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

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

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 $f = gq + r$ 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.

The set of linear combinations of elements of S is an ideal:

- $0 = 0s_1$ (we also consider 0 to be the empty combination);
- given two linear combinations, by including zero coefficients, we can assume our combinations involve the same elements of S, and then $\sum_i a_i s_i + \sum_i b_i s_i = \sum_i (a_i + b_i) s_i$;
- $r(\sum_i a_i s_i) = \sum_i r a_i s_i$.

Any ideal that contains S must contain all of the linear combinations of S, using the definition of ideal. These two facts mean that the set of linear combinations is the smallest ideal containing S.

(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 $\phi : R \to S$ 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 $F \equiv F_1 V + F_0$ modulo $(V^2 - UW)$ for some $F_1, F_0 \in K[U, W]$ with $F_1 V + F_0 \in \ker(\phi)$.
- Use $\phi(F_1 V + F_0) = 0$ to show that $F_1 = F_0 = 0$, and conclude that $F \in \ker(\phi)$.

(a) Showing $(S) \subseteq I$ is the easier containment: it suffices to show that $S \subseteq I$.

(b) This follows from the Second Isomorphism Theorem.

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

(c)
- We check $\phi(V^2 - UW) = (XY)^2 - X^2Y^2 = 0$, so $V^2 - UW \in \ker(\phi)$. This implies $(V^2 - UW) \subseteq \ker(\phi)$.
- By Division, we have $F = (V^2 - UW)Q + R$, with the top degree (in V) of R at most 1. Then $F \equiv R = F_1V + F_0$ modulo $(V^2 - UW)$. Since $F, V^2 - UW \in \ker(\phi)$, we must have $F_1V + F_0 \in \ker(\phi)$.
- We have $0 = \phi(F_1V + F_0) = F_1(X^2, Y^2)XY + F_0(X^2, Y^2)$. The $F_1(X^2, Y^2)XY$ terms only have monomials whose X-degree is odd, and the $F_0(X^2, Y^2)$ terms only have monomials whose X-degree is even, so none can cancel with each other. This means that $F_1(X^2, Y^2) = 0$ and $F_0(X^2, Y^2) = 0$, so $F_1(U, W) = F_0(U, W) = 0$. Thus, $F \equiv 0$ modulo $(V^2 - UW)$, and as above, we conclude $\ker(\phi) = (V^2 - UW)$.

(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 set[2] for $\sqrt{(X^2, XYZ, Y^2)}$.

(a)
- R/I is a field $\iff$ I is maximal
- R/I is a domain $\iff$ I is prime
- R/I is reduced $\iff$ I is radical

(b) The radical of I is the set of elements that map to a nilpotent in the quotient ring R/I. The nilpotents in R/I form an ideal, the nilradical, and the preimage of that ideal is an ideal, so the radical of I is an ideal.

(c) Suppose I is prime. If $x \in \sqrt{I}$, then $x^n \in I$ for some n. Then, by the definition of prime, $x \in I$. Thus, $\sqrt{I} = I$.

(d) Since X^2 and Y^2 are in (X^2, XYZ, Y^2), we have $X, Y \in \sqrt{(X^2, XYZ, Y^2)}$ by definition, so $(X, Y) \subseteq \sqrt{(X^2, XYZ, Y^2)}$. For the other containment, if $F(X, Y, Z) \notin (X, Y)$, consider F as a polynomial in X, Y with coefficients in $K[Z]$; the condition means that the top degree of F is zero, and hence the top degree of F^n is zero for all n, so $F \notin \sqrt{(X^2, XYZ, Y^2)}$.

(4) Evaluation ideals in polynomial rings: Let K be a field and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$.

(a) Let $\mathrm{ev}_\alpha : R \to K$ be the map of evaluation at α: $\mathrm{ev}_\alpha(f) = f(\alpha_1, \ldots, \alpha_n)$, or $f(\alpha)$ for short. Show that $\mathfrak{m}_\alpha := \ker \mathrm{ev}_\alpha$ is a maximal ideal and $R/\mathfrak{m}_\alpha \cong K$.

(b) Apply division repeatedly to show that $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$.

