Recitation 1: Abstract Algebra Refresher

Scribe: Tomer Manket

1 Rings and Ideals

Definition 1. A *commutative ring with identity* is a set $(R, +, \cdot, 0, 1)$ such that

- $(R, +)$ is an abelian group.
- $(R, \cdot)$ is a commutative monoid.
- The multiplication is distributive with respect to addition, i.e.

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{for all } a, b, c \in R.$$

Example 2. The ring of integers $\mathbb{Z}$, a field k, the polynomial ring $R[X_1, \dots, X_n]$ over a ring R.

Definition 3. An *ideal* of a ring R is a subgroup $I \leq (R, +)$ such that for every $r \in R$ and $a \in I$ we have $ra \in I$. We denote $I \trianglelefteq R$.

Example 4. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. A field k has only trivial ideals - $\{0\}$ and k.

Example 5. Let k be a field and let $S \subseteq k^n$. Define

$$I(S) := \{f \in k[X_1, \dots, X_n] \mid f(p) = 0 \text{ for all } p \in S\}.$$

Then $I(S) \trianglelefteq k[X_1, \dots, X_n]$. Note that if $S_1 \subseteq S_2$ then $I(S_1) \supseteq I(S_2)$.

Definition 6. A proper ideal $I \triangleleft R$ is *prime* if for every $a, b \in R$,

$$ab \in I \implies a \in I \text{ or } b \in I.$$

The *spectrum* of R is

$$\operatorname{Spec}(R) := \{I \triangleleft R \mid I \text{ is prime}\}.$$

Definition 7. A proper ideal $I \triangleleft R$ is *maximal* if there is no proper ideal $J \triangleleft R$ such that $I \subsetneq J$. The *maximal spectrum* of R is

$$\operatorname{MaxSpec}(R) := \{I \triangleleft R \mid I \text{ is maximal}\}.$$

Definition 8. An ideal $I \trianglelefteq R$ is called *principal* if there exists $a \in R$ such that

$$I = \langle a \rangle := Ra = \{ra \mid r \in R\}.$$

Claim 9. *$P \lhd R$ is prime $\iff$ R/P is an integral domain.*

Proof.

$$\begin{aligned} P \text{ is prime} &\iff \text{for every } a, b \in R, \\ &\qquad ab \in P \implies (a \in P \vee b \in P) \\ &\iff \text{for every } a, b \in R, \\ &\qquad \overline{ab} = 0 \implies (\bar{a} = 0 \vee \bar{b} = 0) \\ &\iff R/P \text{ is an integral domain.} \end{aligned}$$

□

Claim 10. *$P \lhd R$ is maximal $\iff$ R/P is a field.*

Proof. Left as an exercise. □

Corollary 11. *Every maximal ideal is prime, i.e.* $\mathrm{MaxSpec}(R) \subseteq \mathrm{Spec}(R)$*.*

Example 12. The ideal $\langle x \rangle$ is maximal in $\mathbb{R}[x]$, since $\mathbb{R}[x]/\langle x \rangle \cong \mathbb{R}$. More generally, if k is a field and $a := (a_1, \ldots, a_n) \in k^n$, then $\mathfrak{m}_a := \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ is a maximal ideal of $k[X_1, \ldots, X_n]$ as

$$k[X_1, \ldots, X_n] \big/ \langle X_1 - a_1, \ldots, X_n - a_n \rangle \cong k.$$

This follows from the first isomorphism theorem, as the substitution homomorphism

$$\begin{aligned} \varphi_a \colon k[X_1, \ldots, X_n] &\longrightarrow k \\ f(X_1, \ldots, X_n) &\longmapsto f(a_1, \ldots, a_n) \end{aligned}$$

is surjective and $\ker \varphi_a = \mathfrak{m}_a$. The inclusion $\mathfrak{m}_a \subseteq \ker \varphi_a$ clearly holds. For the opposite inclusion, suppose $f \in \ker \varphi_a$ and consider the Taylor expansion of $f(X_1, \ldots, X_n)$ around a, which takes the form

$$f = \sum_{i_1 + \ldots + i_n = 0}^{\deg f} b_{i_1, \ldots, i_n} (X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}, \quad b_{i_1, \ldots, i_n} \in k.$$

Then $f(a_1, \ldots, a_n) = 0 \implies b_{0, \ldots, 0} = 0 \implies f \in \mathfrak{m}_a$. Another, more algebraic way to show it is presented in Problem Set 0. The following example shows that not all the maximal ideals of $k[X_1, \ldots, X_n]$ are of the form $\mathfrak{m}_a$ for $a \in k^n$.

