Chapter 1

Affine algebraic sets

1.1 The ideal of a set of points

(1.1.1) Prove the following properties:

(a) $\mathcal{I}$ and $\mathcal{V}$ reverse inclusions.

(b) $\mathcal{I}(\mathcal{V}(S)) \supset S$ for all $S \subset k[x_1, x_2, \ldots, x_n]$. Dually, $\mathcal{V}(\mathcal{I}(X)) \supset X$ for all $V \subset \mathbb{A}^n$.

(c) $\mathcal{V}(\mathcal{I}(\mathcal{V}(S))) = \mathcal{V}(S)$ for S a set of polynomials; $\mathcal{I}(\mathcal{V}(\mathcal{I}(X))) = \mathcal{I}(X)$ for X a set of points.

(a) If $X \supset Y$, then any f vanishing on X must necessarily vanish on all of Y, so $\mathcal{I}(X) \subset \mathcal{I}(Y)$.
Similarly, if $I \supset J$, then any x on which all $f \in J$ vanish must also be a point where all $f \in I$ vanish, so $\mathcal{V}(I) \subset \mathcal{V}(J)$.

(b) $f \in S$ means that it vanishes at all $x \in \mathcal{V}(S)$. Now, $\mathcal{I}(\mathcal{V}(S))$ is the set of functions which vanish all over $\mathcal{V}(S)$, and all $f \in S$ do. Hence $\mathcal{I}(\mathcal{V}(S)) \supset S$.
All $f \in \mathcal{I}(X)$ vanish on X. $\mathcal{V}(\mathcal{I}(X))$ is the set of points where all f vanish, and they certainly do on X.

(c) For all sets X of points in $\mathbb{A}^n$, $\mathcal{V}(\mathcal{I}(X')) \supset X'$. Setting $X' = \mathcal{V}(S)$, we have $\mathcal{I}(\mathcal{V}(\mathcal{I}(X))) \supset \mathcal{I}(X)$. We know that $X \subset \mathcal{V}(\mathcal{I}(X))$. Applying $\mathcal{I}$ reverses inclusions, so that $\mathcal{I}(\mathcal{V}(\mathcal{I}(X))) \subset \mathcal{I}(X)$. Together, we get that $\mathcal{I}(\mathcal{V}(\mathcal{I}(X))) = \mathcal{I}(X)$.
The argument for the other side is almost the exact dual of this, so we omit it.

(1.1.2) $\mathcal{I}(X)$ is radical for any $X \subset \mathbb{A}^n$.

We recall the definition of the radical of an ideal:

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some n } > 0\}$$

A radical ideal is any ideal I for which $I = \sqrt{I}$.

The inclusion $I \subset \sqrt{I}$ is trivial (just take $n = 1$ in the definition). We prove the reverse. For an algebraic set V, $\mathcal{I}(V)$ is the set of all polynomials which vanish everywhere on V, that is:

$$\mathcal{I}(V) := \{f \in k[x_1, x_2, \ldots, x_n] : \forall x \in V. f(x) = 0\}$$

Then

$$\sqrt{\mathcal{I}(V)} = \{f \in k[x_1, x_2, \ldots, x_n] : \forall x \in V. f(x)^n = 0 \text{ for some } n > 0\}$$

But if this holds for any n, then it holds for all n: in particular, it holds for $n = 1$, so this definition reduces to the previous one.

(1.1.3) Consider an algebraic set $W \subset \mathbb{A}^n$, and $p \in \mathbb{A}^n$ not in W. Construct a function that is 0 on W and 1 on p.

$\mathcal{I}(W) \neq \mathcal{I}(W \cup \{p\})$ (if not, then p is in W). Hence, there is at least one polynomial, say g, in the latter ideal that does not belong to the former. The required polynomial function is $\frac{g(x)}{g(p)}$.

1.2 The Hilbert basis theorem

Apparently all algebraic sets are an intersection of a finite number of hypersurfaces. In other words, you can define an algebraic set with a finite number of polynomials in every case!

