Algebraic Geometry

Jubayer Ibn Hamid

Contents

1 Introduction **4**

1.1 Terminology 4

2 Affine Varieties **6**

2.1 Algebraic Sets, Affine Varieties and Zariski Topology 6

2.2 Hilbert Basis Theorem 8

2.2.1 Module-finite, Ring-finite, Field extensions 10

2.2.2 Finiteness Conditions of Subrings of a Ring 10

2.2.3 Integral over a Ring, Algebraic over a Ring 11

2.3 Hilbert's Nullstellensatz 14

2.4 Irreducible Components of Algebraic Sets 18

2.5 Coordinate Rings 20

2.6 Dimension of Affine Varieties 20

3 Projective Varieties **23**

4 Ring Theory Revision **26**

4.1 Rings 26

4.2 Integral Domains and Subrings 27

4.3 Ideals 28

4.4 Maximal Ideals 29

4.5 Prime Ideals 30

4.6 Rings of Fractions and Fields of Fractions 30

4.7 Euclidean Domains and Discrete Valuation Rings 31

4.8 Principal Ideal Domains 32

4.9 Irreducible elements and Prime elements 33

4.10 Unique Factorization Domain 33

4.11 Polynomial Rings 34

4.12 Polynomial Rings over Fields 35

4.13 Irreducibility Criteria 36

1 Introduction

Algebraic geometry is about solutions of polynomial equations and the geometric structures on the space of those solutions. We use the language and techniques from abstract algebra on these geometric objects.

Geometry becomes interesting when local properties reveal to us global properties. Algebra provides us a very powerful tool to do that.

These notes are a combination of material from the courses Math 145 by Prof. Zhiyu Zhang and Math 216a by Prof. Ravi Vakil at Stanford University and the texts mentioned in the references.

1.1 Terminology

A field k is algebraically closed if any non-constant polynomial $f \in k[x]$ has at least one root/zero in k i.e if $f \in k[x]$, then $f(x) = \mu \prod (x - \lambda_i)^{e_i}$ where $\lambda_i \in k$ are the roots. The field $\mathbb{R}$ is not algebraically closed as $f(x)x^+1$ has no root in $\mathbb{R}$, whereas $\mathbb{C}$ is algebraically closed.

The affine space of field k is denoted by $\mathbb{A}_k^n$ which is the Cartesian n-product of k.

The true coordinate ring $O(\mathbb{A}^n)$ of functions on $\mathbb{A}^n$ is the commutative ring $k[x_1, ..., x_n]$ of polynomials with n variables.

Let $f \in k[x_1, ..., x_n]$ be a polynomial. Then, $V(f)$ is the set of zeros of f and is called the hypersurface defined by f. If S is a set of polynomials from $k[x_1, .., x_n]$, then $V(S) := \{p \in \mathbb{A}_k^n | f(p) = 0, \forall f \in S\}$. One can check that $V(S) = \cap_{f \in S} V(f)$. When $S = \{f_1, ..., f_r\}$, we write $V(S)$ as $V(f_1, ..., f_r)$.

Example: Consider $k[x]$ which is a principal ideal domain. Therefore, every algebraic set can be written as the set of zeros of a single polynomial.

A subset $X \subseteq \mathbb{A}_k^n$ is called an affine algebraic set if $X = V(S)$ for some set S of polynomials in $k[x_1, ..., x_n]$. Throughout these notes, we will use the term affine variety to mean the same thing as affine algebraic sets (although some texts refer to only *irreducible* algebraic sets as affine varieties). One can easily show that if I is the ideal in $k[x_1, ..., x_n]$ generated by polynomials in S, then $V(S) = V(I)$. Suppose, $I = (f_1, ..., f_n)$, then, $V(I) = \cap_{i=1}^n V(f_i)$. Some more properties:

(1) If $\{I_\alpha\}$ is a collection of ideals, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$. (2) $I \subset J \implies V(J) \subset V(I)$ (3) $V(fg) = V(f) \cup V(g)$ (4) Any finite subset of $\mathbb{A}_k^n$ is an algebraic set (5) $V(A) = V((A))$ where (A) is the ideal generated by A.

