1 Unique Factorization

Theorem 1.1. *If R is a unique factorization domain then so is $R[y]$.*

Corollary 1.2. *$K[x_1, \ldots, x_n]$ is a unique factorization domain.*

The key idea of the proof is to let K be the field of fractions of R; that is $K = \{a/b : a, b \in R \text{ and } b \neq 0\}$. We use the fact that $K[y]$ is a UFD to prove $R[y]$ is.

Since R is a UFD, the GCD and LCM are well-defined. For the GCD,

$$\gcd(\prod_i p_i^{e_i}, \prod_i p_i^{f_i}) = \prod_i p_i^{\min(e_i, f_i)}$$

For any element of $f(y) \in K[y]$ we can write it using fractions in lowest terms for coefficients

$$\begin{aligned} f(y) &= \frac{a_n}{b_n} y^n + \frac{a_{n-1}}{b_{n-1}} y^{n-1} \cdots + \frac{a_1}{b_1} y + \frac{a_0}{b_0} \\ &= \frac{A}{B}\Big(\frac{Ba_n}{Ab_n} y^n + \cdots + \frac{Ba_1}{Ab_1} y + \frac{Ba_0}{Ab_0}\Big) \\ &= \frac{A}{B}\tilde{f}(y) \end{aligned}$$

where A is the GCD of the numerators, B is the LCM of the denominators, and $\tilde{f}(y) \in R[y]$ has the MCC.

Definition 1.3. A polynomial $f(y) \in R[y]$ has the **mutually coprime coefficients** (MCC) property when the GCD of the coefficients is 1.

We will write the MCC factorization as $f(y) = \frac{A}{B}\tilde{f}(y)$. Note that $f(y) \in R[y]$ iff $B = 1$.

To prove the UFD theorem we have to prove existence of a factorization. This is done by factoring A, the GCD of the coefficients, using the fact that R is a UFD, and factoring $\tilde{f}(y)$ using the fact that the degree of a factor has to be less than the degree of $\tilde{f}$.

To prove uniqueness the goal to show that an irreducible in $R[y]$ is also prime in $R[y]$. The logic is this: let $\tilde{f}$ have the MCC. If it irreducible in $R[y]$ it is irreducible in $K[y]$. That implies it is prime in $K[y]$. That in turn implies it is prime in $R[y]$. The key property we use is this.

Proposition 1.4. *Let f, g, h be in $R[y]$ such that $f = gh$. Then f has the MCC if and only if each of g and h has the MCC.*

2 $\mathbb{I}$, $\mathbb{V}$ and Their Basic Properties

Throughout this section K is a field, $\mathbb{A}^n = \mathbb{A}^n_K$ is the set of n-tuples of elements of K. The ring $K[x_1, \dots x_n]$ will sometimes be written $K[\bar{x}]$.

Definition 2.1. Let F be a subset of $\mathbb{A}^n$. The **variety** defined by F is

$$\mathbb{V}(F) = \{p \in \mathbb{A}^n : f(p) = 0 \text{ for all } f \in F\}$$

Let S be a set of points in $\mathbb{A}^n$, the **vanishing ideal** of S is

$$\mathbb{I}(S) = \left\{f \in k[\bar{x}] : f(\bar{b}) = 0 \text{ for all } \bar{b} \in S\right\}$$

Proposition 2.2. $\mathbb{V}(F) = \mathbb{V}(\langle F \rangle)$

Proposition 2.3. $\mathbb{I}(S)$ *is not only an ideal, it is a radical ideal.*

Proposition 2.4. *Here are the three key properties of* $\mathbb{I}$ *and* $\mathbb{V}$.

(1) $\mathbb{I}$ *and* $\mathbb{V}$ *are inclusion reversing:*

$$S \subseteq T \text{ implies } \mathbb{I}(S) \supseteq \mathbb{I}(T)$$
$$F \subseteq G \text{ implies } \mathbb{V}(F) \supseteq \mathbb{V}(G)$$

(2) $\mathbb{I} \circ \mathbb{V}$ *and* $\mathbb{V} \circ \mathbb{I}$ *are increasing.*

$$S \subseteq \mathbb{V}(\mathbb{I}(S)) \text{ for any } S \subseteq \mathbb{A}^n$$
$$F \subseteq \mathbb{I}(\mathbb{V}(F)) \text{ for any } F \subseteq K[\bar{x}]$$

(3) The operations stabilize.

$$\mathbb{I}\big(\mathbb{V}(\mathbb{I}(S)\big) = \mathbb{I}(S)$$
$$\mathbb{V}\big(\mathbb{I}(\mathbb{V}(F))\big) = \mathbb{V}(F)$$

Corollary 2.5. *If* V *and* W *are varieties,* $V \subseteq W$ *if and only if* $\mathbb{I}(V) \supseteq \mathbb{I}(W)$.

