Solutions to Algebraic Curves - An Introduction to Algebraic Geometry - William Fulton

Samy Lahlou

October 20, 2025

Preface

The goal of this document is to share my personal solutions to the exercises in the book Algebraic Curves - An Introduction to Algebraic Geometry by William Fulton during my reading.
As a disclaimer, the solutions are not unique and there will probably be better or more optimized solutions than mine. Feel free to correct me or ask me anything about the content of this document at the following address :
samy.lahloukamal@mcgill.ca

Contents

Chapter 1

Affine Algebraic Sets

1.1 Algebraic Preliminaries

1.1. TODO
Solution TODO

1.2. TODO
Solution TODO

1.3. TODO
Solution TODO

1.4. TODO
Solution TODO

1.5. TODO
Solution TODO

1.6. TODO
Solution TODO

1.7. TODO
Solution TODO

1.2 Affine Space and Algebraic Sets

1.8. Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets, together with $\mathbb{A}^1(k)$ itself.

Solution Let S be an arbitrary set polynomials in $k[x]$. If S is empty or $S = \{0\}$, then $V(S) = \mathbb{A}^1(k)$. If S contains a nonzero polynomial F, then $V(S) \subset V(F)$. Since F is a one-variable polynomial, then it has finitely many roots, and so $V(F)$ is finite. It follows that $V(S)$ is a finite subset of $\mathbb{A}^1(k)$. Conversely, we know that any finite subsets are algebraic sets. Therefore, the algebraic subsets of $\mathbb{A}^1(k)$ are

precisely the finite subsets and $\mathbb{A}^1(k)$ itself.

1.9. If k is a finite field, show that every subset of $\mathbb{A}^1(k)$ is algebraic.

Solution Let U be a subset of $\mathbb{A}^n(k)$, then U us finite and so it must be algebraic by property n°5 of the section.

1.10. Give an example of a countable collection of algebraic sets whose union is not algebraic.

Solution If we let $k = \mathbb{R}$, and $V_i = \{i\}$ for all $i \in \mathbb{Z}$, then all the V_i's are algebraic subsets of $A^1(k)$ but their union is not since it would contradict Problem 1.8.

1.11. Show that the following are algebraic sets:

(a) $\{(t, t^2, t^3) \in \mathbb{A}^3(k) | t \in k\}$;

(b) $\{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) | t \in \mathbb{R}\}$;

(c) the set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r, θ) satisfy the equation $r = \sin(\theta)$.

Solution

(a) Let $U = \{(t, t^2, t^3) \in \mathbb{A}^3(k) | t \in k\}$ and $V = V(x^3 - z, x^2 - y)$. Let $(x, y, z) \in U$, then there is a $t \in k$ such that $x = t$, $y = t^2$, and $z = t^3$. It follows that $x^3 - z = 0$ and $x^2 - y = 0$. Hence, $(x, y, z) \in V$. Conversely, if $(x, y, z) \in V$, and if we let $t = x$, then $y = x^2 = t^2$ and $z = x^3 = t^3$. Hence, $(x, y, z) \in U$. Therefore, $U = V$ and so U is algebraic.

(b) Since the set $U = \{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) | t \in \mathbb{R}\}$ is simply the unit circle in $\mathbb{R}^2$, then we know that we can rewrite it as $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | x^2 + y^2 = 1\}$, or simply as $V(x^2 + y^2 - 1)$. Thus, it is an algebraic set.

(c) Using the fact that $r = \sqrt{x^2 + y^2}$ and $\sin(\theta) = y/\sqrt{x^2 + y^2}$, we get that the set $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | r = \sin(\theta)\}$ is equal to

$$\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | \sqrt{x^2 + y^2} = y/\sqrt{x^2 + y^2}\}.$$

Equivalently, we can rewrite it as $V(x^2 + y^2 - y)$. Hence, it is an algebraic set.

1.12. Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^2(k)$, $L \not\subset C$. Suppose $C = V(F)$, $F \in k[X, Y]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points. (*Hint:* Suppose $L = V(Y - (aX + b))$, and consider $F(X, aX + b) \in k[X]$.)

