Lecture 01: Introduction

Sunday, April 1, 2018 10:29 PM

There are two angles in this course: algebraic number theory, basic properties of certain subrings of number fields (finite extensions of $\mathbb{Q}$), and algebraic geometry, basic properties of common zeros of a family multi-variable polynomials. We will try prove statements in general setting.

In this course all the rings will be assumed to unital and commutative unless we say otherwise. Let's recall for a ring A, $\mathrm{Max}(A) = \{\mathfrak{m} \lhd A \mid \mathfrak{m} \text{ is a maximal ideal}\}$ and

$$\mathrm{Spec}(A) = \{\mathfrak{p} \lhd A \mid \mathfrak{p} \text{ is a prime ideal}\}.$$

- $\mathrm{Max}(A) \subseteq \mathrm{Spec}(A)$
- $\forall\, a \in A \setminus A^{\times}$, $\exists\, \mathfrak{m} \in \mathrm{Max}(A)$ s.t. $a \in \mathfrak{m}$.
- $\forall\, S \subseteq A$ multip. closed, no zero-divisor, $\exists\, \mathfrak{p} \in \mathrm{Spec}(A)$, $S \cap \mathfrak{p} = \emptyset$.
- $\bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathrm{Nil}(A)$

<u>Def.</u> $\bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m} =: J(A)$ is called the Jacobson radical of A.

Lecture 01: Outline of arguments

Monday, April 2, 2018 4:56 PM

- $\mathfrak{m} \in \mathrm{Max}(A) \iff A/\mathfrak{m}$ is a field.
- $\mathfrak{p} \in \mathrm{Spec}(A) \iff A/\mathfrak{p}$ is an integral domain.
- F is a field $\Rightarrow$ F is an integral domain

Suppose $S \subseteq A$ is multiplicatively closed, $\mathfrak{b} \triangleleft A$, s.t. $S \cap \mathfrak{b} = \varnothing$. Then $\Sigma_{\mathfrak{b},S} := \{\mathfrak{a} \triangleleft A \mid \mathfrak{a} \cap S = \varnothing,\ \mathfrak{b} \subseteq \mathfrak{a}\}$ has a maximal element by Zorn's lemma. If $\mathfrak{p}$ is a maximal element of $\Sigma_{\mathfrak{b},S}$, then $\mathfrak{p} \in \mathrm{Spec}(A)$.

- A maximal element of $\Sigma_{\mathfrak{b},\{1\}}$ is a maximal ideal.
- $\left.\begin{array}{l} x^n = 0 \\ \mathfrak{p} \in \mathrm{Spec}(A) \end{array}\right\} \Rightarrow x^n \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ $\Big\} \rightarrow$ $\mathrm{Nil}(A) \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$.
- If $x \notin \mathrm{Nil}(A)$, then $\{1, x, x^2, \dots\} \cap \{0\} = \varnothing \Rightarrow \exists \mathfrak{p} \in \mathrm{Spec}(A),\ x \notin \mathfrak{p}$.

<u>Remark</u>. If A is a non-commutative unital ring, then we define its Jacobson radical to be $\bigcap_{\substack{\mathfrak{m} \\ \text{maximal} \\ \text{left ideal}}} \mathfrak{m}$. It is a theorem that it is equal to $\bigcap_{\substack{\mathfrak{m} \\ \text{max. right ideal}}} \mathfrak{m}$; in particular $J(A) \triangleleft A$. And for any simple A-mod. M, we have $J(A) \subseteq \mathrm{Ann}(M)$.

Lecture 01: Jacobson radical; Chinese remainder

Monday, April 2, 2018 7:59 AM

Lemma. $x \in J(A) \iff \forall y \in A,\ 1-xy \in A^\times$.

Pf. ($\Rightarrow$) For $x \in J(A), y \in A$, suppose $1-xy \notin A^\times$. Then

$\left.\begin{array}{l} \exists\, \mathfrak{m} \in \mathrm{Max}(A) \text{ s.t. } 1-xy \in \mathfrak{m} \\ x \in J(A) \implies x \in \mathfrak{m} \end{array}\right\} \implies 1 \in \mathfrak{m}$ which is a contradiction.

($\Leftarrow$) Suppose $1-xy \in A^\times$ for any $y \in A$, and $x \notin J(A)$.

So $\exists\, \mathfrak{m} \in \mathrm{Max}(A)$ s.t. $x \notin \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\exists\, y \in A$

and $z \in \mathfrak{m}$ s.t. $1 = xy + z$. Hence $1 - xy = z \in \mathfrak{m}$

and so it cannot be a unit, which is a contradiction. ■

Def. We say two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ are coprime if $\mathfrak{a} + \mathfrak{a}' = A$.

