0$.

Thus $x \in \mathcal{N}$, hence $\bar{x} = 0$.

3) If $x^n = 0$, then $\varphi(x)^n = \varphi(x^n) = 0$. Then $\varphi(x) = 0$ since B is reduced. This means $\mathcal{N} \subseteq \ker \varphi$, hence the factorization $\square$

Exercise Compute units and nilradical of the rings

$$\mathbb{Z}/(n) \quad \text{and} \quad \mathbb{C}[\varepsilon]/(\varepsilon^2)\,[T].$$