The ideal generated by a set of functions $f_1, ..., f_m \in k[x_1, ..., x_n]$ is the set $(f_1, ..., f_m) := \{\sum_{i=1}^m g_i f_i : g_i \in k[x_1, ..., x_n]\}$. For a subset $X \subseteq \mathbb{A}_k^n$, consider the ideal in $k[x_1, ..., x_n]$ generated by polynomials that vanish on X. This ideal is called the vanishing ideal of X, denoted by $I(X)$. So, $I(X) = \{f \in k[x_1, ..., x_n] : f(a) = 0, \forall a \in X\}$. So, if $f, g \in I$, then $f + g \in I$ and for any $h \in k[x_1, ..., x_n]$, $hf \in I$. Some more properties:

(1) $X \subset Y \implies I(Y) \subset I(X)$ (2) $I(\emptyset) = k[x_1, ..., x_n], I(\mathbb{A}^n) = \emptyset, I(\{a\}) = (x_1 - a_1, ..., x_n - a_n)$.

We say $f_1, ..., f_m$ scheme-theoretically define the affine variety $X \subset \mathbb{A}^n$ if $I(X) = (f_1, ..., f_m)$ i.e the ideal generated by $f_1, ..., f_m$. Furthermore, the ideal I is said to set-theoretically define variety X if $X = V(I)$ if It can be easily shown that $V(I(X)) = X$. $V(-)$ and $I(-)$ allow us to switch betwen the geometric world and the algebraic world which is a key tool used in algebraic geometry. In particular, later on, we will see that using Hilbert's Nullstellensatz, there is no information lost after we make this switch.

We also define fractional fields. Let R be an integral domain. Its fractional field $K = \text{Frac}(R)$ is defined as the ring

$$K := \{\frac{f}{g} : f, g \in R, g \neq 0\}$$

.

A polynomial mapping/morphism $p : V \to W$, where $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ are varieties, is a mapping such that $(x_1, ..., x_n) \to f(x_1, ..., x_n) := (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$, $f_i \in k[x_1, ..., x_n]$ and the image of the algebraic set V lies inside the algebraic set W. The mapping set Map(V, W) is the set of all polynomial maps from V to W and in our case this is the set of all polynomial maps from V to W. We need polynomial mappings in order to investigate the relationships between varieties. Given X is an affine variety, an **automorphism** of X is a polynomial map $f : X \to X$ which is an isomorphism. $Aux(X)$ denotes the group of all automorphisms of X.

2 Affine Varieties

2.1 Algebraic Sets, Affine Varieties and Zariski Topology

We start by defining the following space:

Definition 1. (Affine n-space over field k). Let k be an algebraically closed field. Then, the affine n-space over k, denoted by $\mathbb{A}_k^n$, is the set of all n-tuples, $(k_1, \cdots, k_n)$, of elements of k.

Now, we look at polynomials over the field k and their zeros.

Definition 2. (Zero set of polynomials). Consider the polynomial ring $k[x_1, \cdots, x_n]$ where k is an algebraically closed field. Then, for $T \subseteq k[x_1, \cdots, x_n]$, define the zero set of T to be

$$Z(T) := \{p \in \mathbb{A}_k^n | f(p) = 0, \forall f \in T\}.$$

If a is the ideal generated by $T \subseteq k[x_1, \cdots, x_n]$, then $Z(T) = Z(a)$.

Definition 3. A subset $Y \subseteq \mathbb{A}_k^n$ is an algebraic set if there exists a subset $T \subseteq k[x_1, \cdots, x_n]$ such that $Y = Z(T)$.

Proposition 1. The union of any two algebraic sets is an algebraic set. The intersection of a family of algebraic sets is an algebraic set. The empty set and the whole space, $\mathbb{A}_k^n$, are algebraic sets.

Proof. One can easily verify that if $Y_1 = Z(T_1)$ and $Y_2 = Z(T_2)$, then $Y_1 \cup Y_2 = Z(T_1 T_2)$ ($T_1 T_2$ is the set of product of elements in T_1 and in T_2). Similarly, if $Y_\alpha = Z(T_\alpha)$ for all α, then $\cap Y_\alpha = Z(\cup_\alpha T_\alpha)$. Lastly, $\emptyset = Z(k[x_1, ..., x_n]) = Z(1)$ and $\mathbb{A}_k^n = Z(0)$. □

This last definition indicates that we can easily define a topology on the space $\mathbb{A}_k^n$, or in short, $\mathbb{A}^n$. This topology is called the Zariski topology.

Definition 4. (Zariski Topology). The Zariski topology on $\mathbb{A}^n$ is defined by letting closed sets be algebraic sets.