(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 $\mathfrak{m}_\alpha$ for some $\alpha \in K^n$. Note: this is *not* a theorem with a fancy German name.

(a) The evaluation map is surjective, since for any $k \in K$, the constant function k maps to k. By the First Isomorphism Theorem, $R/\mathfrak{m}_\alpha \cong K$, so $\mathfrak{m}_\alpha$ is maximal.

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

(b) We have $\mathrm{ev}_\alpha(X_i - \alpha_i) = \alpha_i - \alpha_i = 0$, so $(X_1 - \alpha_1, \dots, X_n - \alpha_n) \subseteq \mathfrak{m}_\alpha$. Given some $F \in \mathfrak{m}_\alpha$, consider F as a polynomial in X_1 and apply division by $X_1 - \alpha_1$, to get $F \equiv F_1$ modulo $(X_1 - \alpha_1, \dots, X_n - \alpha_n)$, for some F_1 not involving X_1. Continue with $X_2 - \alpha_2, \dots$ to get the F is equivalent to a constant, which must be zero. This shows that $F \in (X_1 - \alpha_1, \dots, X_n - \alpha_n)$, so $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$.

(c) $(X^2 + 1)$; $(X^2 + 1, Y)$.

(d) Let $\phi : R \to R/\mathfrak{m} \cong K$ be quotient map followed by the given isomorphism. Set $\alpha_i := \phi(X_i)$. Then $X_i - \alpha_i \in \ker(\phi)$, so $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \dots, X_n - \alpha_n) \subseteq \ker(\phi)$. Since $\mathfrak{m}_\alpha$ is maximal, we must have equality.

(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. Explain[3] 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 $\mathfrak{m}_\alpha$ cannot be generated by a finite set.

(a) Suppose $\mathfrak{m} = (f_1, \dots, f_m)$. Since each polynomial involves only finitely many variables, only finitely many variables occur in $\{f_1, \dots, f_m\}$, and since each f_i has no constant term, these polynomials are linear combinations of those variables $X_1, \dots, X_n$; i.e., $(f_1, \dots, f_m) \subseteq (X_1, \dots, X_n)$. It suffices to show that $\mathfrak{m} \neq (X_1, \dots, X_n)$. To see it, take X_{n+1} and note that $X_{n+1} = \sum_{i=1}^n g_i X_i$ is impossible, since the monomial X_{n+1} can't occur in any summand of the right hand side.

(b) Note that this ideal is the set of all polynomial whose bottom degree is at least n. Given a generating set $f_1, \dots, f_m$ for I, consider the degree n terms of the polynomials f_i. We claim that the degree n terms of $f_1, \dots, f_m$ must span the space of degree n polynomials as a vector space. Indeed, given h of degree n, we have $h \in I$, so $h = \sum_i g_i f_i$. But every term of f_i has degree at least n, so the only things of degree n on the right hand side come from the degree n piece of f_i and the degree zero piece of g_i. This shows the claim. Then the statement is clear, since the degree n terms form an $n + 1$ dimensional vector space.

(c) Let $g = \sum g_i f_i \in (f_1, \dots, f_n)$. By continuity, there is some $\varepsilon > 0$ and some $C > 0$ such that $|g_i| < C/n$ on $(\alpha - \varepsilon, \alpha + \varepsilon)$, so $|g| < |\sum_i g_i f_i| \le \sum_i |g_i||f_i| \le \sum_i C/n \max_i\{|f_i|\} \le C \max_i\{|f_i|\}$ on $(\alpha - \varepsilon, \alpha + \varepsilon)$.

Now, given $f_1, \dots, f_n \in \mathfrak{m}_\alpha$, let $g = \sqrt{\max_i\{|f_i|\}}$. Then g is continuous and $g(\alpha) = 0$, so $g \in \mathfrak{m}_\alpha$, but $g/\max_i\{|f_i|\} = 1/g \to \infty$ as $x \to \alpha$, so there is no constant $C > 0$ and no interval $(\alpha - \varepsilon, \alpha + \varepsilon)$ on which $|g| < C \max_i\{|f_i|\}$. Thus, $\mathfrak{m}_\alpha$ is not finitely generated.