Solution Let $F \in k[X, Y]$ be a polynomial of degree n and suppose that $C = V(F)$. Since L is a line, then we can write $L = V(G)$ with $G = aX + bY + c$ for some $a, b, c \in k$ where a and b cannot be both zero. Suppose without loss of generality that b is non-zero, then $(X, Y) \in L$ if and only if $Y = -\frac{a}{b}X - \frac{c}{b}$. Consider now the

polynomial $F(X, -\frac{a}{b}X - \frac{c}{b}) \in k[X]$, then this is a polynomial of degree n. Let X be one of its roots, then $(X, -\frac{a}{b}X - \frac{c}{b}) \in L \cap C$. Conversely, if $(X, Y) \in L \cap C$, then $Y = -\frac{a}{b}X - \frac{c}{b}$ which implies that $F(X, Y) = 0$ and so X is a root of $F(X, -\frac{a}{b}X - \frac{c}{b})$. Therefore, the roots of X are in bijection with the elements in $L \cap C$. Since $F(X, -\frac{a}{b}X - \frac{c}{b})$ is a polynomial of degree n, then it has at most n roots, and hence, $L \cap C$ is a finite set of no more than n points.

1.13. Show that each of the following sets is not algebraic:

(a) $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin(x)\}$.

(b) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$, where $|x + iy|^2 = x^2 + y^2$ for $x, y \in \mathbb{R}$.

(c) $\{(\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) | t \in \mathbb{R}\}$;

Solution

(a) Suppose that $\{y = \sin(x)\} = V(S)$ for some $S \subset k[X, Y]$. Since $\{y = \sin(x)\} \neq \mathbb{A}^2(\mathbb{R})$, then S must contain a nonzero polynomial $F \in k[X, Y]$, of degree n. Since $F \in S$, then $F(x, \sin(x)) = 0$ for all $x \in \mathbb{R}$. Consider now the polynomial $F(0, X) \in k[X]$, then this polynomial must have at most n roots. However, there are infinitely many $x \in \mathbb{R}$ such that $\sin(x) = 0$ since F has infinitely many roots. Therefore, by contradiction, the set $\{y = \sin(x)\}$ is not algebraic.

(b) Suppose that $\{|z|^2 + |w|^2 = 1\} = V(S)$, since $\{|z|^2 + |w|^2 = 1\} \neq \mathbb{A}^2(\mathbb{C})$, then there must be a nonzero polynomial $F \in k[X, Y]$ such that $F(z, w) = 0$ for all $z, w \in \mathbb{C}$ such that $|z|^2 + |w|^2 = 1$. Let $C = V(F)$, and let $L = V(X)$ be a line. We know that $L \not\subset C$ since $(0, 2) \in L$ but $(0, 2) \notin C$. Hence, by Problem 1.12, $L \cap C$ is finite. However, for every complex number w with $|w| = 1$, we have that $(0, w) \in L \cap C$. Since there are infinitely many such complex numbers w, then $L \cap C$ is infinite, a contradiction. Therefore, $\{|z|^2 + |w|^2 = 1\}$ is not an algebraic set.

(c) Suppose that $\{(\cos(t), \sin(t), t)\}_{t \in \mathbb{R}} = V(S)$ for some $S \subset k[X, Y, Z]$. Since $\{(\cos(t), \sin(t), t)\}_{t \in \mathbb{R}} \neq \mathbb{A}^3(\mathbb{R})$, then S must contain a nonzero polynomial $F \in k[X, Y, Z]$, of degree n. Since $F \in S$, then $F(\cos(t), \sin(t), t) = 0$ for all $t \in \mathbb{R}$. Consider now the polynomial $F(1, 0, X) \in k[X]$, then this polynomial must have at most n roots. However, there are infinitely many $t \in \mathbb{R}$ such that $\cos(x) = 1$, $\sin(x) = 0$, and hence, $F(1, 0, x) = F(\cos(x), \sin(x), x) = 0$, so F has infinitely many roots. Therefore, by contradiction, the set is not algebraic.

1.14. Let F be a nonconstant polynomial in $k[X_1, \ldots, X_n]$, k is algebraically closed. Show that $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 1$, and $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 2$. Conclude that the complement of any proper algebraic set is infinite. (*Hint:* See Problem 1.4.)

Solution First, notice that k must be infinite since it is algebraically closed. Hence, the case $n = 1$ follows from Problem 1.8. For the case $n = 2$, suppose that there are finitely many (x, y) such that $F(x, y) \neq 0$. Let (x_0, y_0) be such a pair, then we get

that there finitely many y such that $F(x_0, y) = 0$. But since $F(x_0, y) \in k[y]$, then we get a contradiction with the case $n = 1$. Therefore, $\mathbb{A}^n(k) \setminus V(F)$ is infinite for the case $n = 2$.