Example: Zariski topology on $\mathbb{A}^1$. Consider any ideal I in $k[x]$ - since $k[x]$ is a principal ideal domain, the ideal $I = (f)$ for some f. Since $f \in k[x]$ and since k is algebraically closed, we can write $f = c(x_1 - a_1) \cdots (x_n - a_n)$ where a_i are the roots of f. Thus, $Z(f) = \{a_1, \cdots, a_n\}$. Therefore, the closed sets in $\mathbb{A}^1$ are the empty set, finite subsets and $\mathbb{A}^1$. Furthermore, note that this space is not Hausdorff since the open sets are $\emptyset$, $\mathbb{A}^1$ and complements of finite subsets.

Definition 5. (Irreducible sets). A non-empty subset Y of the topological spacee X is called irreducible if one cannot write Y as $Y = X_1 \cup X_2$ where X_1 and X_2 are closed and proper (i.e. non-empty and not equal to X). The empty set is not considered irreducible.

Definition 6. (Affine variety). An affine variety is an irreducible closed subset of $\mathbb{A}^n$ in the Zariski topoology. An open subset of an affine variety is called a quasi-affine variety.

Examples:
(1) $\mathbb{A}^1$ is an affine variety - the closed, proper subsets of $\mathbb{A}^1$ are finite so $\mathbb{A}^1$ cannot be written as the union of two such sets.
(2) Any non-empty open subset of an irreducible space is irreducible and dense.
(3) If Y is an irreducible set in X then $\bar{Y}$ in X is also irreducible.

We travel between the world of $\mathbb{A}^n$ and the polynomials in $k[x_1, \cdots, x_n]$ by first defining the following:

Definition 7. (Ideals in $k[x_1, \cdots, x_n]$). For any subset $Y \subseteq \mathbb{A}^n$, define the ideal of Y in $k[x_1, \cdots, x_n]$ to be

$$I(Y) := \{f \in k[x_1, \cdots, x_n] | f(p) = 0, \forall p \in Y\}.$$

We discuss some immediate properties of the objects introduced so far:

Proposition 2. (1) If $T_1 \subseteq T_2$ in $k[x_1, .., x_n]$, then $Z(T_2) \subseteq Z(T_1)$.
(2) If $Y_1 \subseteq Y_2$ in $\mathbb{A}^n$, then $I(Y_2) \subseteq I(Y_1)$.
(3) For any two subsets Y_1 and Y_2 in $\mathbb{A}^n$, $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.

2.2 Hilbert Basis Theorem

We start with the following observation:

Proposition 3. For any $a := (a_1, ..., a_n) \in \mathbb{A}^n_k$, $I(\{a\}) = (x_1 - a_1, ..., x_n - a_n) \subset k[x_1, ..., x_n]$.

Proof. Note that $(x_1 - a_1, ..., x_n - a_n) \subset I(\{a\})$ which is straightforward. To see the other direction, suppose $f \in I(\{a\})$. Since $f \in k[x_1, .., x_n]$, we can write it as $f = \sum_{i_1,...i_n \geq 0} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$. Since $f(a) = 0$, we can write this as $f(x) = \sum_{i_1,...i_n \geq 0} b_{i_1 \cdots i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}$ and so $f(x) \in (x_1 - a_1, ..., x_n - a_n)$. □

Definition 8. A ring R is called Noetherian if every ideal in R is finitely generated.

Example: **Fields and Principal Ideal Domains (PIDs) are Noetherian rings.**

One can easily verify the following equivalent definition of a Noetherian ring:

Proposition 4. R is Noetherian if and only if every sequence of ideals $I_1 \subset I_2 \subset \cdots$ stabilizes i.e there exists N such that $I_N = I_{N+1} = \cdots$.

Proof. Forward direction: If every ideal is finitely generated then the ideal $\cup_i I_i$ is finitely generated and so the generating set of $\cup_i I_i$ must lie in some I_N. Conversely, suppose the sequence stabilizes but there exists an I that is not finitely generated. Then take a sequence of $f_i \in I$ such that $f_i \notin (f_1, ..., f_{i-1})$ yields an increasing sequence of ideals i.e $(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \cdots$ that does not stabilize - contradiction. □

Theorem 5. (Hilbert Basis Theorem) If R is a Noetherian ring, then $R[x_1, ..., x_n]$ is a Noetherian Ring.