Def $\mathfrak{a}, \mathfrak{b} \lhd A$, $\mathfrak{a}\mathfrak{b} := \{\sum_{i=1}^{m} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$.

Observation. $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$;

Theorem (Chinese Remainder) Suppose $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \lhd A$. Then

(1) If $\mathfrak{a}_i$'s are pairwise coprime, then $\bigcap \mathfrak{a}_i = \prod \mathfrak{a}_i$

(2) Let $\phi: A \longrightarrow \prod_{i=1}^{n} A/\mathfrak{a}_i$, $\phi(x) := (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$. Then ϕ is

surjective $\iff$ $\mathfrak{a}_i$'s are pairwise coprime

(3) ϕ is injective $\iff$ $\bigcap_{i=1}^{n} \mathfrak{a}_i = 0$.

Lecture 01: Chinese Remainder;

Monday, April 2, 2018 8:21 AM

Pf. (1) Claim. $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are coprime.

Pf of claim. $\forall 2 \le i \le n$, $\exists\ x_i \in \mathfrak{a}_1$ and $y_i \in \mathfrak{a}_i$ s.t.

$$1 = x_i + y_i \Rightarrow y_2 \cdots y_n = (1-x_2)(1-x_3)\cdots(1-x_n) \in \mathfrak{a}_2 \cdots \mathfrak{a}_n$$

$$\Rightarrow 1 - x \in \mathfrak{a}_2 \cdots \mathfrak{a}_n \text{ for some } x \in \mathfrak{a}_1$$

$$\Rightarrow \mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n = A. \quad \square$$

Case of $n=2$. $\mathfrak{a}_1 + \mathfrak{a}_2 = A \Rightarrow \exists\ x_i \in \mathfrak{a}_i$, $1 = x_1 + x_2$.

$\forall y \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, $y = y \cdot 1 = y(x_1 + x_2) = \underbrace{y x_1}_{\text{in } \mathfrak{a}_2 \mathfrak{a}_1} + \underbrace{y x_2}_{\text{in } \mathfrak{a}_1 \mathfrak{a}_2}$

$\Rightarrow y \in \mathfrak{a}_1 \mathfrak{a}_2$.

General case. We proceed by induction on n.

By the induction hypothesis, $\bigcap_{i=2}^{n} \mathfrak{a}_i = \prod_{i=2}^{n} \mathfrak{a}_i$. So by claim and case of $n=2$ we get

$$\bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{a}_1 \cdot \left(\bigcap_{i=2}^{n} \mathfrak{a}_i\right) = \prod_{i=1}^{n} \mathfrak{a}_i.$$

(2) ($\Rightarrow$) ϕ is surjective $\Rightarrow \exists\ x \in A$ s.t. $(x + \mathfrak{a}_i, x + \mathfrak{a}_j) = (1 + \mathfrak{a}_i, 0 + \mathfrak{a}_j)$

$\Rightarrow 1 - x \in \mathfrak{a}_i$ and $x \in \mathfrak{a}_j \Rightarrow \mathfrak{a}_i + \mathfrak{a}_j = A$.

($\Leftarrow$) By the above claim, $\exists\ x \in \mathfrak{a}_2 \cdots \mathfrak{a}_n$ s.t. $1 - x \in \mathfrak{a}_1$. And so

Lecture 01: Chinese remainder; union of primes

Monday, April 2, 2018 8:36 AM

$\phi(x) = (\bar{1}, \bar{0}, \ldots, \bar{0})$. Similarly $(\bar{0}, \ldots, \bar{0}, \underset{i\text{-th}}{\bar{1}}, \bar{0}, \ldots, \bar{0})$ is in $\phi(A)$. As ϕ is an A-module homomorphism and $\prod_{i=1}^{n} A/\mathfrak{a}_i$ is generated by $(\bar{0}, \ldots, \bar{1}, \ldots, \bar{0})$ as an A-mod, we get surjectivity of ϕ.

(3) $\ker \phi$ is clearly $\bigcap_{i=1}^{n} \mathfrak{a}_i$. ■

Union of ideals is far from being an ideal. We will be needing the following proposition later in this course, and it is a very good indication of the mentioned claim about union of ideals.

<u>Proposition.</u> Suppose $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(A)$. If $\mathfrak{a} \trianglelefteq A$ and $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, then $\exists i$, $\mathfrak{a} \subseteq \mathfrak{p}_i$.

We will prove this next time.