Now, let $n \geq 1$, $F \in k[X_1, ..., X_n]$, and suppose that $\mathbb{A}^n(k) \setminus V(F)$ is finite. Let $(a_1, ..., a_n) \in \mathbb{A}^n(k)$ be such that $F(a_1, ..., a_n) \neq 0$, then the polynomial $F(a_1, ..., a_{n-1}, X) \in k[X]$ is such that there are finitely many $x \in k$ such that it is nonzero. But this is in contradiction with the case $n = 1$. Thus, by contradiction, the set $\mathbb{A}^n(k) \setminus V(F)$ is infinite.

1.15. Let $V \subset \mathbb{A}^n(k)$, $W \subset \mathbb{A}^m(k)$ be algebraic sets. Show that

$$V \times W = \{(a_1, ..., a_n, b_1, ..., b_m) \mid (a_1, ..., a_n) \in V, (b_1, ..., b_m) \in W\}$$

is an algebraic set in $\mathbb{A}^{n+m}(k)$. It is called the *product* of V and W.

Solution For all $F \in V$ and $G \in W$, define $F^\times, G^\times \in k[X_1, ..., X_{n+m}]$ by

$$F^\times(X_1, ..., X_{n+m}) = F(X_1, ..., X_n) \text{ and } G^\times(X_1, ..., X_{n+m}) = G(X_{n+1}, ..., X_{n+m}).$$

If we consider the set $V(\{F^\times\}_{F \in V})$, we get that it is equal to the elements in $\mathbb{A}^{n+m}(k)$ where the first n entries are in V. Similarly, $V(\{G^\times\}_{G \in W})$ is equal to the elements in $\mathbb{A}^{n+m}(k)$ where the last m entries are in V. It follows that $V(\{F^\times\}_{F \in V} \cup \{G^\times\}_{G \in W}) = V \times W$. Therefore, $V \times W$ is an algebraic set.

1.3 The Ideal of a Set of Points

1.16. Let V, W be algebraic sets in $\mathbb{A}^n(k)$. Show that $V = W$ if and only if $I(V) = I(W)$.

Solution If $V = W$, then $I(V) = I(W)$ trivially. Now, if $I(V) = I(W)$, then $V(I(V)) = V(I(W))$. Since V and W are algebraic sets, then $V(I(V)) = V$ and $V(I(W)) = W$. Hence, $V = W$.

1.17. (a) Let V be an algebraic set in $\mathbb{A}^n(k)$, $P \in \mathbb{A}^n(k)$ a point not in V. Show that there is a polynomial $F \in k[X_1, ..., X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$. (*Hint:* $I(V) \neq I(V \cup \{P\})$.) (b) Let $P_1, ..., P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $F_1, ..., F_r \in I(V)$ such that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$. (*Hint:* Apply (a) to the union of V and all but one point.) (c) With $P_1, ..., P_r$ and V as in (b), and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $G_i \in I(V)$ with $G_i(P_j) = a_{ij}$ for all i and j. (*Hint:* Consider $\sum_j a_{ij} F_j$.)

Solution

(a) Since $P \notin V$, then $V \neq V \cup \{P\}$ and so $I(V) \neq I(V \cup \{P\})$ by Problem 1.16. Since $V \subset V \cup \{P\}$, then $I(V \cup \{P\}) \subset I(V)$ and so it must be that $I(V) \not\subset I(V \cup \{P\})$. This implies that there is a $F_0 \in I(V) \subset k[X_1, ..., X_n]$ such that $F_0 \notin I(V \cup \{P\})$. In other words, there is polynomial $F_0 \in k[X_1, ..., X_n]$ such that $F_0(Q) = 0$ for all $Q \in V$ and $F_0(P) \neq 0$. Define $F(x) = F_0(P)^{-1} F_0(x)$ for all $x \in \mathbb{A}^n(k)$, then $F(Q) = 0$ for all $Q \in V$ and $F(P) = 1$.

(b) Let $i \in [\![1, r]\!]$, since $V \cup \{P_j\}_{j \neq i}$ is an algebraic set that doesn't contain P_i, then by part (a) there is a function $F_i \in I(V)$ such that $F_i(P_j) = 0$ whenever $j \neq i$ and $F_i(P_i) = 1$.

(c) Since the set up is the same as in (b), then we already showed that, for all $i \in [\![1, r]\!]$, there exists a polynomial $F_i \in I(V)$ such that $F_i(P_j) = 0$ for all $j[\![1, r]\!] \setminus \{i\}$ and $F_i(P_i) = 1$. For all $i \in [\![1, r]\!]$, define $G_i = \sum_{k=1}^{r} a_{ik} F_k$. Since the F_i's are all in the ideal $I(V)$, then $G_i \in I(V)$. Moreover, for all $j \in [\![1, r]\!]$, we have that $G_i(P_j) = \sum_{k=1}^{r} a_{ik} F_k(P_j) = a_{ij}$.