Example 13. The ideal $\langle x^2 + 1 \rangle$ is also maximal in $\mathbb{R}[x]$, since $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.

However, when k is algebraically closed then every maximal ideal in $k[X_1, \ldots, X_n]$ is of the form $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ for some $(a_1, \ldots, a_n) \in k^n$. This follows from Hilbert's Nullstellensatz which is a famous result in commutative algebra. Thus, when k is algebraically closed we have a bijection

$$\mathrm{MaxSpec}(k[X_1,\dots,X_n]) \xleftrightarrow{\cong} k^n$$

We will focus on the special cases $n = 1$ and $n = 2$. But first, let us recall some definitions.

Definition 14. Let R be an integral domain and let $0 \neq a \in R$. Then

- a is a *unit* if there exists $b \in R$ such that $ab = 1$. Denote the set of units by $R^\times$.
- a is *prime* if $a \notin R^\times$ and for every $b, c \in R$,

$$a \mid bc \implies a \mid b \text{ or } a \mid c.$$

- a is *irreducible* if $a \notin R^\times$ and for every $b, c \in R$,

$$a = bc \implies b \in R^\times \text{ or } c \in R^\times.$$

Claim 15. *Let R be an integral domain and let $0 \neq a \in R$. Then*

$$\langle a \rangle \text{ is prime} \iff a \text{ is prime} \implies a \text{ is irreducible.}$$

Moreover, if R is a PID, then

$$\langle a \rangle \text{ is prime} \iff a \text{ is prime} \iff a \text{ is irreducible} \iff \langle a \rangle \text{ is maximal.}$$

Let k be an algebraically closed field.

Corollary 16. $\mathrm{MaxSpec}(k[x]) = \{\langle x - a \rangle \mid a \in k\}$ *and* $\mathrm{Spec}(k[x]) = \mathrm{MaxSpec}(k[x]) \cup \{0\}$.

We proceed to the (more interesting) case of plane curves.

Claim 17. *Let $f \in F[x, y]$ be a non-constant polynomial and let*

$$Z(f) := \{(a, b) \in \overline{F} \times \overline{F} \mid f(a, b) = 0\}.$$

Then $Z(f)$ is infinite. In particular, $Z(f) \neq \emptyset$.

Proof. Left as an exercise. □

Claim 18. *Let $f \in F[x, y]$ be a non-constant polynomial. Then the ideal $\langle f \rangle$ of $F[x, y]$ is not maximal.*

Proof. By Claim 17 there exists a point $(a, b) \in \overline{F} \times \overline{F}$ such that $f(a, b) = 0$. Let $\overline{M} := \langle x - a, y - b \rangle \triangleleft \overline{F}[x, y]$. Then M is a maximal ideal of $\overline{F}[x, y]$ (as it is the kernel of the substitution homomorphism $\varphi_{(a,b)} \colon \overline{F}[x, y] \to \overline{F}$).
Now consider $M := \overline{M} \cap F[x, y]$. It is easy to check that M is a proper ideal of $F[x, y]$[1].

[1] In fact, M is a maximal ideal of $F[x, y]$. To see this, consider the restriction of $\varphi_{(a,b)}$ to $F[x, y]$. Its kernel is exactly M and its image is $F[a, b]$, which is an algebraic field extension of F. By the first isomorphism theorem, ${}^{F[x,y]}\!/_{M} \cong F[a, b]$.

Observe that $f(a,b)=0$ implies that $f \in \ker(\varphi_{(a,b)}) = \overline{M}$. Hence $f \in \overline{M} \cap F[x,y] = M$ and so $\langle f \rangle \subseteq M$. If $\langle f \rangle \subsetneq M$ then we are done, so assume $\langle f \rangle = M$. Let $p_a \in F[x]$ be the minimal polynomial of $a \in \overline{F}$. Since $(x-a) \mid p_a$ in $\overline{F}[x]$, we have $p_a \in \overline{M} \cap F[x,y] = M$. Hence $p_a \in \langle f \rangle$, i.e. there exists $g \in F[x,y]$ such that $p_a = fg$. It follows that $f, g \in F[x]$, and since p_a is irreducible in $F[x]$ and f is non-constant, g must be constant. Therefore

$$F[x,y]/\langle f \rangle = F[x,y]/\langle p_a \rangle \cong \left(F[x]/\langle p_a \rangle\right)[y] \cong (F[a])[y].$$

But the latter is not a field, so $\langle f \rangle$ is not maximal in $F[x,y]$. $\square$

Remark. In the above proof we showed that $\langle f \rangle \subseteq M$. As mentioned in the footnote, M is a maximal ideal of $F[x,y]$. Since $\langle f \rangle$ is not maximal, we must have $\langle f \rangle \subsetneq M$.