Proof. We know $R[x_1, ..., x_n] \cong R[x_1, ..., x_{n-1}][x_n]$. So, if we can prove that R Noetherian implies $R[x]$ is Noetherian, by induction we will have proven that $R[x_1, ..., x_n]$ is also Noetherian.

Suppose R is Noetherian. Let I be an ideal in $R[x]$. Let J denote the set of leading coefficients of polynomials in I. Then, given I is an ideal, J is an ideal in R. Since R is Noetherian, we can write that J is generated by the leading coefficients of $f_1, ..., f_r \in I$. Suppose $N \in \mathbb{Z}$ such that N is greater than the degrees of all polynomials $f_1, ..., f_r$. Then, for any $m \leq N$, we define J_m to be the ideal in R generated by the leading coefficients of all polynomials f in I such that $deg(f) \leq m$. Once again, since J_m is an ideal in R, we can say that J_m is generated by the finite set of polynomials, $\{f_{mj}\}$, such that each polynomial's degree is less than or equal to m. Finally, define I' be the ideal generated by polynomials $\{f_{mj}\}$ and f_i.

We claim $I' = I$. Suppose not i.e suppose there exists elements in I that are not in I'. Let g be the minimal element such that $g \in I$, $g \notin I'$.

Case 1: $deg(g) > N$. Then, there exists polynomials Q_i such that $\sum_i Q_i f_i$ has the same leading term as g. Therefore, $deg(g - \sum_i Q_i f_i) < deg(g)$. Since g is the minimal element and $deg(g - \sum_i Q_i f_i) < deg(g)$, therefore $g - \sum_i Q_i f_i \in I'$, which implies $g \in I'$.

Case 2: $m := deg(g) \leq N$. Then, there exists polynomials Q_j such that $\sum_j Q_j f_{mj}$ and g have the same leading term. Using a similar argument, we get that $g \in I'$. □

This has the following interesting implication:

Theorem 6. An algebraic set is the intersection of a finite number of hypersurfaces.

Proof. Let $V(I)$ be an algebraic set. We prove that I is finitely generated since that implies $V(I) = V(f_1, ..., f_r) = \cap_{i=1}^{r} V(f_i)$. Given k is a field, k is a Noetherian ring and by the Hilbert Basis Theorem, $k[x]$ is also Noetherian. Therefore, the ideal I in $k[x]$ is finitely generated. □

Corollary 7. $k[x_1, ..., x_n]$ is a Noetherian ring for any field k.

Proof. Follows from the Hilbert Basis Theorem. □

We have some other useful corollaries:

Corollary 8. Any descending chain of subvarieties of $\mathbb{A}^n$ must stabilize i.e if $V_1 \supset V_2 \supset V_3 \cdots$, then there exists N such that $V_N = V_{N+1} = \cdots$.

Corollary 9. There exists a finite subset $B \subset A$ such that $V(A) = V(B)$.

Exercise:

Define

$$R[[x]] = \{f(x) = \sum_{n=0}^{\infty} a_n x^n : a_n \in R\}.$$

Prove (1) Given $f \in R[[x]], f(x) = \sum_{n=0}^{\infty} a_n x^n$ and suppose there exists b_0 s.t $a_0 b_0 = 1$. Then, there exists $g \in R[[x]]$ s.t $fg = 1$. (2) Given R is Noetherian, $R[[x]]$ is also Noetherian. *Hint: Similar proof to Theorem 1, but use trailing coefficient (coefficient of the smallest power) instead of leading coefficient.*

2.2.1 Module-finite, Ring-finite, Field extensions

Definition 9. (R-Module). Let R be a ring. Let M be an abelian group $(M, +)$. Then, an R-module is M with multiplication $R \times M \to M$ such that for any $a, b \in R$, $m \in M$, $(a+b)m = am + bm, a(m+n) = am + an, (ab)m = a(bm), 1_R m = m$.

Examples of modules:
(1) $\mathbb{Z}^n$ where addition is defined as $(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n)$ and scalar multiplication is defined as $k \cdot (x_1, \cdots, x_n) = (kx_1, \cdots, kx_n)$. Similarly, $\mathbb{R}^n$ and other vector spaces are also modules.
(2) $R[x]$ is an R-module.

Definition 10. (Submodule). A submodule N is a subgroup of R-module, M, such that $an \in N$ for any $a \in R, n \in N$.