The Hilbert basis theorem. If R is Noetherian, then $R[x_1, x_2, \ldots, x_n]$ is Noetherian too.

Proof. Note that $R[x_1, x_2, \ldots, x_n]$ is canonically iso to $R[x_1, x_2, \ldots, x_{n-1}][x_n]$, so if we show that R Noetherian implies $R[x]$ Noetherian, then we are done by induction (the base case is obviously R, which is Noetherian by assumption). Let I be an ideal of $R[x]$. We have to find a finite set of generators for I.
Let J be the set of leading coefficients of polynomials in $R[x]$.

Lemma. J is an ideal of R.
Closure under addition: if j and j' are two elements of J corresponding to the

polynomials f and f' of $R[x]$, then the leading coefficient of the polynomial $f + f' \in R[x]$ is $j + j' \in J$.
Closure under R-multiplication: If $j \in J$ corresponds to $f \in R[x]$, then for all $r \in R$, rj is the leading coefficient of $rf \in R[x]$.

Since R is Noetherian, this implies that J is finitely generated. Let the polynomials in $R[x]$ whose leading coefficients generate J be $F = \{F_1, F_2, \ldots, F_r\} \subset I$, and let N be an integer greater than $\max \deg F$.

For each $m \leq N$, let J_m be the ideal of R consisting of the leading coefficients of all $F \in R[x]$ with $\deg F \leq m$. (The argument that this is an ideal is almost identical to that in the lemma.) Let $F_m := F_{m_j}{}_1^k$ be a finite generating set for J_m. (Again, by Noetherian-ness, this exists.)

Crux move: Let I' be the ideal generated by F and all the F_ms. We claim $I \subseteq I'$. Since we have, in that case, constructed a finite generating set for any arbitrary ideal I, will have shown that $R[x]$ is Noetherian.

Assume the contrary, i.e. that there are $G \in I$ not in I'. Choose the one with the least degree. There are then two cases:

(a) $\deg G > N$. We can then find some polynomials Q_i such that $T = \sum Q_i F_i$ has the same leading coefficient as G does. Now, T is an element of I', so $G - T \in I'$. Since I' is an ideal, G must also be in I'.

(b) $\deg G = m \leq N$, then we can lower the degree by subtracting off some $\sum Q_j F_{m_j}$, and $G \in I'$ again.

In both cases, we arrive at a contradiction. Thus, no such G exists, and hence we see that $I' \supseteq I$. Since I' has been shown to be finitely generated, I is too. □

Corollary. For all fields k, $k[x_1, x_2, \ldots, x_n]$ is Noetherian.

Theorem. Any algebraic set V is the intersection of finitely many hypersurfaces.

Proof. Let $V = \mathcal{V}(I)$ for some ideal I of $k[x_1, x_2, \ldots, x_n]$. As an ideal of a polynomial ring over a field, it is finitely generated by the previous theorem. Consider a generating set $F = \{F_1, F_2, \ldots, F_n\}$ for I. Then $V = \mathcal{V}(I) = \mathcal{V}(F_1) \cap \mathcal{V}(F_2) \cap \cdots \cap \mathcal{V}(F_n)$. Each $\mathcal{V}(F_i)$ is the zero set of a single polynomial in $k[x_1, x_2, \ldots, x_n]$, which is by definition a hypersurface. □

(1.2.1) Let $\pi : R \to R/I$ be the projection map from a ring onto a quotient ring. Show that

(a) For every ideal J containing I, $\pi(J)$ is an ideal of R/I, and for every ideal J of R/I, $\pi^{-1}(J)$ is an ideal of R containing J.

(b) If J is mapped to J', then J is radical (resp. prime, maximal) iff J' is.

(c) If J is finitely generated, $\pi(J)$ is as well. Conclude that R/I is Noetherian if R is.