1.18. Let I be an ideal in a ring R. If $a^n \in I$, $b^m \in I$, show that $(a+b)^{n+m} \in I$. Show that $\mathrm{Rad}(I)$ is an ideal. Show that any prime ideal is radical.

Solution By the Binomial Formula, we have that

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

When $k \in [\![0, n-1]\!]$, we have that the term of index k is in I because it can be written as $\binom{n+m}{k} a^k b^{n-k} \cdot b^m$ and b^m is in I. Similarly, if $k \in [\![n, n+m]\!]$, the term of index k can be written as $\binom{n+m}{k} a^{k-n} b^{n+m-k} \cdot a^n$, and $a^n \in I$, so it is also in I. All the terms in the sum above are in I so $(a+b)^{n+m}$ must be in I.

Since $\mathrm{Rad}(I) \supset I$ and $0 \in I$, then $0 \in \mathrm{Rad}(I)$. If $a, b \in \mathrm{Rad}(I)$, then there exist positive integers n and m such that $a^n, b^m \in I$. By the previous part, $(a+b)^{n+m} \in I$ which implies that $a + b \in \mathrm{Rad}(I)$. Thus, $\mathrm{Rad}(I)$ is closed under addition. Finally, if $a \in \mathrm{Rad}(I)$ and $r \in R$, then there is a positive integer n such that $a^n \in I$. Since $(ra)^n = r^n a^n \in I$, then $ra \in \mathrm{Rad}(I)$. Therefore, $\mathrm{Rad}(I)$ is an ideal.

Let I be a prime ideal, to prove that I is radical, it suffices to prove that $\mathrm{Rad}(I) \subset I$. Let $i \in \mathrm{Rad}(I)$, then $i^n \in I$ where $n \geq 1$ is the smallest positive integer for which $i^n \in I$. If $n = 1$, we are done. Suppose that $n > 1$, then we have that $i \cdot i^{n-1} \in I$. Since I is prime, then either i or i^{n-1} is in I. Since n is minimal, then both cases are impossible. Therefore, $\mathrm{Rad}(I) = I$ and so I is radical.

1.19. Show that $I = (X^2 + 1) \subset \mathbb{R}[X]$ is a radical (even a prime) ideal, but I is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$.

Solution Suppose that $p^n \in (X^2+1)$, then $X^1 + 2 \mid p^n$. Since X^2+1 is irreducible in $\mathbb{R}[X]$, then $X^2 + 1 \mid p$ which implies that $p \in (X^2 + 1)$. Therefore, $(X^2 + 1)$ is radical. Suppose that $(X^2 + 1) = I(X)$ for some $X \subset \mathbb{A}^1(\mathbb{R})$. If $X = \varnothing$, then $(X^2 + 1) = I(\varnothing) = \mathbb{R}[X]$ which is false since $X \notin (X^2 + 1)$. Hence, there is a $x \in \mathbb{A}^1(\mathbb{R})$ such that $x \in X$. Since $X^2 + 1 \in I(X)$, then $x^2 + 1 = (X^2 + 1)(x) = 0$ which is impossible since $X^2 + 1$ has no roots in $\mathbb{R}$. Therefore, $(X^2 + 1)$ is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$.

1.20. Show that for any ideal I in $k[X_1, ..., X_n]$, $V(I) = V(\mathrm{Rad}(I))$, and $\mathrm{Rad}(I) \subset I(V(I))$.

Solution Since $I \subset \text{Rad}(I)$, then $V(\text{Rad}(I)) \subset V(I)$. Conversely, let $P \in V(I)$ and $F \in \text{Rad}(I)$, then $F^n \in I$ for some $n \geq 1$. It follows that $F^n(P) = 0$ and so $F(P)$. Thus, $P \in V(\text{Rad}(I))$. Therefore, $V(I) = V(\text{Rad}(I))$.

Now, from the fact that $S \subset I(V(S))$ for all subsets S of $k[X_1, ..., X_n]$, if we take $S = \text{Rad}(I)$, then $\text{Rad}(I) \subset I(V(\text{Rad}(I))) = I(V(I))$ by the first part of the exercise.

1.21. Show that $I = (X_1 - a_1, ..., X_n - a_n) \subset k[X_1, ..., X_n]$ is a maximal ideal, and that the natural homomorphism from k to $k[X_1, ..., X_n]/I$ is an isomorphism.