One can check that for any $m \in M$, $0_R m = 0_M$ by noting that $0_R m = (x-x)m = xm - xm = 0_M$ for any $x \in R, m \in M$. Also, the submodule N of an R-module is an R-module itself.

Definition 11. (Submodule generated by S). Let $S := \{s_1, s_2, ...\}$ be a set of elements of the R-module M. Then the submodule generated by S is $\{\sum_i r_i s_i | r_i \in R, s_i \in S\}$.

When S is finite, we denote the submodule generated by S as $\sum_i Rs_i$.

2.2.2 Finiteness Conditions of Subrings of a Ring

Definition 12. (Finiteness conditions of subrings of a ring). Let S be a ring and let R be a subring of S.
(1) S is module-finite over R if S is finitely-generated as an R-module i.e $S = \sum_{i=1}^n Rv_i$ where $v_1, ..., v_n \in S$. More explicitly, $S = \{\sum_{i=1}^n r_i v_i : r_i \in R\}$, for $v_1, ..., v_n \in S$ fixed.
(2) S is ring-finite over R if $S = R[v_1, ..., v_n] = \{\sum_i a_i v_1^{i_1} \cdots v_n^{i_n} | a_i \in R\}$ where $v_1, ..., v_n \in S$.
(3) S is a finitely-generated field extension of R if S and R are fields and $S = R(v_1, ..., v_n)$ (the quotient field of $R[v_1, ..., v_n]$) where $v_1, ..., v_n \in S$.

(Recall: the definition of field extension. Firstly, given A is a field, then a subset $B \subseteq A$ is a subfield if it contains 1 and it is closed under addition and multiplication and taking the inverse of non-zero elements of B. Given B is a subfield of A, we call A a field extension of B.)

Proposition 10. (Properties of finiteness conditions)
1. If S is module-finite over R, then S is ring-finite over R.
2. If $L = K(x)$, then L is a finitely-generated field extension of K but L is not ring-finite over K.

Proof. (1) follows from definitions. We prove (2). Using the definition, L is a finitely generated field extension of K and so $K(x)$ is a finitely-generated field extension of K. Now, suppose L is ring-finite over K. Then, $L = K[v_1, ..., v_n]$ and so $K(x) = K[v_1, ..., v_n]$, where $v_1, ..., v_n \in k(x)$. Then, there exists $v_i := \frac{s_i}{t_i} \in K(x)$ that generate L where $i = 1, ..., n$. Define $p := 1/q$ where q is an irreducible polynomial that has a higher degree than all t_i's. Then, as $p \in K(x) = L$, $p = \frac{h}{t_1^{e_1} \cdots t_n^{e_n}}$. Since q has a higher degree than all the t_i's and q is irreducible (which means only one t_i survives whose $e_i = 1$), we see that p cannot be equal to $\frac{1}{q}$. □

2.2.3 Integral over a Ring, Algebraic over a Ring

Definition 13. (Integral over R, Algebraic over R). Let R be a subring of the ring S. Then, $v \in S$ is integral over R if there exists a monic polynomial $f = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$ such that $f(v) = 0$ and $a_i \in R$. If R and S are fields, we say v is algebraic over R.

When all elements of S is integral over R, we say S is integral over R. When S and R are fields and S is integral over R, we call S an algebraic extension of R.

Theorem 11. Let R be a subring of an integral domain S and let $v \in S$. Then, the following are equivalent:

(1) v is integral over R.

(2) $R[v]$ is module-finite over R.

(3) There exists a subring R' of S such that R' contains $R[v]$ and it is module-finite over R.

Proof. We see (2) implies (3) readily. Now, (1) implies (2): Suppose v is integral over R with the monic polynomial $f(x) = x^n + a_1 x^{n-1} + ... + a_n$. Then, $f(v) = 0 \implies v^n \in \sum_{i=0}^{n-1} R v^i$. Therefore, for any integer m, $v^m \in \sum_{i=0}^{n-1} R v^i$. This implies $R[v]$ is module-finite over R.