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

(a) Let $\mathrm{ev}_\alpha : \mathcal{C}([0, 1]) \to \mathbb{R}$ be the map of evaluation at α: $\mathrm{ev}_\alpha(f) = f(\alpha)$. Show that $\mathfrak{m}_\alpha := \mathrm{ev}_\alpha$ 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 R is of the form $\mathfrak{m}_\alpha$ 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 $f_1^2 + \dots + f_t^2$.

[3]Hint: 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 $(X_1, \dots, X_n) \subsetneq \mathfrak{m}$

(a) $\mathrm{ev}_\alpha : \mathcal{C}([0,1]) \to \mathbb{R}$ is a surjective ring homomorphism, since $\mathrm{ev}_\alpha(r) = r$ for any $r \in \mathbb{R}$. Thus, by the First Isomorphism Theorem, $R/\mathfrak{m}_\alpha \cong \mathbb{R}$, and hence $\mathfrak{m}_\alpha$ is a maximal ideal.
(b) It suffices to note that $\mathrm{ev}_\alpha(x - \alpha) = 0$.
(c) Argue by contradiction: if not, there is a proper ideal I that is not contained in some $\mathfrak{m}_\alpha$; this means that for every α, some element of I does not vanish at α. Since for any continuous f, the set $U_f := \{x \in [0,1] \mid f(x) \neq 0\}$ is open, the collection $\{U_f \mid f \in I\}$ is an open cover of $[0,1]$. Since $[0,1]$ is compact, there is a finite subcover $U_{f_1}, \dots, U_{f_t}$. For these f_i's consider $h = f_1^2 + \cdots + f_t^2$. Each f_i^2 is nonnegative, and for any α, one of these is strictly positive at α. This means that $h(x) \neq 0$ for all $x \in [0,1]$, so h is a unit, and hence $I = R$, a contradiction.

(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 $f = gq + r$ 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]

(a) Given f, write $f = \sum_{i \geq 0} b_i X_n^i$ with $b_i \in R'$. For existence, just take $r = \sum_{i=0}^{d-1} b_i X_n^i$ and $q = \sum_{i=d}^{\infty} b_i X_n^{i-d}$. For uniqueness, note that if $f = gq + r = gq' + r'$ with the top degree of r and r' as polynomials in X_n are less than d. Then $0 = g(q - q') + (r - r')$, so the uniqueness claim reduces to the case $f = 0$; we will use this in the other parts without comment. Every term of r has X_n-degree less than d, whereas every term of qg has X_n-degree at least d, so no terms can cancel. Thus $qg + r = 0$ implies $q = r = 0$ (here and henceforth, we assume r is as in the statement when we write $qg + r$).
(b) If $a_i = 0$ for $i < d$, then $g = X_n^d u$ where $u = \sum_{i \geq 0} a_{i-d} X_n^i$. Since the constant coefficient of u is a_d, which is a unit in R', u is a unit in R. Thus, we can apply (a) to f and X_n^d to get $f = q_0 X_n^d + r_0 = (q_0 u^{-1}) g + r_0$; thus, $q = q_0 u^{-1}$ and $r = r_0$ satisfy the existence clause of the theorem. For uniqueness, if $f = q' g + r'$, then $f = q' u X_n^d + r'$, so by the uniqueness part of (a), we must have $q' u = q_0$ and $r' = r_0$, and thus $q' = q$ and $r' = r$.

[4]Hint: 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 $\mathrm{ord}'(b_i)$ is minimal, and in case of a tie, choose the smallest such i among these.

[5]Hint: Write $g_- = \sum_{i=0}^{t-1} a_i X_n^i$ and $g_+ = \sum_{i=t}^{\infty} a_i X_n^i$. 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 $\mathrm{ord}'(q_i), \mathrm{ord}'(r_i) \geq i$, and use this to make sense of $q = \sum_i q_i$ and $r = \sum_i r_i$.