Solution Let J be an ideal properly containing I, and let $F \in J \setminus I$. Write F as

$$F(X_1, ..., X_n) = F_k(X_1, ..., X_{n-1})X_n^k + \cdots + F_0(X_1, ..., X_{n-1}).$$

Since $F \in J$ and $F_k(X_1, ..., X_{n-1})(X_n - a_n)^k \in I \subset J$, then $F - F_k(X_1, ..., X_{n-1})(X_n - a_n)^k \in J$ where the resulting polynomial is now a polynomial in $k[X_1, ..., X_{n-1}][X_n]$ of degree $k-1$. By repeating this process, we can obtain a polynomial $G \in J$ which is a polynomial in $k[X_1, ..., X_{n-1}]$. Again, if we repeat the same procedure, we get a constant polynomial $H \in J$. This constant polynomial is nonzero because otherwise, we would get that F is the sum of all the polynomials in I that we subtracted and so F would be in I. Thus, $H \in J$ is a nonzero constant so $1 \in J$. It follows that $J = k[X_1, ..., X_n]$. Therefore, I is maximal.

Consider the natural homomorphism $\varphi : k \to k[X_1, ..., X_n]/I$ that maps each scalar to equivalence class of its respective constant polynomial. This is a well defined homomorphism because it is equal to the natural homomorphism from k to $k[X_1, ..., X_n]$ composed with the projection homomorphism from $k[X_1, ..., X_n]$ to $k[X_1, ..., X_n]/I$. This homomorphism is injective because it is a field homomorphism. This homomorphism is injective because in the first part of this exercice, we showed that every polynomial in $k[X_1, ..., X_n]$ is equivalent to a constant polynomial. Therefore, φ is an isomorphism.

1.4 The Hilbert Basis Theorem

1.22. Let I be an ideal in a ring R, $\pi : R \to R/I$ the natural homomorphism. (a) Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is an ideal of R containg I, and for every ideal J of R containg I, $\pi(J) = J'$ is an ideal of R/I. This sets up a natural one-to-one correspondence between {ideals of R/I} and {ideals of R that contain I}. (b) Show that J' is a radical ideal if and only if J is radical. Similarly for prime and maximal ideals. (c) Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Any ring of the form $k[X_1, ..., X_n]/I$ is Noetherian.

Solution

(a) Let J' be an ideal of R/I and consider the set $J = \pi^{-1}(J')$. Since $\pi(0) = I = 0 \in J'$, then $0 \in \pi^{-1}(J') = J$. Let $a, b \in J$, then $\pi(a), \pi(b) \in J'$ which implies that $\pi(a + b) = \pi(a) + \pi(b) \in J'$. It follows that $a + b \in J$. Similarly, if $a \in J$ and $r \in R$, then $\pi(a) \in J'$ which implies that $\pi(ra) = \pi(r)\pi(a) \in J'$. Hence, $ra \in J$. Thus, J is an ideal of R. Finally, for all $i \in I$, we have that $\pi(i) = 0 \in J'$ so $i \in J$. Therefore, J is an ideal of R containing I.

Next, let J be an ideal of R that contains I, and define $J' = \pi(J)$. Since $0 \in J$ and $\pi(0) = 0$, then $0 \in J'$. Let $\pi(a), \pi(b) \in J'$, then $\pi(a)+\pi(b) = \pi(a+b) \in J'$ since $a + b \in J$. If $\pi(r) \in R/I$ and $\pi(a) \in J'$, then $\pi(r)\pi(a) = \pi(ra) \in J'$ since $ra \in J$. Therefore, J' is an ideal of R/I.

(b) Suppose that J' is radical and let $j^n \in J$, then $\pi(j)^n = \pi(j^n) \in J'$. Since J' is radical, then $\pi(j) \in J' = \pi(J)$ which implies that $j \in \pi^{-1}(\pi(J))$. Therefore, J is radical. Conversely, suppose that J is radical and let $\pi(j)^n \in J'$, then $\pi(j^n) \in J' = \pi(J)$. It follows that $j^n \in J$ which implies that $j \in J$. Thus, $\pi(j) \in J'$. Therefore, J' is radical.

Suppose that J' is prime and let $ab \in J$, then $\pi(a)\pi(b) = \pi(ab) \in J'$. By the primality of J', either $\pi(a)$ or $\pi(b)$ is in J'. Without loss of generality, if $\pi(a) \in J'$ then $a \in J$. It follows that J is prime. Conversely, if J is prime and $\pi(ab) = \pi(a)\pi(b) \in J'$, then $ab \in J$ which implies that $a \in J$ (wlog). It follows that $\pi(a) \in J'$. Therefore, J is prime.