(a) *Proof.* Apply the Correspondence Theorem to π. □

(b) *Maximal ideals.*
This follows trivially from the lattice isomorphism theorem, in both directions. □

Prime ideals.
$\mathfrak{j}$ prime $\implies$ $\pi(\mathfrak{j})$ prime:

Let $\mathfrak{j}$ be a prime ideal in R, and $a'b' = \bar{a}\bar{b} \in \pi(\mathfrak{j})$. Then there are i_a, i_b in I such that $a + i_a, b + i_b \in R$.
Multiply $a + i_a$ and $b + i_b$:

$$(a + i_a)(b + i_b) = ab + (bi_a + ai_b + i_a i_b)$$

Suppose $ab \in \mathfrak{j}$. Then this expression is in $\mathfrak{j}$, since $\mathfrak{j} \supseteq I$. Since $\mathfrak{j}$ is prime, wlog $a \in \mathfrak{j}$, so $a + i_a$ in $\pi(\mathfrak{j})$. Hence, $\mathfrak{j}$ prime implies $\pi(\mathfrak{j})$ prime.

$\pi(\mathfrak{j})$ prime $\implies$ $\mathfrak{j}$ prime:

Let $\bar{a}\bar{b} \in \pi(\mathfrak{j})$. Then $\pi^{-1}(\bar{a}\bar{b}) = ab \in \mathfrak{j}$. Since $\mathfrak{j}$ is prime, wlog $\bar{a} \in \pi(\mathfrak{j})$. Then $a = \pi^{-1}(\bar{a}) \in \mathfrak{j}$. Hence, $\mathfrak{j}$ is prime. □

Radical ideals.
$\mathfrak{j}$ radical $\implies$ $\pi(\mathfrak{j})$ radical:

If $\mathfrak{j}$ is radical, this means that $\sqrt{\mathfrak{j}} \subseteq \mathfrak{j}$. (The other direction holds trivially). Since $I \subseteq \mathfrak{j}$, we can apply π and use the lattice iso theorem:

$$\pi(\sqrt{\mathfrak{j}}) = \sqrt{\pi(\mathfrak{j})} \subseteq \pi(\mathfrak{j}),$$

hence $\pi(\mathfrak{j})$ is a radical ideal too.

$\pi(\mathfrak{j})$ radical $\implies$ $\mathfrak{j}$ radical:

The proof of this is just the previous one in reverse, so we omit it. □

(c) *Proof.* Let J be finitely generated by $f_1, f_2, \ldots, f_n$. Any $j \in \pi(J)$ is the image (residue?) of some $k \in J$. Since there exist a_i such that

$$k = \sum a_i f_i$$

we can apply π to both sides of this to get

$$j = \pi(k) = \pi(\sum a_i f_i) = \sum \pi(a_i)\pi(f_i)$$

so the $\pi(f_i)$ form a finite generating set for $\pi(J)$. Since every ideal in R/I is the homomorphic image of some ideal of R, all ideals of the quotient ring are finitely generated.

□

Alternative proof. We can directly show that for any $\eta : R \to S$, if R is Noetherian, $S' := \operatorname{im} R$ is as well. One way of doing this is the proof given above (note that it does not use the fact that we are mapping into the quotient ring anywhere!), but there is also another way, using the alternative "ascending chain condition" definition of Noetherian-ness.

Let $\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \cdots$ be a chain of ideals in S'. We will show that this must stabilize, by using the fact that homomorphisms preserve inclusions (i.e. basically the lattice isomorphism theorem).

To that end, apply η^{-1} to this chain. This gives us a chain of ideals in R which all contain $\ker \eta$, since $\operatorname{im} R \cong R/\ker \eta$ and hence $\eta(\ker \eta) = (0)$ in S'. This chain must stabilize since R is Noetherian:

$$\eta^{-1}(\mathfrak{i}_1) \subseteq \eta^{-1}(\mathfrak{i}_2) \subseteq \cdots \subseteq \eta^{-1}(\mathfrak{i}_n) = \eta^{-1}(\mathfrak{i}_{n+1}) = \cdots$$

This chain stabilizes at the nth position. Apply η to this again, to get

$$\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \cdots \subseteq \mathfrak{i}_n = \mathfrak{i}_{n+1} = \cdots$$

so this chain stabilizes as well. Hence, $\operatorname{im} R$ is also Noetherian. □

1.3 Irreducible components of an alg. set

Theorem. An algebraic set V is irreducible iff $\mathcal{I}(V)$ is prime.

