Lecture 2: Rings, ideals & modules II.

0) Quotient rings: cont'd.
1) Operations with ideals.
2) Maximal ideals.
3) Prime ideals

Ref's: [AM], Chapter 1, Sections 3 and 6;

BONUS: Non-commutative counterparts 2.

0) Recall Proposition & Exercise 1 from Sec 3.2 of Lec 1.

Examples (of quotient rings)

1) $A=\mathbb{Z}$, $I=(n)$ $(=n\mathbb{Z})$, $A/I=\mathbb{Z}/n\mathbb{Z}$ - residues mod n.

2) $A=\mathbb{Z}[x]$, $d\in\mathbb{Z}$ not a complete square, $I:=(x^2-d)\subset A$.

Claim: A/I is isomorphic to the subring $\mathbb{Z}[\sqrt{d}]:=\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\}$ of $\mathbb{C}$.

Proof:

homomorphism $\varphi: \mathbb{Z}[x]\to\mathbb{Z}[\sqrt{d}]$, $f(x):=f(\sqrt{d})$

• $\varphi(x^2-d)=0 \Rightarrow I\subset\ker\varphi \rightsquigarrow \underline{\varphi}: \mathbb{Z}[x]/I\longrightarrow\mathbb{Z}[\sqrt{d}]$

• $\varphi(a+bx)=a+b\sqrt{d}$ so φ is surjective $\Rightarrow$ [Exer 1] $\underline{\varphi}$ is surj've.

• $\forall f\in\mathbb{Z}[x]$ $\exists!$ $a,b\in\mathbb{Z}$ & $g(x)\in\mathbb{Z}[x] \mid f(x)=a+bx+g(x)(x^2-d)$ (division w. remainder) $\Rightarrow \ker\varphi=I \Rightarrow$ [Exer 1] $\underline{\varphi}$ is injective.

So $\underline{\varphi}: \mathbb{Z}[x]/I \xrightarrow{\sim} \mathbb{Z}[\sqrt{d}]$, an isomorphism.

$\square$

Exercise 1 (to be used below in this lecture)

Here we compare sets of ideals in A & in A/I. Namely show that the following maps are mutually inverse bijections:

$$\begin{array}{ccc} \pi^{-1}(\underline{J}) \in \{\text{ideals } J \subset A \mid J \supset I\} \ni J \\ \uparrow \qquad\qquad\qquad\qquad\qquad\qquad \downarrow \\ \underline{J} \in \{\text{ideals } \underline{J} \subset A/I\} \ni \pi(J) = J/I \end{array}$$

Exercise 2: Let $F_y \in A[x_1, \dots x_n]$, $y \in Y$, where Y is a set. Then there's a bijection between:

(i) Ring homomorphisms $A[x_1,\dots,x_n]/(F_y \mid y \in Y) \longrightarrow B$ and

(ii) $\{\varphi, b_1, \dots b_n\}$, where $\varphi: A \to B$ is a ring homomorphism & $b_i \in B$ are s.t. ${}^{\varphi}F_y(b_1, \dots b_n) = 0$ $\forall y \in Y$. Here ${}^{\varphi}F_y \in B[x_1 \dots x_n]$ is obtained from $F_y \in A[x_1 \dots x_n]$ by applying φ to the coefficients.

This generalizes Example 2 from Section 2 of Lec 1.

1) Operations with ideals

Def: A is commutative ring, pick ideals $I, J \subset A$. Then define:

The **sum** $I + J := \{a + b \mid a \in I, b \in J\} \subset A$,

The **product** $IJ := \{\sum_{i=1}^{k} a_i b_i \mid k \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J\}$,

The **ratio** $I : J := \{a \in A \mid aJ \subset I\}$,

The **radical** $\sqrt{I} := \{a \in A \mid \exists\, n \in \mathbb{Z}_{>0} \text{ w. } a^n \in I\}$.

Proposition: $I\cap J$, $I+J$, IJ, $I:J$, $\sqrt{I}$ are ideals.

Proof for $\sqrt{I}$ (the other parts are exercises):

Need to check

(0) $\sqrt{I}\ni 0$.

