

§1.2: IDEALS

DEFINITION: Let S be a subset of a ring R . The **ideal generated by S** , denoted (S) , is the smallest ideal containing S . Equivalently,

$$(S) = \left\{ \sum r_i s_i \mid r_i \in R, s_i \in S \right\} \quad \text{is the set of } R\text{-linear combinations}^1 \text{ of elements of } S.$$

We say that S **generates** an ideal I if $(S) = I$.

DEFINITION: Let I, J be ideals of a ring R . The following are ideals:

- $IJ := (ab \mid a \in I, b \in J)$.
- $I^n := \underbrace{I \cdot I \cdots I}_{n \text{ times}} = (a_1 \cdots a_n \mid a_i \in I)$ for $n \geq 1$.
- $I + J := \{a + b \mid a \in I, b \in J\} = (I \cup J)$.
- $rI := (r)I = \{ra \mid a \in I\}$ for $r \in R$.
- $I : J := \{r \in R \mid rJ \subseteq I\}$.

DEFINITION: Let I be an ideal in a ring R . The **radical** of I is $\sqrt{I} := \{f \in R \mid f^n \in I \text{ for some } n \geq 1\}$. An ideal I is **radical** if $I = \sqrt{I}$.

DIVISION ALGORITHM: Let A be a ring, and $R = A[X]$ be a polynomial ring. Let $g \in R$ be a **monic** polynomial; i.e., the leading coefficient of f is a unit. Then for any $f \in R$, there exist unique polynomials $q, r \in R$ such that $f = qg + r$ and the top degree of r is less than the top degree of g .

- (1) Briefly discuss why the two characterizations of (S) in Definition 2.1 are equal.
- (2) Finding generating sets for ideals: Let S be a subset of a ring R , and I an ideal.
- (a) To show that $(S) = I$, which containment do you think is easier to verify? How would you check?
 - (b) To show that $(S) = I$ given $(S) \subseteq I$, explain why it suffices to show that $I/(S) = 0$ in $R/(S)$; i.e., that every element of I is equivalent to 0 modulo S .
 - (c) Let K be a field, $R = K[U, V, W]$ and $S = K[X, Y]$ be polynomial rings. Let $\phi : R \rightarrow S$ be the ring homomorphism that is constant on K , and maps $U \mapsto X^2, V \mapsto XY, W \mapsto Y^2$. Show that the kernel ϕ is generated by $V^2 - UW$ as follows:
 - Show that $(V^2 - UW) \subseteq \ker(\phi)$.
 - Think of R as $K[U, W][V]$. Given $F \in \ker(\phi)$, use the Division Algorithm to show that $F \equiv F_1V + F_0$ modulo $(V^2 - UW)$ for some $F_1, F_0 \in K[U, W]$ with $F_1V + F_0 \in \ker(\phi)$.
 - Use $\phi(F_1V + F_0) = 0$ to show that $F_1 = F_0 = 0$, and conclude that $F \in \ker(\phi)$.
- (3) Radical ideals:
- (a) Fill in the blanks and convince yourself:
 - R/I is a field $\iff I$ is _____
 - R/I is a domain $\iff I$ is _____
 - R/I is reduced $\iff I$ is _____
 - (b) Show that the radical of an ideal is an ideal.
 - (c) Show that a prime ideal is radical.
 - (d) Let K be a field and $R = K[X, Y, Z]$. Find a generating set² for $\sqrt{(X^2, XYZ, Y^2)}$.

¹Linear combinations always means *finite* linear combinations: the axioms of a ring can only make sense of finite sums.

²Hint: To show your set generates, you might consider the bottom degree of F considered as a polynomial in X and Y .

- (4) Evaluation ideals in polynomial rings: Let K be a field and $R = K[X_1, \dots, X_n]$ be a polynomial ring. Let $\alpha = (\alpha_1, \dots, \alpha_n) \in K^n$.
- (a) Let $\text{ev}_\alpha : R \rightarrow K$ be the map of evaluation at α : $\text{ev}_\alpha(f) = f(\alpha_1, \dots, \alpha_n)$, or $f(\alpha)$ for short. Show that $\mathfrak{m}_\alpha := \ker \text{ev}_\alpha$ is a maximal ideal and $R/\mathfrak{m}_\alpha \cong K$.
 - (b) Apply division repeatedly to show that $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$.
 - (c) For $K = \mathbb{R}$ and $n = 1$, find a maximal ideal that is not of this form. Same question with $n = 2$.
 - (d) With K arbitrary again, show that every maximal ideal \mathfrak{m} of R for which $R/\mathfrak{m} \cong K$ is of the form \mathfrak{m}_α for some $\alpha \in K^n$. Note: this is *not* a theorem with a fancy German name.