Lastly, (3) implies (1) as follows: Suppose R' is module-finite over R. Then, $R' = \sum_{i=1}^{n} R w_i$, where $w_i \in R'$. Then, $v w_i \in R'$, so $v w_i = \sum_j a_{ij} w_j$ where $a_{ij} \in R$. Now, $v w_i - v w_i = 0$ implies $\sum_{j=1}^{n} \delta_{ij} v w_j - v w_i = 0$ which then implies $\sum_{j=1}^{n} (\delta_{ij} v - a_{ij}) w_j = 0$ (here $\delta_{ij} = 1\{i = j\}$. Write this in matrix notation and consider these equations in the quotient field of S and note than $(w_1, ..., w_n)$ is a non-trivial solution to these equations (as we see, they give 0). Therefore, $det(\delta_{ij} v - a_{ij}) = 0$ from which we get $v^n + a_1 v^{n-1} + ... + a_n = 0$. Therefore, v is integral over R. □

Corollary 12. The set of elements of S that are integral over R is a subring of R that contains R.

Proof. Suppose a, b are elements in S that are integral over R. Now. b is integral over R implies b is integral over $R[a]$ as $R \subset R[a]$. Therefore, by Theorem 11, $R[a, b]$ is module-finite over R. Then, $a + b, a - b, ab \in R[a, b]$ and so they are all integral over R. □

We will need one simple fact from linear algebra:

Lemma 13. If $A = (r_{ij})$ is an $n \times n$ matrix over R and V is a column vector s.t $AV = 0$, then $det(A)V = 0$.

Proof. This is because $det(A)V = det(A)I_nV = adj(A)AV = 0$. □

We will require the following results:

Theorem 14. Suppose an integral domain S is ring-finite over R. Then, S is module-finite over R if and only if S is integral over R.

Proof. For the forward direction: suppose the generators of S are $s_1, ..., s_n$ (where we take $s_1 = 1$ because we enlarge the set of generators as we please as long as it's finite) so $S = \sum_{i=1}^{n} Rs_i$. Then, for any $s \in S$, we can write s as $s = r_1s_1 + \cdots + r_ns_n$.

Now, $ss_i = \sum_{j=1}^{n} r_{ij}s_j$ because $ss_i \in S$ so can be written as a linear combination of s_i. Then, let I_n be the $n \times n$ identity matrix, V is the n dimensional column vectors where $V_i = s_i$ and $B = (r_{ij})$. Then, we can write these equations as $sIV = BV \implies (sI - B)V = 0$. Then, $det(sI - B)V = 0$. However, $v_1 = s_1 = 1$, so $det(sI - B) = 0$ which implies s is the root of a characteristic polynomial of B over R so s is integral over R.

Conversely, suppose S is integral over R and we are told that S is ring-finite over R i.e $S = R[s_1, ..., s_n]$. Then, for each $s_i \in S$, we have a monic polynomial from which we can write, after rearranging $s_i^{k_i} = a_{1,i}s_i^{k_i-1} + \cdots + a_{k_i-1,i}s_i + a_{k_i,i}$. Therefore, $s_i^{k_i}$ is in the submodule of S generated by $\{s_i, \cdots, s_i^{k_i-1}\}$ i.e s_i^m is in this submodule for any m. We know S is ring-finite over R with $s_1, ..., s_n$ as the generators. Now, the direct sum of the submodules (as we saw for each s_i) is also a finitely generated as an R-module and so S is itself module-finite over R. □

Theorem 15. Let L be a field and let k be an algebraically closed subfield of L. Then an element of L that is algebraic over k is in k. Furthermore, an algebraically closed field has no module-finite field extension except itself.

Proof. Proof of the first part - suppose $p \in L$ that is algebraic over k. Therefore, $p^n + a_1p^{n-1} + \cdots + a_n = 0$ with $a_i \in k$. This is a polynomial in $k[x]$ with a root, so by definition of algebraic closure, $p \in k$.

Now, we prove the second part. Suppose L is module-finite over k. Then, by theorem 14, L is integral over k. Then, by the first part $L = k$. □

Lastly,

Theorem 16. Let k be a field. Let $L = k(x)$ be the field of rational functions over k. Then, (a) any element of L that is integral over $k[x]$ is also in $k[x]$. (b) There is no non-zero element $f \in k[x]$ such that $\forall z \in L$, $f^n z$ is integral over $k[x]$ for some $n > 0$.

Proof. (a) p is integral over $k[x]$ implies there exists the following polynomial $p^n + a_1 p^{n-1} + ... = 0$. Now, since $p \in k(x)$, we may write it as $p = \frac{s}{t}$ where $s, t \in k[x], t \neq 0$. Then, we get $s^n + a_1 s^{n-1} t + \cdots + a_n t^n = 0$. Rearranging, we get $s^n = -a_1 s^{n-1} t - \cdots - a_n t^n$. Since t divides the right hand side, t divides s. This means, s/t is a polynomial in $k[x]$. Therefore, $p \in k[x]$.