Proof. Suppose $\mathcal{I}(V)$ is not prime. Then there is some $fg \in \mathcal{I}(V)$ (vanishing all over V) for which $f \notin \mathcal{I}(V), g \notin \mathcal{I}(V)$ (so the factors do not vanish all over $\mathcal{I}(V)$). Then

$$\begin{aligned} V &= V \cap \mathcal{V}(\mathcal{I}(\mathcal{V}(fg))) \\ &= V \cap \mathcal{V}(fg) \\ &= V \cap (\mathcal{V}(f) \cup \mathcal{V}(g)) \\ &= (V \cap \mathcal{V}(f)) \cup (V \cap \mathcal{V}(g)) \end{aligned}$$

and neither of the last two sets are equal to V.

In the other direction, let $V = V_1 \cup V_2$. Pick some f vanishing on V_1 but not all over V_2, and a g vanishing on V_2 but not all over V_1. Then fg vanishes all over V, so $fg \in \mathcal{I}(V)$, but neither f nor g are in $\mathcal{I}(V)$. Hence $\mathcal{I}(V)$ is not prime. □

Theorem.

1.4 Algebraic subsets of the plane

"Weak Bézout's theorem". Let f and g be coprime polynomials in $k[x][y]$. Then f and g intersect in finitely many points.

Proof. Since f and g have no common factors in $k[x][y]$, they also have no common factors in $F = k(x)[y]$. Since F is a PID and f and g are coprime, $(f, g) = (1)$.

From this, we can say that there exist $r, s \in F$ such that $rf + sg = 1$ in F. Then we can "clear fractions" by multiplying by some $d \in k[x][y]$, to get $af + bg = d$.

If the point (p, q) is in $\mathcal{V}(f, g)$, then

$$a(p, q)f(p, q) + b(p, q)g(p, q) = d(p).$$

Now the LHS is zero at common zeros of f and g. If (p, q) is a zero, then $d(p) = 0$, and d has finitely many zeros. Hence the set of x-coordinates is finite in size. A similar argument holds for the y-coordinates (using $k[x](y)$ instead), so the set of common zeros is finite as well. □

Classification of affine varieties. Let k be infinite. Then the irreducible affine subsets of $\mathbb{A}^2_k$ are:

(a) $\mathbb{A}^2_k$

(b) $\emptyset$

(c) points

(d) **irreducible plane curves** $\mathcal{V}(f)$, where f is irreducible and $\mathcal{V}(f)$ is infinite.

Proof. Let V be an irreducible affine algebraic set in $\mathbb{A}^2_k$. Then:

1. *V is finite.* Either V is empty, or V consists of a countable collection of points (x_i, y_i). For $\mathcal{I}(V)$ to be irreducible, there must only be one such point.

2. $\mathcal{I}(V) = (0)$. Then $V = \mathbb{A}^2_k$.

3. Else, $\mathcal{I}(V)$ contains some nonconstant f. Since $\mathcal{I}(V)$ is a prime ideal (since V is irreducible), some irreducible factor of f is also in the ideal. Hence we may assume that f is irreducible as well.

   We claim that $\mathcal{I}(V) = (f)$. Indeed, notice that if $G \in \mathcal{I}(V)$, $g \notin (f)$, then f and g are coprime. ($f = gh$ is ruled out because f is irreducible, and $g = fh$ would imply that $g \in (f)$.) Then $V \subset \mathcal{V}(()f, g)$ is finite, and we go back to case (a).

□

1.5 The Nullstellensatz

Weak Nullstellensatz. If I is a proper ideal in $k[x_1, x_2, \ldots, x_n]$, then $\mathcal{V}(I) \neq \emptyset$.