3 Operations Interacting with $\mathbb{I}$ and $\mathbb{V}$

Here we look at the correspondence between set operations (intersection and union) on varieties and operations on ideals. As with the inclusion-reversing property of $\mathbb{I}$ and $\mathbb{V}$, there is a reversing aspect when considering these operations.

Recall that for ideals I and J in a ring,

$$I + J = \{f + g : f \in I \text{ and } g \in J\} \qquad \text{(This set is already an ideal!)}$$
$$IJ = \langle fg : f \in I \text{ and } g \in J\rangle \qquad \text{(The ideal generated by the products.)}$$

As an exercise, show that $IJ \subseteq I \cap J$.

Proposition 3.1. *Let I and J be ideals in $K]\bar{x}]$.*

$$\mathbb{V}(I) \cap \mathbb{V}(J) = \mathbb{V}(I + J) = \mathbb{V}(I \cup J),$$
$$\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cap J) = \mathbb{V}(IJ)$$

Thus, the intersection and the union of two varieties is a variety.

Definition 3.2. The **Zariski topology** on $\mathbb{A}^n$ is defined by letting the closed sets be varieties. The open sets are the complements of varieties.

Proposition 3.3. *The Zariski topology does indeed satisfy the requirements of a topology.*

(1) A finite union of closed sets (that is, varieties) is closed.

$$\mathbb{V}(I_1) \cup \mathbb{V}(I_2) \cup \cdots \cup \mathbb{V}(I_t) = \mathbb{V}\Big(I_1 \cap I_2 \cap \cdots \cap I_t\Big)$$

(2) An arbitrary intersection of closed sets is closed. For any index set S,

$$\bigcap_{s\in S} \mathbb{V}(I_s) = \mathbb{V}\Big(\sum_{s\in S} I_s\Big) = \mathbb{V}\Big(\bigcup_{s\in S} I_S\Big)$$

4 Ideal Properties: radical, prime and maximal

For any set $S \subseteq \mathbb{A}^n$, $\mathbb{I}(S)$ is a radical ideal.

For a point $\bar{a} = (a_1, a_2, \ldots, a_n)$, $\mathbb{I}(\bar{a}) = \langle x - a_1, \ldots, x - a_n\rangle$ is a maximal ideal.

Definition 4.1. A variety $V \subseteq \mathbb{A}^n$ is **irreducible** when it satisfies the following property. For varieties W_1, W_2, if $V = W_1 \cup W_2$ then either $V = W_1$ or $V = W_2$.

It is easy to show that V is irreducible if and only if it satisfies this property: If $V \subseteq W_1 \cup W_2$ then $V \subseteq W_1$ or $V \subseteq W_2$.

Proposition 4.2. *V is irreducible if and only if $\mathbb{I}(V)$ is prime.*

This is all very neat, but notice that some maximal ideals do not correspond to points: $\langle x^2 + 1\rangle$ in $\mathbb{R}[x]$. Also, some prime ideals do not correspond to irreducible varieties: $\langle x^2(x-1)^2 + y^2\rangle$ in $\mathbb{R}[x, y]$. You may observe a similar problem arises in both cases.

5 Hilbert's Nullstellensatz

Definition 5.1. Let I be an ideal in any ring R. The **radical** of I is

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

It is straightforward to verify that $\sqrt{I}$ is not only an ideal, it is a radical ideal.

Theorem 5.2. *Suppose that K is algebraically closed. Then $\mathbb{IV}(I) = \sqrt{I}$.*

This gives a 1-1 correspondence between points in, irreducible varieties, and arbitrary varieties with, respectively, maximal ideals, prime ideals, and radical ideals.