Suppose that J' is maximal and let M be an ideal properly containing J, then its image $M' = \pi(M)$ is an ideal that contains J'. Let $m \in M \setminus J$, then $\pi(m) \in M' \setminus J'$ because if $\pi(m) \in J'$, then $m \in J$. Hence, M' properly contains J'. Since J' is maximal, then $M' = R/I$. By the bijection between the ideal classes, we must have $M = R$. Therefore, J is a maximal ideal. Conversely, suppose that J is maximal and let M' be an ideal that properly contains J'. Let $M = \pi^{-1}(M')$, then M is an ideal that contains J. Since M' contains J' properly, there must be an $m \in M$ such that $\pi(m) \in M' \setminus J'$. From this, it must be that $m \in M \setminus J$ and so M contains J properly. Since J is maximal, then $M = R$ and so $M' = R/I$. Therefore, J' is maximal.

(c) Suppose that J is finitely generated, then we can write $J = (j_1, ..., j_n)$. Let $\pi(j) \in J'$, then

$$\pi(j) = \pi\left(\sum_k r_k j_k\right) = \sum_k \pi(r_k)\pi(j_k) \in (\pi(r_1), \ldots, \pi(r_n)).$$

It follows that $J' \subset (\pi(r_1), \ldots, \pi(r_n))$. On the other hand, since the $\pi(j_k)$'s are in J', then $(\pi(r_1), \ldots, \pi(r_n)) \subset J'$. Therefore, J' is finitely generated.

Now, suppose that R is Noetherian and let J' be an ideal of R/I, then $J' = \pi(J)$ where J is an ideal of R containing I. Since R is Noetherian, then J is finitely generated and so J' is also finitely generated. Therefore, R/I is Noetherian.

1.5 Irreducible Components of an Algebraic Set

1.23. Give an example of a collection $\mathscr{S}$ of ideals in a Noetherian ring such that no maximal member of $\mathscr{S}$ is a maximal ideal.

Solution Take the ring to be $\mathbb{Z}$ and take the collection $\mathscr{S} = \{(4)\}$ containing only one element. It is clear that (4) is a maximal element of $\mathscr{S}$ even though it is not a maximal ideal of $\mathbb{Z}$.

1.24. Show that every proper ideal in a Noetherian ring is contained in a maximal ideal. (*Hint:* If I is the ideal, apply the lemma to {proper ideals that contain I}.)

Solution Let I be a proper ideal and let $\mathscr{S}$ be the collection of proper ideals that contain I. By the lemma, $\mathscr{S}$ must contain a maximal element J that contain I. If J is not a maximal ideal, then it must be itself contained in a proper ideal of the ring. However, this new proper ideal would be in $\mathscr{S}$ and would contradict the maximality of J in $\mathscr{S}$. Therefore, J is a maximal ideal that contain I.

1.25. (a) Show that $V(Y - X^2) \subset \mathbb{A}^2(\mathbb{C})$ is irreducible; in fact, $I(V(Y - X^2)) = (Y - X^2)$. (b) Decompose $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^2(\mathbb{C})$ into irreducible components.

Solution

(a) Let's show that $I(V(Y - X^2))$ is a prime ideal. First, notice that $I(V(Y - X^2)) = (Y - X^2)$. Since $Y - X^2$ is irreducible in $\mathbb{C}[X, Y]$, then $(Y - X^2)$ is prime. Therefore, $V(Y - X^2)$ is irreducible.

(b) First, notice that $Y^4 - X^2 = (Y^2 - X)(Y^2 + X)$ and $Y^4 - X^2Y^2 + XY^2 - X^3 = (Y^2 - X^2)(Y^2 + X) = (Y - X)(Y + X)(Y^2 + X)$. Let's prove that our algebraic set V is equal to $V(Y^2 + X) \cup \{(1, 1)\} \cup \{(1, -1)\}$. First, if $(x, y) \in V$, then $y^4 = x^2$ and $(y - x)(y + x)(y^2 + x) = 0$. From the second equation, we have the following cases: if $y = x$, then either $x = y = 0$ or $y^4 = x^2$ implies that $y^2 = 1$, and hence, that $x = y = \pm 1$; if $y = -x$, then either $x = y =$ or the same considerations as before gives us that $y = \pm 1$, and hence, $x = \mp 1$, $y = \pm 1$; finally, if $y^2 = -x$, then $y^2 + x = 0$. The outcome of all of these cases show that $(x, y) \in V(Y^2 + X) \cup \{(1, 1)\} \cup \{(1, -1)\}$. The converse is even easier to prove, if $y^2 + x = 0$, then (x, y) satisfy both polynomials describing V and so it is in V; if $x = 1$ and $y = \pm 1$, then it clearly satisfies both polynomials again and so it is in V. Therefore, $V = V(Y^2 + X) \cup \{(1, 1)\} \cup \{(1, -1)\}$. The three sets are clearly irreducible algebraic sets so we are done.