Proof. Assume I is maximal. (This is okay because there is some maximal ideal J containing I anyway, and $V(I) \supset V(J)$, so it works for this case.) Then $L := k[x_1, x_2, \ldots, x_n]/I$ is a field, and k can be considered a subfield of L.

Suppose that $k = L$. Then, for each $1 \leq i \leq n$, choose some $a_i \in k$ such that $\bar{x_i} = a_i$, i.e. $x_i - a_i \in I$. Then these generate $(x_1 - a_1, \ldots, x_n - a_n)$, which is maximal, hence equal to I. Hence $\mathcal{V}(I) = (a_1, \ldots, a_n) \neq \emptyset$. □

Of course, this hinges on the k being equal to L. In fact, it always is:

Theorem. Suppose k is an algebraically closed subfield of a field L, and there is a ring homomorphism from $k[x_1, x_2, \ldots, x_n]$ onto L. Then $k = L$.

We prove this later. For now, we develop some results that we will need to do so.

"The" Nullstellensatz. Let k be algebraically closed, and I be an ideal in $k[x_1, x_2, \ldots, x_n]$. Then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.

This basically says this: if g and f_i are in $k[x_1, x_2, \ldots, x_n]$, and g vanishes whenever the f_i do, then there is some relation of the form

$$G^N = a_1 f_1 + a_2 f_2 + \cdots + a_n f_n,$$

for $a_i \in k[x_1, x_2, \ldots, x_n]$ and $N > 0$.

Proof. We know that $I \subset \mathcal{I}(\mathcal{V}(I))$, and since I is a radical ideal, that gives us $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$.

To prove the other inclusion, we use the acclaimed "Rabinowitsch trick". Suppose that g is in the ideal $\mathcal{I}(\mathcal{V}(f_1, \ldots f_r)), f_i \in k[x_1, x_2, \ldots, x_n]$. Out of nowhere, we decide to set

$$J := (f_1, f_2, \ldots, f_n, x_{n+1}g - 1) \subset k[x_1, \ldots, x_n, x_{n+1}].$$

Now notice that $\mathcal{V}(J) \subset \mathbb{A}_k^{n+1}$ is empty. By the Weak Nullstellensatz, we see that this is not a proper ideal, and hence (1). This means that $1 \in J$, which in turn means that there is an equation

$$a(x_{n+1}g - 1) + \sum b_i f_i = 1.$$

where a and b are polynomials in $x_1, \ldots, x_n, x_{n+1}$. Let $y := 1/x_{n+1}$. Multiply both sides by a high enough power of y to get

$$y^n = a'(g - y) + \sum b'_i f_i.$$

where a' and b' are polynomials in $x_1, \ldots, x_n, y$. Crux move: Substitute $y = g$. □

We now have a raft of definitions for our algebra-geometry dictionary:

Corollary. Let I be a radical ideal. Then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$. Hence radical ideals correspond to algebraic sets. □

Corollary. Let I be a prime ideal. Then $\mathcal{V}(I)$ is irreducible. Hence prime ideals correspond to irreducible algebraic sets. □

Corollary. Let $f = f_1^{i_1} f_2^{i_2} \cdots f_n^{i_n}$ be a polynomial in $k[x_1, x_2, \ldots, x_n]$. Then $\mathcal{I}(\mathcal{V}(f)) = (f_1 f_2 \cdots f_r)$, and $\mathcal{V}(f) = \mathcal{V}(f_1) \cup \mathcal{V}(f_2) \cup \cdots \cup \mathcal{V}(f_n)$ are the irreducible components of f. Hence, irreducible polynomials correspond to irreducible hypersurfaces in $\mathbb{A}^n$. □

1.5.1 Exercises

(1.5.1) Let V be the set of all points in $\mathbb{A}^3_{\mathbb{C}}$ parametrized by (t, t^2, t^3) where $t \in \mathbb{C}$. Find $\mathcal{I}(V)$ and show that V is irreducible.