(1) $a\in A, b\in\sqrt{I} \Rightarrow ab\in\sqrt{I}$ — here take $a=-1$.

(2) $a,b\in\sqrt{I} \Rightarrow a+b\in\sqrt{I}$

$\Rightarrow \sqrt{I}$ is abelian subgroup.

(0) $\Leftarrow \sqrt{I}\supset I$.

b/c A is commutative

(1): $b\in\sqrt{I} \Rightarrow \exists n$ w. $b^n\in I \Rightarrow (ab)^n = a^n b^n \in I \Rightarrow ab\in\sqrt{I}$.

(2) $a,b\in\sqrt{I} \Rightarrow \exists n$ w. $a^n, b^n\in I$

$$(a+b)^{2n} = \sum_{i=0}^{2n}\binom{2n}{i}a^i b^{2n-i}\in I \Rightarrow a+b\in\sqrt{I}$$

again, use that A is comm've

$\in I$ if $i\geq n$ $\quad\quad$ $\in I$ if $i\leq n$ $\quad\quad$ $\square$

Example (generators): $I=(f_1,\dots f_n)$, $J=(g_1,\dots g_m)$. Then:

- $I+J=(f_1,\dots f_n, g_1,\dots g_m)$: $0\in I,J \Rightarrow f_i, g_j\in I+J \Rightarrow$ $(f_1,\dots f_n, g_1,\dots g_m)\subset I+J$; $I+J\subset(f_1,\dots f_n, g_1,\dots g_m)$ is manifest.

Exercise: Show that $IJ=(f_i g_j \mid i=1,\dots n, j=1,\dots m)$

Rem: For $I\cap J$, $I:J$, $\sqrt{I}$ - generators may be tricky...

Example: $A=\mathbb{Z}$, $I=(a)$. Want to compute $\sqrt{I}$:

$a=p_1^{d_1}\cdots p_k^{d_k}$, p_i primes, $d_i\in\mathbb{Z}_{>0}$.

$b \in \sqrt{I} \Leftrightarrow b^n \vdots a$ for some $n \Leftrightarrow b \vdots p_1 \cdots p_k \Leftrightarrow \sqrt{(a)} = (p_1 \cdots p_k)$.

divisible by

Exercise: for general A, I, show $\sqrt{\sqrt{I}} = \sqrt{I}$.

2) Maximal ideals

2.1) Definition

Def: An ideal $\mathfrak{m} \subset A$ is *maximal* if:

- $\mathfrak{m} \neq A$.
- If $\mathfrak{m}'$ another ideal s.t. $\mathfrak{m} \subseteq \mathfrak{m}' \subsetneq A$, then $\mathfrak{m}' = \mathfrak{m}$.

i.e. maximal = maximal w.r.t. inclusion among ideals $\neq A$.

Lemma (equivalent characterization): TFAE:

(1) $\mathfrak{m}$ is maximal

(2) $A/\mathfrak{m}$ is a field

Proof: We claim that both (1) & (2) are equivalent to:

(3) The only two ideals in $A/\mathfrak{m}$ are $\{0\}$ & $A/\mathfrak{m}$.

(1) $\Leftrightarrow$ (3): b/c of bijection $\{\text{ideals in } A \text{ containing } \mathfrak{m}\} \xrightarrow{\sim} \{\text{ideals in } A/\mathfrak{m}\}$, Exercise 1 in Sec 0.

(3) $\Leftrightarrow$ (2): Remark & exercise in the end of Section 3.1 of Lecture 1. $\square$

2.2) Examples of maximal ideals.

1) $A=\mathbb{Z}$, so every ideal is of the form $(a):=a\mathbb{Z}$ for $a\in\mathbb{Z}$. (a) is maximal $\Leftrightarrow$ a is prime. Indeed, the inclusion $(a)\subseteq(b)$ is equivalent to $b \vdots a$.

2) $A=\mathbb{F}[x]$ ($\mathbb{F}$ is field), (f) is maximal $\Leftrightarrow f$ is irreducible, for the same reason as in the previous example. For example, for $\mathbb{F}=\mathbb{C}$ (or any alg. closed field), the maximal ideals are exactly $(x-\alpha)$ for $\alpha\in\mathbb{F}$.

