MA 252 notes: Commutative algebra
(Distilled from [Atiyah-MacDonald])

Dan Abramovich

Brown University

January 27, 2016

Conventions

- All rings will be commutative and unitary.
- All ring homomorphisms preserve 1.
- There is one ring with $1 = 0$ (up to unique isomorphism), namely the one ring $\{0\} = \{1\}$.
- Ideals are submodules.
- There are various isomorphism theorems, e.g. $\{\mathfrak{a} \subset \mathfrak{b} \subset A\} \leftrightarrow \{\bar{\mathfrak{b}} \subset A/\mathfrak{a}\}$.
- Prime ideal $\mathfrak{p} \subset A \Leftrightarrow$ quotient is an integral domain.
- Maximal ideal $\mathfrak{m} \subset A \Leftrightarrow$ quotient is a field.
- Zorn $\Rightarrow$: if A is not the one ring, it has a maximal ideal.
- Corollary: there is a maximal ideal containing a given non-unit $a \in A$.
- Corollary: there is a maximal ideal containing a given non-unit ideal $\mathfrak{a} \subset A$.

Examples and notes

- $k[x_1, \ldots, x_n] \ni f$ and f irreducible then (f) prime since UFD.
- Prime ideals in $\mathbb{Z}$ are 0 and (p), with p prime.
- generally in a PID every nonzero prime is maximal: if $(x) \neq 0$ prime and $(y) \supsetneq (x)$ then $x = yt \Rightarrow t \in (x) \Rightarrow t = xz \Rightarrow x = yzx \Rightarrow yz = 1 \Rightarrow (y) = A$.
- The inverse image of prime is prime.
- One forms ideal sums, products, powers, intersections.
- Note: $\mathfrak{a}\mathfrak{b} =$ ideal generated by $\{a, b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$
- $\mathfrak{a}^n = \mathfrak{a}\mathfrak{a} \cdots \mathfrak{a} =$ ideal generated by $\{\prod_{i=1}^n a_i : a_i \in \mathfrak{a}\}$.

Local rings

Recall:

- $a \in A$ nilpotent if there is $n > 0$ such that $a^n = 0$.
- $a \in A$ unit if there is $b \in A$ with $ab = 1$, equivalently $(a) = A$.

Definition

A is a local ring if it has a unique maximal ideal.

Proposition

Given $\mathfrak{m} \neq A$ an ideal.

- *(*) $A \setminus \mathfrak{m} \subset A^\times$ if and only if (**) $(A, \mathfrak{m})$ local.*
- *If $\mathfrak{m}$ maximal and $1 + \mathfrak{m} \subset A^\times$ then $(A, \mathfrak{m})$ local*

$\mathfrak{a} \neq A \Rightarrow \mathfrak{a} \cap A^\times = \emptyset \Rightarrow \mathfrak{a} \subset \mathfrak{m}$. $x \notin \mathfrak{m} \Rightarrow (x, \mathfrak{m}) = a \Rightarrow xy + t = 1 \Rightarrow xy = 1 - t \Rightarrow xy \in A^\times \Rightarrow x \in A^\times$

Nilradicals

Proposition

$\mathfrak{N}(A) := \{x \in A \text{ nilpotent}\}$ *is an ideal, and* $\mathfrak{N}(A/\mathfrak{N}(A)) = 0$.

(use binomial theorem).

Proposition

Let $\mathfrak{N}' = \cap_{P \text{ prime}} P$. *Then* $\mathfrak{N}(A) = \mathfrak{N}'$.

Given P, $f^n = 0 \Rightarrow f^n \in P \Rightarrow f \in P$. So f nilpotent $\Rightarrow f \in \cap P = \mathfrak{N}'$. So $\mathfrak{N}(A) \subset \mathfrak{N}'$.
If f is not nilpotent, let $\Sigma = \{\mathfrak{a} \subset A : f^n \not\in A \forall n > 0\}$. Then $\Sigma \in 0$ and Σ partially ordered by inclusion. If $\mathcal{C} = \{\mathfrak{a}_\alpha\}$ a chain then $\cup \mathfrak{a}_\alpha \in \Sigma$. Let $P \in \Sigma$ be a maximal element. We claim P prime. Suppose $x, y \not\in P$. Then $P + (x), P + (y) \supsetneq P$, so $f^n \in P + (x)$ and $f^m \in P + (y)$, so $f^{n+m} \in P + (xy)$, so $xy \not\in P$, as reuired.
Remark: P comes from a maximal ideal in the localization $A[f^{-1}]$.

Jacobson radicals

$\mathfrak{R}(A) := \cap_{\mathfrak{m}\text{ maximal}}\mathfrak{m}$ for a nonzero ring.

Proposition

$\mathfrak{R}(A) = \{x|1 - xy \in A^\times \forall y\}$.

If for some y the element $1 - xy \notin A^\times$ then $1 - xy \in \mathfrak{m}$ maximal, and so is x, so $1 \in \mathfrak{m}$, contradiction.
If $x \notin \mathfrak{m}$ for some $\mathfrak{m}$, then
$(x, \mathfrak{m}) = 1 \Rightarrow xy + t = 1 \Rightarrow 1 - xy \in \mathfrak{m} \Rightarrow 1 - xy \notin A^\times$.

Observations on operations

- $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.
- but $\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\cap\mathfrak{b} + \mathfrak{a}\cap\mathfrak{c}$ if $\mathfrak{a} \supset \mathfrak{b}$ or $\mathfrak{a} \supset \mathfrak{c}$ (as if $b + c \in \mathfrak{a}$ then in the first case $c \in \mathfrak{a}$)
- $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$,
- and we have equality if $\mathfrak{a}+\mathfrak{b} = 1$ (so giving $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}$ in this case).
- We say $\mathfrak{a}, \mathfrak{b}$ coprime if $\mathfrak{a}+\mathfrak{b} = 1$.