Table 1: The Algebra Geometry Dictionary

In $K[X_1, \ldots, x_n]$		Varieties in $\mathbb{A}^n$
Q a radical ideal	$\longleftrightarrow$	$\mathbb{V}(Q)$ a variety
P a prime ideal	$\longleftrightarrow$	$\mathbb{V}(P)$ an irreducible variety
M a maximal ideal	$\longleftrightarrow$	$\mathbb{V}(M)$ a point in $\mathbb{A}^n$
f an irreducible polynomial	$\longleftrightarrow$	$\mathbb{V}(f)$ an irreducible variety of dimension $n-1$
$Q_1 \cap Q_2$ (is still radical!)	$\longleftrightarrow$	$\mathbb{V}(Q_1) \cup \mathbb{V}(Q_2)$
$\sqrt{Q_1 + Q_2}$ (have to take the radical!)	$\longleftrightarrow$	$\mathbb{V}(Q_1) \cap \mathbb{V}(Q_2)$

Next we look at ring homomorphisms and *continuous* maps (in the Zariski topology) of varieties.

6 Problems

Problems 6.1. The Mutually Coprime Coefficients Property

Let R be an integral domain. Let $f = gh$ in $R[y]$. Prove that f has the MCC if and only if g and h both have the MCC. Hints follow:

(a) $\Longrightarrow$ Show that if either g or h does not have the MCC then f does not have the MCC.

(b) $\Longleftarrow$ Let p be any prime in R. Let k be minimal such that p does not divide g_k, let j be minimal such that p does not divide h_j. Consider f_{jk} (the index is j times k).

Problems 6.2. Use ideas from Theorem 1.1 and $\big(K(x)\big)[y]$ in the following.

(a) Let $f(x,y)$ and $g(x,y)$ be polynomials with no common factor. Show that a Groebner basis for $\langle f, g\rangle$ with lex $y > x$, has a polynomial with leading term x^m.

(b) Show that $\mathbb{V}(f,g)$ in $\mathbb{A}^2$ consists of a finite number of points.

Problems 6.3. Details to clean up: ideals

(a) Show that $IJ \subseteq I \cap J$ for ideals I, J in a ring R.

(b) Let I be an ideal in a ring R. Prove that $\sqrt{I}$ is an ideal and is radical.

Problems 6.4. Details to clean up: varieties

(a) Show that $\mathbb{V}(IJ) \supseteq \mathbb{V}(I \cap J) \supseteq \mathbb{V}(I) \cup \mathbb{V}(J)$ using just the inclusion reversing property of $\mathbb{V}$.

(b) Prove: for varieties V, W, $V \subseteq W$ if and only if $\mathbb{I}(V) \supseteq \mathbb{I}(W)$.

(c) Prove that V is irreducible if and only if $V \subseteq W_1 \cup W_2$ implies that $V \subseteq W_1$ or $V \subseteq W_2$.

Problems 6.5. An irreducible variety [CR: 2.3.7] over any infinite field.

(a) Show that a general element of the ring $K[x,y]/\langle xy-1\rangle$ may be expressed in a unique way as $a + \tilde{x}f(\tilde{x}) + \tilde{y}g(\tilde{y})$ where $\tilde{x} = x + \langle xy-1\rangle$ and similarly for $\tilde{y}$.

(b) Compute the product of two arbitrary general elements.

(c) Show that $K[x,y]/\langle xy-1\rangle$ has no zero-divisors, and conclude that $\langle xy-1\rangle$ is a prime ideal.

(d) Show that for a given $f \in K[x,y]/\langle xy-1\rangle$ that there is some $m \in \mathbb{N}$ such that $x^m f$ is equal to a polynomial in $\tilde{x}$.

(e) Use the previous result and the fact that K is infinite to show that no nonzero element of $K[x,y]/\langle xy-1\rangle$ can vanish on all points of $\mathbb{V}(xy-1)$. Conclude that $\mathbb{V}(xy-1)$ is irreducible.

Problems 6.6. Homomorphisms and ideal properties

Let $\varphi : R \longrightarrow S$ be a homomorphism of rings.

(a) If Q is a radical ideal in S prove that $\varphi^{-1}(Q)$ is a radical ideal in R.

(b) If P is a prime ideal in S prove that $\varphi^{-1}(P)$ is a prime ideal in R.

(c) If M is a maximal ideal in S show that $\varphi^{-1}(M)$ may *not* be maximal in R.

(d) If φ is surjective and M is a maximal ideal in S show that $\varphi^{-1}(M)$ is maximal in R.