1.26. Show that $F = Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ is an irreducible polynomial, but $V(F)$ is reducible.

Solution By contradiction, suppose that there exist two polynomials $p, q \in \mathbb{R}[X, Y]$ such that $y^2 + x^2(x - 1)^2 = p(x, y)q(x, y)$, then in particular, if we fix any $x \in \mathbb{R} \setminus \{0, 1\}$, we can view this equation as an equation where y is the only variable. But this would mean that the polynomial $y^2 + x^2(x - 1)^2$ is reducible in $\mathbb{R}[y]$ which is false. Therefore, the polynomial F is irreducible.

To show that $V(F)$ is reducible, notice that the only solutions to the equation $Y^2 + X^2(X - 1)^2 = 0$ are $(0, 0)$ and $(1, 0)$. Therefore, $V(F) = \{(0, 0)\} \cup \{(1, 0)\}$.

1.27. Let V, W be algebraic sets in $\mathbb{A}^n(k)$, with $V \subset W$. Show that each irreducible component of V is contained in some irreducible component of W.

Solution First, write $V = \bigcup_i V_i$ and $W = \bigcup_j W_j$ where the unions are finite. Since $V \subset W$, then for each i, we have $V_i = \bigcup_j (W_j \cap V_i)$. Since V_i is irreducible, then

we must have that $V_i = W_j \cap V_i \subset W_j$ for some j. Therefore, every irreducible component of V is contained in an irreducible component of W.

1.28. If $V = V_1 \cup \cdots \cup V_r$ is the decomposition of an algebraic set into irreducible components, show that $V_i \not\subset \bigcup_{i \neq j} V_j$.

Solution First, recall that $V_i \not\subset V_j$ for all $i \neq j$. Next, suppose that $V_i \subset \bigcup_{i \neq j} V_j$, then $V_i = \bigcup_{i \neq j}(V_j \cap V_i)$. But since V_i is irreducible, then $V_i = V_j \cap V_i \subset V_j$ for some $i \neq j$. This contradiction proves that the original claim holds.

1.29. Show that $\mathbb{A}^n(k)$ is irreducible if k is infinite.

Solution Simply notice that when k is infinite, we have $I(\mathbb{A}^n(k)) = \{0\}$ and $\{0\}$ is a prime ideal. Therefore, $\mathbb{A}^n(k)$ is irreducible.

1.6 Algebraic Subsets of the Plane

1.30. Let $k = \mathbb{R}$. (a) Show that $I(V(X^2 + Y^2 + 1)) = (1)$. (b) Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[X, Y]$.

Solution

(a) Since $X^2 + Y^2 + 1$ has no roots in $\mathbb{A}^2(\mathbb{R})$, then

$$I(V(X^2 + Y^2 + 1)) = I(\varnothing) = \mathbb{A}^2(\mathbb{R}) = (1).$$

(b) Let V be an algebraic subset of $\mathbb{A}^2(\mathbb{R})$. If $V = \mathbb{A}^2(\mathbb{R})$, then $V = V(0)$; if $V = \varnothing$, then $V = V(1)$; if $V = \{(a, b)\}$, then we can write V as $V((X-a)^2+(Y-b)^2)$ because $(X-a)^2+(Y-b)^2 = 0$ if and only if $X = a$ and $Y = b$; if V is any other algebraic set, then we already know that $V = V(F)$ for some $F \in \mathbb{R}[X, Y]$ using Corollary 2.

1.31. (a) Find the irreducible components of $V(Y^2-XY-X^2Y+X^3)$ in $\mathbb{A}^2(\mathbb{R})$, and also in $\mathbb{A}^2(\mathbb{C})$. (b) Do the same for $V(Y^2-X(X-1)^2)$, and for $V(X^3+X-X^2Y-Y)$.

Solution

(a) Notice that $Y^2 - XY - X^2Y + X^3 = (Y - X^2)(Y - X)$, then $V(Y^2 - XY - X^2Y + X^3) = V(Y - X^2) \cup V(Y - X)$. This decomposition is the irreducible decomposition in $\mathbb{C}[X, Y]$ because both $Y - X^2$ and $Y - X$ are irreducible, and using Corollary 3. This is also the irreducible decomposition in $\mathbb{A}^2(\mathbb{C})$ because both $Y - X^2$ and $Y - X$ are irreducible in $\mathbb{R}[X, Y]$ and both have an infinite associated algebraic set.