3) $A=\mathbb{F}[x_1,\dots x_n]$

$\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{F}^n \rightsquigarrow \mathfrak{m}_\alpha:=\{f\in\mathbb{F}[x_1,\dots x_n] \mid f(\alpha)=0\}$ is an ideal (exercise). We claim it's maximal $\Leftrightarrow$ ideal $I\supsetneq\mathfrak{m}_\alpha$ contains 1.

$\exists f\in I$ w. $f(\alpha)\neq 0$. Write f as polynomial in $x_1-\alpha_1,\dots x_n-\alpha_n$ $(\in\mathfrak{m}_\alpha)$ $\rightsquigarrow f=f(\alpha)+g$ w. $g\in\mathfrak{m}_\alpha\subset I \Rightarrow f(\alpha)\in I\Rightarrow 1\in I$.

In fact, this way we get <u>all</u> max. ideals in $\mathbb{F}[x_1,\dots x_n]$, if $\mathbb{F}$ is algebraically closed. This claim, to be proved later in the class, is one of most basic connections between Commutative algebra & Algebraic geometry.

2.3) Existence.

Proposition: Every nonzero (commutative) ring has at least one maximal ideal.

We will prove this later for "Noetherian" rings (all ideals are finitely generated), a justification is that essentially every ring we encounter in this course is Noetherian.

The general proof, based on Zorn's lemma from Set theory ($\Leftrightarrow$ axiom of choice) is provided below as a bonus.

Definitions: Let X be a set.

- A partial order $\leq$ on X is a binary relation s.t.
  - $x \leq x$,
  - $x \leq y$ & $y \leq x \Rightarrow x = y$
  - $x \leq y$ & $y \leq z \Rightarrow x \leq z$

  $\forall\, x, y, z \in X$

- $Y \subseteq X$ is linearly ordered (under $\leq$) if $\forall\, x, y \in Y$ have $x \leq y$ or $y \leq x$.
- poset = a set equipped with partial order.

Example: $X := \{\text{ideals } I \subset A \mid I \neq A\}$, $\leq := \subseteq$

Zorn lemma: Let X be a poset. Suppose that:

(*) $\forall$ linearly ordered subset $Y \subseteq X$ $\exists$ an upper bound in X, i.e $x \in X$ s.t. $y \leq x$ $\forall\, y \in Y$.

Then $\exists$ a maximal element $z \in X$ (i.e. $x \in X$ & $z \leq x \Rightarrow z = x$).

Note that both the condition & the conclusion are essentially vacuous for finite sets.

Proof of Proposition: $X, \leq$ are as in Example. Want to show (*): let Y be linearly ordered subset of X, being linearly ordered in our case means: $\forall\, I, J \in Y$ have $I \subseteq J$ or $J \subseteq I$. Set $\tilde{I} := \bigcup_{I \in Y} I$. We claim this is an ideal, $\neq A$ (note: unlike the intersection, the union of ideals may fail to be an ideal).

Need to show:

(i) $\tilde{I}$ is an ideal $\Leftarrow a+b \in \tilde{I}$ as long as $a, b \in \tilde{I}$,

Check: $a, b \in \tilde{I} = \bigcup_{I \in Y} I \Rightarrow \exists\, I, J \in Y$ s.t. $a \in I$, $b \in J$.
Can assume $I \subseteq J \Rightarrow a, b \in J \Rightarrow a+b \in J \subseteq \tilde{I}$. This shows (i).

(ii) $\tilde{I} \neq A \Leftrightarrow 1 \notin \tilde{I}$

$\tilde{I}$ is an ideal

But $1 \notin I$ for every $I \in Y \Rightarrow \tilde{I} = \bigcup_{I \in Y} I \not\ni 1$

Apply Zorn's lemma to finish the proof of Proposition. $\square$

3) Prime ideals

A is comm've ring.

Definitions:
- $a \in A$ is a **zero divisor** if $a \neq 0$ & $\exists\, b \in A$ s.t. $b \neq 0$ but $ab = 0$.
- A is **domain** if A has no zero divisors.
- Ideal $\mathfrak{p} \subset A$ is **prime** if $\mathfrak{p} \neq A$ & $A/\mathfrak{p}$ is domain.