(5) Lots of generators:

- (a) Let K be a field and $R = K[X_1, X_2, \dots]$ be a polynomial ring in countably many variables. Explain³ why the ideal $\mathfrak{m} = (X_1, X_2, \dots)$ cannot be generated by a finite set.
- (b) Show that the ideal $(X^n, X^{n-1}Y, \dots, XY^{n-1}, Y^n) \subseteq K[X, Y]$ cannot be generated by fewer than $n + 1$ generators.
- (c) Let $R = \mathcal{C}([0, 1], \mathbb{R})$ and $\alpha \in (0, 1)$. Show that for any element $g \in (f_1, \dots, f_n) \subseteq \mathfrak{m}_\alpha$, there is some $\varepsilon > 0$ and some $C > 0$ such that $|g| < C \max_i \{|f_i|\}$ on $(\alpha - \varepsilon, \alpha + \varepsilon)$. Use this to show that \mathfrak{m}_α cannot be generated by a finite set.

(6) Evaluation ideals in function rings: Let $R = \mathcal{C}([0, 1], \mathbb{R})$. Let $\alpha \in [0, 1]$.

- (a) Let $\text{ev}_\alpha : \mathcal{C}([0, 1]) \rightarrow \mathbb{R}$ be the map of evaluation at α : $\text{ev}_\alpha(f) = f(\alpha)$. Show that $\mathfrak{m}_\alpha := \ker \text{ev}_\alpha$ is a maximal ideal and $R/\mathfrak{m}_\alpha \cong \mathbb{R}$.
- (b) Show that $(x - \alpha) \subseteq \mathfrak{m}_\alpha$.
- (c) Show that every maximal ideal \mathfrak{m} of R is of the form \mathfrak{m}_α for some $\alpha \in [0, 1]$. You may want to argue by contradiction: if not, there is an ideal I such that the sets $U_f := \{x \in [0, 1] \mid f(x) \neq 0\}$ for $f \in I$ form an open cover of $[0, 1]$. Take a finite subcover U_{f_1}, \dots, U_{f_t} and consider $f_1^2 + \dots + f_t^2$.

(7) Division Algorithm.

- (a) What fails in the Division Algorithm when g is not monic? Uniqueness? Existence? Both?
- (b) Review the proof of the Division Algorithm.

(8) Let K be a field and $R = K[[X_1, \dots, X_n]]$ be a power series ring in n indeterminates. Let $R' = K[[X_1, \dots, X_{n-1}]]$, so we can also think of $R = R'[[X_n]]$. In this problem we will prove the useful analogue of division in power series rings:

WEIERSTRASS DIVISION THEOREM: Let $r \in R$, and write $g = \sum_{i \geq 0} a_i X_n^i$ with $a_i \in R'$. For some $d \geq 0$, suppose that $a_d \in R'$ is a unit, and that $a_i \in R'$ is *not* a unit for all $i < d$. Then, for any $f \in R$, there exist unique $q \in R$ and $r \in R'[X_n]$ such that $f = qg + r$ and the top degree of r as a polynomial in X_n is less than d .

- (a) Show the theorem in the very special case $g = X_n^d$.
- (b) Show the theorem in the special case $a_i = 0$ for all $i < d$.
- (c) Show the uniqueness part of the theorem.⁴
- (d) Show the existence part of the theorem.⁵

³Hint: You might find it convenient to show that $(f_1, \dots, f_m) \subseteq (X_1, \dots, X_n)$ for some n , and then show that $(X_1, \dots, X_n) \subsetneq \mathfrak{m}$

⁴Hint: For an element of R' or of R , write ord' for the order in the X_1, \dots, X_{n-1} variables; that is, the lowest total X_1, \dots, X_{n-1} -degree of a nonzero term (not counting X_n in the degree). If $qg + r = 0$, write $q = \sum_i b_i X_n^i$. You might find it convenient to pick i such that $\text{ord}'(b_i)$ is minimal, and in case of a tie, choose the smallest such i among these.

⁵Hint: Write $g_- = \sum_{i=0}^{d-1} a_i X_n^i$ and $g_+ = \sum_{i=d}^{\infty} a_i X_n^i$. Apply (b) with g_+ instead of g , to get some q_0, r_0 ; write $f_1 = f - (q_0 g_+ + r_0)$, and keep repeating to get a sequence of q_i 's and r_i 's. Show that $\text{ord}'(q_i), \text{ord}'(r_i) \geq i$, and use this to make sense of $q = \sum_i q_i$ and $r = \sum_i r_i$.