Proof. $(z - xy) \supset \mathcal{I}(V)$ is obvious. To prove the reverse inclusion, consider any point parametrized as given. Since $z = xy$ and $y = x^2$, we get $z = x^3, y = x^2, x = x$, so all polynomials in $\mathcal{I}(V)$ vanish on this point.

Now, $\mathbb{C}[x, y, z]/(z - xy) = \mathbb{C}[x, y, xy] = \mathbb{C}[x, y]$, which is a domain: hence $\overline{(z - xy)}$ is prime, implying that V is irreducible. (That might seem hand-wavy: $\overline{f(x, y, z)} \mapsto f(x, y, xy)$ gives an explicit isomorphism.) □

(1.5.2) Let $I := (x^2 + y^2, x^2 - y^2) \subset \mathbb{C}[x, y]$. Find $\mathcal{V}(I)$ and $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I)$.

Solution. If $(x, y) \in \mathcal{V}(I) = \mathcal{V}(x^2 + y^2) \cap \mathcal{V}(x^2 - y^2)$, then $x^2 + y^2 = x^2 - y^2 = 0$, then $y^2 = 0 \implies y = 0$ and, further, $x = 0$ as well. Hence $\mathcal{V}(I) = \{(0, 0)\}$.

Direct computation shows that $\mathbb{C}[x, y]/I$ is the set of all linear combinations of x, y and xy: hence it can be represented as $\mathbb{C}[x, y]/(x^2, y^2)$. □

(1.5.3) k a field, f a polynomial in $k[x]$ of degree $n > 0$. Show that $S := \{\bar{1}, \bar{x}, \bar{x}^2, \cdots, \bar{x}^{n-1}\}$ form a basis of $k[x]/(f)$ over k.

Solution. Take any polynomial g in $R := k[x]/(f)$. We construct a simple algorithm to reduce high powers of x in g until it is a linear combination of elements of S. Let us denote by h the polynomial formed by removing the leading term from f.

Let the leading term of g be ax^{n+t}, $t \geq 0$. Replace it by $ax^t(x^n) = ax^t(f - h) = ax^t f - ax^t h = -ax^t h$. Since the degree of h is lower than that of f, this operation replaces g by another polynomial of lower degree in the same ideal. This can be continued until the highest degree of x in g is $n-1$, at which point we are done.

This procedure expresses any polynomial in R as a finite linear combination of elements of S, so S is a basis of R over k. An example: let $k = \mathbb{C}$, $f = x^3 + x + 3$. Let us try to express $x^5 + x^4 + 2$ in terms of elements from $\{1, x, x^2\}$. This is simple: in $\mathbb{C}[x]/(f)$,

$$\begin{aligned} x^5 + x^4 + 2 &= x^2(x^3 + x + 3) - x^2(x + 3) + x(x^3 + x + 3) - x(x + 3) + 2 \\ &= -x^3 - 3x^2 - x^2 - 3x + 2 \\ &= x + 3 - 4x^2 - 3x + 2 \\ &= -4x^2 - 2x + 5. \end{aligned}$$

□

1.6 Modules and finiteness

1.6.1 Exercises

(1.6.1) Module-finite implies ring-finite.

Solution. Let $T = \{s_1, s_2, \ldots, s_n\}$ be the "generating set" for S as an f.g. module over R. Then $S = R[s_1, s_2, \ldots, s_n]$, so it is ring-finite over R by definition. □

(1.6.2) Show that $R[x]$ is ring-finite over R, but not module-finite.

Solution. By the definition of ring-finiteness, $S = R[x]$ is ring-finite because $R[x] = R[v]$ for $v = x \in S$.

However, it is not module-finite. There is no finite "basis", as that would have to include every power of x. □

(1.6.3) For K, L fields, L ring-finite over K implies that L is an f.g. field ext of K.

Solution. $L = K[v_1, v_2, \ldots, v_n] = K(v_1, v_2, \ldots, v_n)$ since K is a field. □

1.7 Integral elements

1.8 Field extensions

Chapter 2

Affine varieties

2.1 Coordinate rings