Chinese remainder theorem

Consider ideals $\mathfrak{a}_i$ and homomorphism $\phi : A \to \prod A/\mathfrak{a}_i$.

Proposition

(i) *If $\mathfrak{a}_i$ pairwise coprime then $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$.*

(ii) *ϕ surjective $\Leftrightarrow$ $\mathfrak{a}_i$ pairwise coprime.*

(iii) *ϕ injective $\Leftrightarrow \cap \mathfrak{a}_i = 0$.*

(iii) follows since $\mathrm{Ker}\phi = \cap \mathfrak{a}_i$.
(i) The case $n = 2$ was done on previous page. Assume known for $n-1$, so $\mathfrak{b} := \prod_{i=1}^{n-1} \mathfrak{a}_i = \cap_{i=1}^{n-1} \mathfrak{a}_i$.
Claim: $\mathfrak{a}_n + \mathfrak{b} = 1$. Indeed we have $\mathfrak{a}_i + \mathfrak{a}_n = 1$ so $x_i + y_i = 1$ with $x_1 \in \mathfrak{a}_i$ and $y_i \in \mathfrak{a}_n$. Now $x := \prod x_i \in \mathfrak{b}$ and $x = \prod 1 - y_i \equiv 1 (\mathfrak{a}_n)$.
By the case $n = 2$ we have $\prod \mathfrak{a}_i = \mathfrak{a}_n \mathfrak{b} = \mathfrak{b} \cap \mathfrak{a}_n = \cap \mathfrak{a}_i$.
(ii) If ϕ surjective there is $x_1 \in A$ such that $x \equiv \delta_{i,1} \mod \mathfrak{a}_i$ so $\mathfrak{a}_1 + \mathfrak{a}_i = 1$. For $\leftarrow$ take $x_i + y_i = 1$ as above and $y := \prod y_i \in \mathfrak{a}_n, y \equiv 1 \mod \mathfrak{a}_i$.

ideals and primes

Proposition

(i) $\mathfrak{p}_i, i = 1, \ldots, n$ *primes,* $\mathfrak{a} \subset \cup \mathfrak{p}_i$. *Then* $\mathfrak{a} \subset \mathfrak{p}_i$ *for some* i.
(ii)$\cap \mathfrak{a}_i \subset \mathfrak{p} \Rightarrow \mathfrak{a}_i \subset \mathfrak{p}$ *for some* i. *If* $\mathfrak{p} = \cap \mathfrak{a}_i$ *then* $\mathfrak{p} = \mathfrak{a}_i$ *for some* i.

(i) Suppose true for $n-1$ and assume $\forall i, \mathfrak{a} \not\subset \mathfrak{p}_i$. By induction there is $x_j \in \mathfrak{a}$ such that $x_j \notin \mathfrak{p}_i$ for $i \neq j$. If for some i we have $x \notin \mathfrak{p}_i$ we are done. Otherwise all $x_i \in \mathfrak{p}_i$ and consider $y_j := \prod_{i \neq j} x_i$ and $y = \sum y_j$. Then $y \in \mathfrak{a}$ and for all i we have $y \notin \mathfrak{p}_i$, as needed.
(ii) If $\mathfrak{p} \not\subset \mathfrak{a}_i$ for all i then can choose $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$, so $\prod x_i \in \cap \mathfrak{a}_i \setminus \mathfrak{p}$.
If $\mathfrak{p} = \cap \mathfrak{a}_i$ then by (i) there is i so $\mathfrak{a}_i \subset \mathfrak{p} \subset \mathfrak{a}_i$.

Colon ideals, radicals of ideals

$(\mathfrak{a} : \mathfrak{b}) := \{x \in A : x\mathfrak{b} \subset \mathfrak{a}\}$.
Note: $(0 : \mathfrak{b}) = Ann(\mathfrak{b})$. In general $(\mathfrak{a} : \mathfrak{b}) = Ann(\mathfrak{b}/(\mathfrak{b} \cap \mathfrak{a}))$
$r(\mathfrak{a}) := \{x | \exists n : x^n \in \mathfrak{a}\}$.
Note: $r(\mathfrak{a}) = \phi^{-1}\mathfrak{N}(A/\mathfrak{a})$, where $\phi : A \to A/\mathfrak{a}$. This implies:

Proposition

$r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

The binomial theorem says that $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$. Also $r(\mathfrak{a}) = 1 \Leftrightarrow \mathfrak{a} = 1$. These imply

Proposition

$\mathfrak{a} + \mathfrak{b} = 1 \Leftrightarrow r(\mathfrak{a}) + r(\mathfrak{b}) = 1.$

Ideals and homomorphisms

If $f : A \to B$ and $\mathfrak{b} \subset B$ an ideal then $\mathfrak{b}^c := f^{-1}\mathfrak{b}$ an ideal. If $\mathfrak{a} \subset A$ and ideal one defines $\mathfrak{a}^e := f(\mathfrak{a})B$ the ideal generated in B. We immediately have

Proposition

(i) $\mathfrak{a} \subset \mathfrak{a}^{ec}, \mathfrak{b} \supset \mathfrak{b}^{ce}$, *implying (ii)* $\mathfrak{a}^e = \mathfrak{a}^{ece}, \mathfrak{b}^c = \mathfrak{b}^{cec}$ *and (iii) if* E *is the set of extended and* C *the set of contracted ideals, then* $\mathfrak{b} \mapsto \mathfrak{b}^c$ *is a bijection with inverse* $\mathfrak{a} \mapsto \mathfrak{a}^e$.