3. Points and Irreducible Varieties

3.1 Definition: Let R be a commutative ring. An ideal P in R is called **prime** if $P \neq R$ and for all $a, b \in R$, if $ab \in P$ then $a \in P$ or $b \in P$. An ideal M in R is called **maximal** if $M \neq R$ and there is no ideal A with $M \subsetneqq A \subsetneqq R$. Recall that every maximal ideal in R is prime. Also recall that for any ideal $A \subsetneqq R$, A is prime if and only if R/A is an integral domain, and A is maximal if and only if R/A is a field. Recall also that in a unique factorization domain such as $\mathbf{F}[x_1, \cdots, x_n]$, an element f is irreducible if and only if the principal ideal $\langle f \rangle$ is prime.

3.2 Theorem: *(The Correspondence Between Points and Maximal Ideals) Let X be a variety in $\mathbf{F}^n$. Then X consists of a single point if and only if $I(X)$ is maximal. Indeed, if $a = (a_1, \cdots, a_n) \in \mathbf{F}^n$ and $M = \big\langle x_1 - a_1, \cdots, x_n - a_n \big\rangle$ so that $\{a\} = V(M)$, then $I(\{a\}) = M$ and M is maximal.*

Proof: Note that if $I(X)$ is maximal then by the correspondence between varieties and closed ideals, X must be minimal, which means that X must consist of a single point.

Conversely, let $X = \{a\}$ and let $M = \big\langle x_1 - a_1, \cdots, x_n - a_n \big\rangle$ so that $X = \{a\} = V(M)$. We claim that $I(X) = M$. We have $I(X) = I(V(M))$ and we know that $M \subseteq I(V(M))$. We need to show that $I(V(M)) \subseteq M$. Suppose that $f \in I(V(M)) = I(\{a\})$ so $f(a) = 0$. Write f in the form $f = \sum c_{k_1, \cdots, k_n} (x_1 - a_1)^{k_1} \cdots (x_n - a_n)^{k_n}$ $\big($this can be done by replacing each occurence of x_i in f by $((x_i - a_i) + a_i)$ and expanding$\big)$. Then since $f(a) = 0$, we have $c_{0, \cdots, 0} = 0$ so that $f \in \big\langle x_1 - a_1, \cdots, x_n - a_n \big\rangle = M$. Thus $I(X) = M$, as claimed.

It remains to show that M is a maximal ideal. Define $\phi : \mathbf{F}[x_1, \cdots, x_n]/M \to \mathbf{F}$ by $\phi(f + M) = f(a)$. Verify that ϕ is a well-defined bijective ring homomorphism, so we have $\mathbf{F}[x_1, \cdots, x_n]/M \cong \mathbf{F}$, which is a field, and so M is maximal.

3.3 Definition: Let X be a non-empty variety in $\mathbf{F}^n$. X is called **irreducible** if it cannot be decomposed into a union $X = Y \cup Z$ of two proper subvarieties $Y \subsetneqq X$, $Z \subsetneqq X$. Otherwise, X is called **reducible**

3.4 Example: In $\mathbf{R}^2$, the varieties $V(xy)$, $V((y - x^2)(x + y - 2))$ and $V(y - x^2, x + y - 2)$ are all reducible since they can be decomposed into proper subvarieties as $V(xy) = V(x) \cup V(y)$, $V((y - x^2)(x + y - 2)) = V(y - x^2) \cup V(x + y - 2)$ and $V(y - x^2, x + y - 2) = \{(-2, 4)\} \cup \{(1, 1)\}$ $= V(x + 2, y - 4) \cup V(x - 1, y - 1)$.

3.5 Example: If $\mathbf{F}$ is a finite field, then the irreducible varieties in $\mathbf{F}^n$ are precisely the one-point sets.

3.6 Theorem: *(The Correspondence Between Irreducible Varieties and Prime Ideals) Let X be a variety in $\mathbf{F}^n$. Then X is irreducible if and only if $I(X)$ is prime.*

Proof: Suppose that X is irreducible. Note that $X \neq \emptyset$ implies that $I(X) \neq \mathbf{F}[x_1, \cdots, x_n]$. Suppose that $f \notin I(X)$ and $g \notin I(X)$. Choose $a \in X$ so that $f(a) \neq 0$ and choose $b \in X$ so that $g(b) \neq 0$. Let $Y = X \cap V(f)$ and let $Z = X \cap V(g)$. Then $Y \subsetneqq X$ (since $a \in X \setminus Y$) and $Z \subsetneqq X$ (since $b \in X \setminus Z$) so, since X is irreducible, we must have $Y \cup Z \subsetneqq X$. Choose $c \in X \setminus (Y \cup Z)$. Since $c \notin Y$ we have $f(c) \neq 0$, and since $c \notin Z$ we have $g(c) \neq 0$, and so $(fg)(c) \neq 0$. Thus $fg \notin I(X)$. This shows that $I(X)$ is prime.