(c) For an element of R' or of R, write ord' for the order in the $X_1, \ldots, X_{n-1}$ variables; that is, the lowest total $X_1, \ldots, X_{n-1}$-degree of a nonzero term (not counting X_n in the degree). Suppose that $qg + r = 0$, and write $q = \sum_i b_i X_n^i$. Suppose that q is nonzero, so $b_i \neq 0$ for some i. Pick i such that $\operatorname{ord}'(b_i) \leq \operatorname{ord}'(b_j)$ for all j with $b_j \neq 0$, and $\operatorname{ord}'(b_i) = \operatorname{ord}'(b_j)$ implies $i < j$; we can do this by well ordering of $\mathbb{N}$. Say $\operatorname{ord}'(b_i) = t$. Consider the coefficient of X_n^{d+i} in $0 = qg + r$. Byt he degree constraint on r, this is the same as the coefficient of X_n^{d+i} in qg. Multiplying out, this is $\sum_{j=0}^{d+i} a_{d+i-j} b_j$. For $j = i$, the order of $a_d b_i$ is t. For $j < i$, we have $\operatorname{ord}'(a_{d+i-j} b_j) \geq \operatorname{ord}'(b_j) > t$ by choice of i. For $j > i$, since $\operatorname{ord}'(a_{d+i-j}) > 0$ and ord'(b$_j$) $\geq t$, we have $\operatorname{ord}'(a_{d+i-j} b_j) > t$. Thus, the no term can cancel the $a_d b_i$ term, so $qg + r \neq 0$. On the other hand, if $q = 0$ and $r \neq 0$, clearly $qg + r \neq 0$. It follows there there are unique q, r such that $qg + r = 0$.

(d) First, we observe that in the context of (b), if $\operatorname{ord}'(f) = t$, then $\operatorname{ord}'(q), \operatorname{ord}'(r) \geq t$. This is clear in the setting of (a), and following the proof of (b), we just need to observe that if u is a unit in R, then $\operatorname{ord}'(q_0 u^{-1}) \geq \operatorname{ord}'(q_0)$, which is clear since any coefficient of the product $q_0 u^{-1}$ is a sum of multiples of the coefficients of q_0.

Now we begin the main proof. Write $g_- = \sum_{i=0}^{t-1} a_i X_n^i$ and $g_+ = \sum_{i=t}^{\infty} a_i X_n^i$. Apply (b) with g_+ to write $f = q_0 g_+ + r_0$, and set $f_1 = f - (q_0 g + r_0) = -q_0 g_-$. Repeat with f_1 to write $f_1 = q_1 g_+ + r_1$, and $f_2 = f_1 - (q_1 g + r_1) = -q_1 g_-$. Continue like so to obtain a sequence of series $q_0, q_1, \ldots$ and $r_0, r_1, \ldots$. From the observation above, we have that $\operatorname{ord}'(q_i), \operatorname{ord}'(r_i) \geq \operatorname{ord}'(f_i) \geq \operatorname{ord}'(q_{i_1}) + 1$, since the constant term of each coefficient of g_- vanishes. It follows that $\operatorname{ord}'(q_i), \operatorname{ord}'(r_i) \geq i$ for each i.

For a series h, write $[h]_i$ for the degree i part of h, and $[h]_{\leq i}$ for the sum of all parts of degree $\leq i$. Define q to be the series such that $[q]_i = \sum_{j=0}^{i} [q_j]_i$, and likewise with r. Note that r is a still a polynomial in X_n of top degree less than d. We claim that $f = qg + r$. To show this, it suffices to show that $[f]_i = [qg + r]_i$. Note that to compute $[qg + r]_i$, we can replace q, g, r by $[q]_{\leq i}$, and similarly for the others. But $[q]_{\leq i} = [\sum_{j=0}^{i} q_j]_{\leq i}$ (and likewise with r), so $[qg + r]_i = [(\sum_{j=0}^{i} q_j) g + (\sum_{j=0}^{i} r_j)]_i$. Then, by construction of the sequences $\{q_i\}, \{r_i\}, \{f_i\}$, we have $[f - (qg + r)]_i = [f_{i+1}]_i$ and since $\operatorname{ord}'(f_{i+1}) \geq i + 1$, we have $[f_{i+1}]_i = 0$. It follows that $f - (qg + r) = 0$; i.e., $f = qg + r$.