Lemma: TFAE (the following are equivalent)

i) $\mathfrak{p}$ is prime

ii) If $a, b \in A$ are s.t. $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (note that "$\Leftarrow$" is automatic).

iii) If $I, J \subset A$ are ideals, $IJ \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.

Proof: $\pi: A \twoheadrightarrow A/\mathfrak{p}$, $a \mapsto a + \mathfrak{p}$.

i) $\Leftrightarrow$ ii): $a \notin \mathfrak{p} \Leftrightarrow \pi(a) = 0$, $ab \in \mathfrak{p} \Leftrightarrow \pi(a)\pi(b) = \pi(ab) = 0$.

ii) $\Rightarrow$ iii): $I, J \not\subseteq \mathfrak{p} \Rightarrow \exists\, a \in I \setminus \mathfrak{p}, b \in J \setminus \mathfrak{p} \overset{(ii)}{\Rightarrow} ab \notin \mathfrak{p} \Rightarrow IJ \not\subseteq \mathfrak{p}$.

iii $\Rightarrow$ ii): $I := (a)$, $J := (b)$. Then $I \not\subseteq \mathfrak{p} \Leftrightarrow a \notin \mathfrak{p}$; $IJ \subseteq \mathfrak{p} \Leftrightarrow ab \in \mathfrak{p}$. $\square$

Examples:
- $\mathfrak{m} < A$ max'l $\Leftrightarrow A/\mathfrak{m}$ is field (so domain) $\Rightarrow \mathfrak{m}$ is prime.
- $\{0\} \subset A$ is prime $\Leftrightarrow A$ is domain.
- $A = \mathbb{Z}$. Every ideal is (n) for $n \in \mathbb{Z}$; (n) is prime $\Leftrightarrow \pm n$ is prime or $n = 0$. So every prime is max'l or $\{0\}$.
- Same conclusion for $A = \mathbb{F}[x]$ if $\mathbb{F}$ is field.
- $A = \mathbb{F}[x,y]$, (x) is prime (but not maximal): $\mathbb{F}[x,y]/(x) \xrightarrow{\sim} \mathbb{F}[y]$ (domain but not field).
- The ideal $(xy) \subset \mathbb{F}[x,y]$ is not prime.

BONUS: Non-commutative counterparts part 2.

B1) Proper generalizations or what we discussed in this lecture will be for two-sided ideals. For two such ideals I, J it still makes sense to talk about $I\cap J, I+J, IJ, I:J$ - those are still 2-sided ideals. For $\sqrt{I}$ the situation is more interesting: the definition we gave doesn't produce an ideal (look at $I=\{0\}$ in $Mat_2(\mathbb{C})$). Under some addit'l assumptions, still can define a 2-sided ideal. We'll explain this for $I=\{0\}$, for the general case just take the preimage of $\sqrt{\{0\}}\subset A/I$ under $A\twoheadrightarrow A/I$.

Definition: A two-sided ideal $I\subset A$ is called <u>nilpotent</u> if $\exists\, n\in\mathbb{Z}_{>0} \mid I^n=\{0\}$.

Exercise: The sum of two nilpotent ideals is a nilpotent ideal.

Under additional assumption: A is "Noetherian" for 2-sided ideals there's an automatically unique maximal nilpotent ideal. We take this ideal for $\sqrt{\{0\}}$!

B2) Now we discuss maximal ideals.

Definition: A ring A is called <u>simple</u> if it has only 2 two-sided ideals, $\{0\}$ & A.

Exercise: $\mathrm{Mat}_n(\mathbb{F})$ is simple for any field $\mathbb{F}$.

Premium exercise: $\mathrm{Weyl}_1 = \mathbb{F}\langle x,y\rangle / (xy - yx - 1)$ is simple if $\mathrm{char}\,\mathbb{F} = 0$ & not simple if $\mathrm{char}\,\mathbb{F} > 0$.

A two-sided ideal $\mathfrak{m} \subset A$ is maximal if $A/\mathfrak{m}$ is simple.