Conversely, suppose that $I(X)$ is prime. Note that $I(X) \neq \mathbf{F}[x_1, \cdots, x_n]$ implies that $X \neq \emptyset$. Suppose, for a contradiction, that X is reducible, say $X = Y \cup Z$ where Y and Z are proper subvarieties of X. Since $Y \subsetneqq X$ and $Z \subsetneqq X$ we have $I(X) \subsetneqq I(Y)$ and $I(X) \subsetneqq I(Z)$, so we can choose $f \in I(Y) \setminus I(X)$ and $g \in I(Z) \setminus I(X)$. Since $f \in I(Y)$ and $g \in I(Z)$ we have $fg \in I(Y \cup Z) = I(X)$. Since $I(X)$ is prime we have $f \in I(X)$ or $g \in I(X)$, which contradicts our choice of f and g. Thus X is irreducible.

3.7 Example: Recall that if $\mathbf{F}$ is an infinite field and $X = V(y - f(x)) \subset \mathbf{F}^2$ is the graph of $f \in \mathbf{F}[x]$, then $I(X) = \langle y - f(x) \rangle$. Since $y - f(x)$ is irreducible in $\mathbf{F}[x, y]$ (since it is monic and linear in y), the ideal $I(X) = \langle y - f(x) \rangle$ is prime. Thus X is irreducible. Similarly, varieties of the form $Y = V(x - f(y))$ are irreducible.

3.8 Example: Verify (using an inductive argument) that if $\mathbf{F}$ is an infinite field then $I(\mathbf{F}^n) = \{0\}$. Since $\{0\}$ is a prime ideal, it follows that $\mathbf{F}^n$ is irreducible. On the other hand, if $\mathbf{F}$ is finite then $\mathbf{F}^n$ is a finite set of points, which is reducible.

3.9 Theorem: *(The Decomposition of a Variety into Irreducible Components) Every nonempty affine variety X can be decomposed as a finite union $X = X_1 \cup \cdots \cup X_l$ of irreducible varieties, with no X_i being a subset of any X_j when $i \neq j$. This decomposition is unique up to order, and the varieties X_i are called the* **irreducible components** *of X.*

Proof: First we claim that for any reducible variety X, we can find varieties $Y \subsetneqq X$ and $Z \subsetneqq X$ with Z irreducible such that $X = Y \cup Z$. Let X be a reducible variety, and say $X = Y_1 \cup Z_1$ where $Y_1 \subsetneqq X$ and $Z_1 \subsetneqq X$. If Z_1 is irreducible then we are done (with $Y = Y_1$ and $Z = Z_1$). Otherwise say $Z_1 = Y_2 \cup Z_3$ with $Y_2 \subsetneqq Z_1$ and $Z_2 \subsetneqq Z_2$. Then $X = Y_1 \cup Y_2 \cup Z_3$. If Z_3 is irreducible we are done (with $Y = Y_1 \cup Y_2$ and $Z = Z_3$). Otherwise say $Z_3 = Y_3 \cup Z_4$, and so on. Eventually this process must end, since otherwise we would obtain an infinite chain $Z_1 \supsetneqq Z_2 \supsetneqq \cdots$ of varieties, and hence an infinite chain $I(Z_1) \subsetneqq I(Z_2) \subsetneqq \cdots$ of ideals, which is impossible by the Hilbert basis theorem.

Now suppose that X is any nonempty affine variety. We shall show the existence of the required decomposition. If X is irreducible then we are done (with $X_1 = X$). Otherwise, by the claim proven above, we can say $X = X_1 \cup Y_2$ with $X_1 \subsetneqq X$, $Y_2 \subsetneqq X$ and X_1 irreducible. If Y_2 is irreducible then we are done (with $X_2 = Y_2$). Otherwise we can say $Y_2 = X_2 \cup Y_3$ with $X_2 \subsetneqq Y_2$, $Y_3 \subsetneqq Y_2$ and X_2 irreducible. If Y_3 is irreducible then we are done (with $X_3 = Y_3$). Otherwise we continue the procedure. As above, the procedure must end, so we obtain $X = X_1 \cup X_2 \cup \cdots X_l$ for some irreducible X_i. By discarding some of the varieties X_i if necessary, we can assume that no X_i is a subset of any other X_j.

Finally we show the uniqueness of this kind of decomposition. Suppose that X admits two such decompositions, say $X = X_1 \cup \cdots \cup X_l = Y_1 \cup \cdots \cup Y_m$. Fix an index i. We have $X_i = X \cap X_i = (Y_1 \cup \cdots \cup Y_m) \cap X_i = (Y_1 \cap X_i) \cup \cdots \cup (Y_m \cap X_i)$. Since X_i is irreducible we must have $Y_j \cap X_i = X_i$ for some j, and so $Y_j \subseteq X_i$. By a similar argument, we also have $X_k \subseteq Y_j$ for some k. Then $X_k \subseteq X_i$ which implies that $k = i$. But then we have $X_k = X_i \subseteq Y_j \subseteq X_i$ which implies that $Y_j = X_i$. Thus each X_i is equal to some Y_j and similarly each Y_j is equal to some X_i.