(b) The first polynomial is irreducible and has infinitely many solutions in $\mathbb{A}^2(\mathbb{R})$, hence, its associated algebraic set is irreducible. The second polynomial has the same factorization into irreducible polynomials in $\mathbb{A}^2(\mathbb{R})$ and in $\mathbb{A}^2(\mathbb{C})$ so again, the factorization is the same in the two cases.

1.7 Hilbert's Nullstellensatz

1.32. Show that both theorems and all of the corollaries are false if k is not algebraically closed.

Solution For the Weak-Nullstellensatz, take $k = \mathbb{R}$, $n = 1$, $I = (X^2 + 1)$, then $V(I) = \varnothing$ since $X^2 + 1$ has no roots in $\mathbb{R}$. The same set up disproves the Hilbert's Nullstellensatz, as well as Corollary 1 and 2. For the third corollary, it suffices to look at $V(Y^2 + X^2(X-1)^2)$ in $\mathbb{R}$ and see that even though the polynomial is irreducible, the algebraic set is reducible into $\{(0,0)\}$ and $\{(1,0)\}$. Similarly, if we take $I = (X^2+Y^2) \subset \mathbb{R}[X,Y]$, then $V(I) = \{(0,0)\}$ is finite but $\mathbb{R}[X,Y]/(X^2+Y^2)$ is infinite dimensional. This last example shows that corollary 4 doesn't hold if k is not algebraically closed.

1.33. (a) Decompose $V(X^2 + Y^2 - 1, X^2 - Z^2 - 1) \subset \mathbb{A}^3(\mathbb{C})$ into irreducible components. (b) Let $V = \{(t, t^2, t^3) \in \mathbb{A}^3(\mathbb{C}) | t \in \mathbb{C}\}$. Find $I(V)$, and show that V is irreducible.

Solution

(a) Let $I = (X^2+Y^2-1, X^2-Z^2-1)$, then $V(X^2+Y^2-1, X^2-Z^2-1) = V(I)$. Since $\mathbb{C}[X,Y,Z]/I \cong \mathbb{C}[X,Y]$ is an integral domain, then I is a prime ideal, and hence, $V(I)$ is irreducible.

(b) First, notice that $V = V(Y-X^2, Z-X^3)$. Hence, if we let $I = (Y-X^2, Z-X^3)$ and notice that $\mathbb{C}[X,Y,Z]/I \cong \mathbb{C}[X]$ is an integral domain, then we get that I is a prime ideal, and hence, $I(V) = I(V(I)) = I = (Y - X^2, Z - X^3)$ by the Nullstellensatz.

1.34. Let R be a UFD. (a) Show that a monic polynomial of degree two or three in $R[X]$ is irreducible if and only if if has no roots in R. (b) The polynomial $X^2 - a \in R[X]$ is irreducible if and only if a is not a square in R.

Solution

(a) First, notice that if a polynomial of degree 2 or 3 is reducible, then it must be divisible by a polynomial of degree 1. Moreover, in the decomposition of the polynomial into two smaller (in the sense of the degree) polynomials, the leading coefficients of each smaller polynomial must be inverses of each other since the original polynomial is monic. In that case, we can multiply the two polynomials by constants such that the degree one polynomial dividing the original polynomial is monic as well. It follows that a reducible, monic, degree 2 or 3 polynomial must have a root since it is divisible by a polynomial which has a root. The converse is easy.

(b) This follows from part (a) using the fact that $X^2 - a$ has a root if and only if a has a root in R.

1.35. Show that $V(Y^2 - X(X-1)(X-\lambda)) \subset \mathbb{A}^2(k)$ is an irreducible curve for any algebraically closed field k, and any $\lambda \in k$.

Solution TODO

1.36. TODO

Solution TODO

1.37. TODO

Solution TODO

1.38. TODO

Solution TODO

1.39. TODO

Solution TODO

1.40. TODO

Solution TODO

1.8 Modules; Finiteness Conditions

1.41. TODO

Solution TODO

1.42. TODO

Solution TODO

1.43. TODO

Solution TODO

1.44. TODO

Solution TODO

1.45. TODO

Solution TODO

1.9 Integral Elements

1.46. TODO

Solution TODO

1.47. TODO

Solution TODO

1.48. TODO

Solution TODO

1.49. TODO

Solution TODO

1.50. TODO

Solution TODO

1.10 Field Extensions

1.51. TODO

Solution TODO

1.52. TODO

Solution TODO

1.53. TODO

Solution TODO

1.54. TODO

Solution TODO