Claim 19. *Let A be a UFD and let M be a maximal ideal in $A[y]$. If M is not principal, then $M \cap A \neq 0$.*

Proof. Let us prove by contra-positive that if $M \cap A = 0$ then M is principal. Consider the field $L := A[y]/M$ and the natural projection $\varphi \colon A[y] \to L$. The restriction $\varphi|_A \colon A \to L$ is injective, as $\ker(\varphi|_A) = M \cap A = 0$. Thus, if $K = \operatorname{Frac}(A)$, we may extend φ to an injection $\tilde{\varphi} \colon K[y] \to L$ via

$$\tilde{\varphi}\left(\sum_{i=0}^{n} \frac{a_i}{b_i} y^i\right) := \sum_{i=0}^{n} \frac{\varphi(a_i)}{\varphi(b_i)} \varphi(y)^i.$$

The kernel of $\tilde{\varphi}$ is a non-trivial prime ideal of $K[y]$ that contains M. Hence $M \subseteq \ker(\tilde{\varphi}) = \langle f(y) \rangle$ for some monic irreducible $f \in K[y]$. Multiplying f by an appropriate constant to clear the denominators of the coefficients, we may assume that $f \in A[y]$ is primitive. Now, if $g \in M$ then $g \in \langle f \rangle$, i.e. $f \mid g$ in $K[y]$. Since $f, g \in A[y]$ and f is primitive, it follows from Gauss' Lemma that $f \mid g$ in $A[y]$. Thus, $M \subseteq \langle f \rangle$ in $A[y]$. As M is maximal, we conclude that $M = \langle f \rangle$ in $A[y]$. $\square$

Corollary 20. *Let M be a maximal ideal in $k[x,y]$. Then $M \cap k[x] \neq 0$.*

Proposition 21. *Let M be a maximal ideal in $k[x,y]$. Then there exists a point $(a,b) \in k^2$ such that $M = \langle x-a,\, y-b \rangle$.*

Proof. Let $P := M \cap k[x]$. Note that P is a prime ideal of $k[x]$, and by Corollary 20 it is non-zero. By Corollary 16, $P = \langle x-a \rangle$ for some $a \in k$. Hence $x - a \in P \subseteq M$. By symmetry there also exists $b \in k$ such that $y - b \in M$. It follows that $\langle x-a,\, y-b \rangle \subseteq M$, and since both are maximal they must be equal. $\square$

Corollary 22. *Let $f \in k[x,y]$ be an irreducible polynomial and let $C_f := k[x,y]/\langle f \rangle$. Then the map*

$$\begin{aligned} I_f \colon Z(f) &\xrightarrow{\ \approx\ } \operatorname{MaxSpec}(C_f) \\ (a,b) &\longmapsto I_f(a,b) := \langle \overline{x-a},\, \overline{y-b} \rangle \end{aligned}$$

is a bijection.

Proof. The map I_f is well-defined: Let $\pi\colon k[x,y] \to C_f$ denote the natural quotient map. If $(a,b) \in Z(f)$ then $f(a,b) = 0$ so $\langle f \rangle \subseteq \langle x-a,\, y-b \rangle =: M$. Hence $I_f(a,b) = \pi(M) \in \mathrm{MaxSpec}(C_f)$.

- Injectivity: Suppose $I_f(a,b) = I_f(c,d)$. Then $\overline{(x-a)} - \overline{(x-c)} = \overline{c-a} \in I_f(a,b)$. Since $I_f(a,b) \neq k[x,y]$ we must have $\overline{c-a} = \overline{0}$, i.e. $c - a \in \langle f \rangle$ which implies that $c - a = 0$, i.e. $a = c$. Similarly, $b = d$ and therefore $(a,b) = (c,d)$.
- Surjectivity: Let $\overline{M} \in \mathrm{MaxSpec}(C_f)$. Then $\overline{M} = \pi(M)$ for some maximal ideal M of $k[x,y]$ with $\langle f \rangle \subseteq M$. By Proposition 21 there exists $(a,b) \in k^2$ such that $M = \langle x-a,\, y-b \rangle$. Since $f(x,y) \in M$ we find that $f(a,b) = 0$ so that $(a,b) \in Z(f)$. Hence, $I_f(a,b) = \overline{M}$.

□