3.10 Example: Since, for infinite fields, varieties of the form $V(y - f(x))$ and $V(x - f(y))$ are irreducible, and since points are irreducible varieties, the decompositions of example 3.4 were in fact decompositions into irreducible components.

3.11 Theorem: *(The Classification of Irreducible Varieties in the Affine Plane) Let* $\mathbf{F}$ *be an infinite field. Let* $f, g \in \mathbf{F}[x, y]$. *Then*

(1) If f *and* g *have no common factors then* $V(f) \cap V(g)$ *is finite.*
(2) If f *is irreducible and* $X = V(f)$ *is an infinite set then* X *is irreducible with* $I(X) = \langle f \rangle$.
(3) The irreducible varieties in $\mathbf{F}^2$ *are the one-point sets, the infinite sets of the form* $V(f)$ *with* f *irreducible, and* $\mathbf{F}^2$ *itself.*

Proof: Before beginning the proof, we recall that if R is a unique factorization domain with quotient field Q, then if a polynomial $f \in R[x]$ factors over Q as $f = hk$, where $h, k \in Q[x]$, then f factors over R as $f = u\bar{h}\bar{k}$, where u is a greatest common divisor of the coefficients of f in R and where $\bar{h} \in R[x]$ is obtained from $h \in Q[x]$ by first multiplying h by the least common multiple of the denominators of its coefficients, and then by dividing the resulting polynomial by the greatest common divisor of its coefficients. In particular, for $f, g \in R[x]$, if f and g have a common factor $h \in Q[x]$, then they also have a common factor $\bar{h} \in R[x]$.

To prove part 1, suppose that f and g have no common factors in $\mathbf{F}[x][y]$. Then f and g have no common factors in $\mathbf{F}(x)[y]$. Using the Euclidean Algorithm we can find $s, t \in \mathbf{F}(x)[y]$ such that $f(x, y)s(x, y) + g(x, y)t(x, y) = 1 \in \mathbf{F}(x)[y]$. Multiply this by a common multiple $r(x)$ of the denominators of all the coefficients of s and t to get $f(x, y)p(x, y) + g(x, y)q(x, y) = r(x) \in \mathbf{F}[x, y]$. Then for every $(x, y) \in V(f) \cap V(g)$ we have $f(x, y) = 0$ and $g(x, y) = 0$ so that $r(x) = 0$. Since r can only have finitely many roots, there are only finitely many values of x for which $(x, y) \in V(f) \cap V(g)$ for some y. Similarly, there are finitely many values of y for which $(x, y) \in V(f) \cap V(g)$ for some x.

To prove part 2, let f be irreducible and suppose that $X = V(f)$ is infinite. We have $\langle f \rangle \subseteq I(V(\langle f \rangle)) = I(X)$. Let $g \in I(X)$. Then $V(f) = X = V(I(X)) \subseteq V(g)$ so $V(f) \cap V(g) = V(f)$, which is infinite. By part 1, f and g must have a common factor. Since f is irreducible, this implies that f is a factor of g, so $g \in \langle f \rangle$. This shows that $I(X) = \langle f \rangle$. Since f is irreducible, $\langle f \rangle$ is prime, and since $I(X) = \langle f \rangle$ is prime, X is irreducible.

Finally, we prove part 3. Let $X \subset \mathbf{F}^2$ be an irreducible variety. If X is finite, then since X is irreducible, X can only be a one-point set. Suppose that X is infinite. If $I(X) = \{0\}$ then $X = \mathbf{F}^2$. Suppose that $I(X) \neq \{0\}$. Choose $0 \neq h \in I(X)$. Note that h is not constant, since otherwise we would have $X = \emptyset$. Since X is irreducible, $I(X)$ is prime, and so some irreducible factor, say f, of h must also lie in $I(X)$. We claim that $I(X) = \langle f \rangle$. Indeed, for $g \in I(X)$, we have $X \subseteq V(g)$ and we have $X \subseteq V(f)$, so that $X \subseteq V(f) \cap V(g)$, and hence $V(f) \cap V(g)$ is infinite and so, as in the proof of part 2, we must have $g \in \langle f \rangle$.

3.12 Example: In $\mathbf{R}^2$, the varieties $V(x^2+y^2-1)$, $V(x^2-y^2-1)$ and $V(y^2-x^3+x^2)$ are irreducible, since they are all infinite sets and since the polynomials x^2+y^2-1, x^2-y^2-1 and $y^2-x^3+x^2$ are all irreducible in $\mathbf{F}[x, y]$.

3.13 Example: Let $f(x, y) = (x^4 - y^4)(x^5y^2 + x^3y^3 - x^4y + x^4) \in \mathbf{R}[x, y]$. Find the irreducible components of $V(f) \subset \mathbf{R}^2$.

Solution: We can factor f as $f(x, y) = (x^2 + y^2)(x + y)(x - y)(x^3)(y^3 + x^2y - xy + x)$, so the irreducible components of $V(f)$ are $V(x+y)$, $V(x-y)$, $V(x)$ and $V(y^3+x^2-xy+x)$.