(b) Suppose, not. Let f be such a function. Let $p(x) \in k[x]$ such that $p(x)$ does not divide f^m for any m. Set $z = \frac{1}{p}$, so $z \in L = k(x)$. Then, $f^n z = \frac{f^n}{p}$ is integral over $k[x]$. This means, there exists $a_i \in k[x]$ such that $(\frac{f^n}{p})^d + \sum_{i=1}^{d-1} a_i (\frac{f^n}{p})^i = 0$. From this, we get $f^{nd} = \sum_{i=1}^{d-1} a_i p^{d-i} f^{in}$. Since p divides the right hand side, we get that p divides f^{nd} which contradicts our definition of p. □

2.3 Hilbert's Nullstellensatz

First, we prove the following:

Theorem 17. (Zariski) If a field L is ring-finite over a subfield k, then L is module finite (and, hence, algebraic) over k.

Note that L is module finite over k if and only if L is integral over k which means L is algebraic over k.

Proof. Suppose L is ring-finite over k. Then, $L = k[v_1, ..., v_n]$ where $v_i \in L$. We proceed by induction.

Suppose $n = 1$. We have that k is a subfield of L and $L = k[v]$. Let $\psi : k[x] \to L$ be a homomorphism that takes x to v. Now $ker(\psi) = (f)$ for some f since $k[x]$ is a principal ideal domain. Then, $k[x]/(f) \cong k[v]$ by the first isomorphism theorem. This implies (f) is prime (since $k[v]$ is an integral domain).

Now, if $f = 0$. Then $k[x] \cong k[v]$, so $L \cong k[x]$. However, by the second property in proposition 10, this cannot be true. Therefore, $f \neq 0$.

Given $f \neq 0$, we can assume f is monic. Then, (f) prime implies f is irreducible and (f) is a maximal ideal (since every non-zero prime ideal in a PID is a maximal ideal). This means, $k[v] \cong k[x]/(f)$ is a field. Therefore, $k[v] = k(v)$ (since the quotient field is the "smallest" field containing $k[v]$). Since $f(v) = 0$, so v is algebraic over k and so, by theorem 11, $L = k[v]$ is module-finite over k. This concludes the proof for $n = 1$.

Now, for the inductive step, assume true for $n - 1$ i.e $k[v_1, ..., v_{n-1}]$ is module-finite over k. Let $L = k_1[v_2, ..., v_n]$ where $k_1 = k(v_1)$. Then, by the inductive hypothesis, $k_1[v_2, \cdots, v_n]$ is module-finite over k_1.

We show that v_1 is algebraic over k which would say $k[v_1]$ is module-finite over k concluding the proof. Suppose, v_1 is not algebraic over k. Then, using the inductive hypothesis, for each $i = 2, ..., n$, we have an equation $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots = 0$ where $a_{ij} \in k_1$.

Let $a \in k[v_1]$ such that a is a multiple of all the denominators of $a_{ij} \in k(v_1)$. We get $av_i^{n_i} + aa_{i1}(av_1)^{n_i-1} + \cdots = 0$. Then, by corollary 12, for any $z \in L = k[v_1, \cdots, v_n]$, there exists N such that $a^N z$ is integral over $k[v_1]$ (since the set of integral elements forms a subring). Since this holds for any $z \in L$, this also holds for any $z \in k(v_1)$. But by theorem 16, this is impossible. This gives us the contradiction. □

Theorem 18. (Nullstellensatz Version I) Assume k is algebraically closed. If I is a proper ideal in $k[x_1, ..., x_n]$, then $Z(I) \neq \emptyset$.

Proof. For any proper ideal I, there exists a maximal ideal J containing I. So, for simplicity, we assume I is the maximal ideal itself since $Z(J) \subset Z(I)$. Then, $L = k[x_1, \cdots, x_n]/I$ is a field (since I is maximal) and k is an algebraically closed subfield of L. Note that there is a ring-homomorphism from $k[x_1, ..., x_n]$ onto L by the natural projection. This means, L is ring-finite over k. Then, by theorem 17, L is module-finite over k. Then, by theorem 15, $L = k$ i.e $k = k[x_1, ..., x_n]/I$.

Now, since $k = L$, in particular this means $k \cong k[x_1, ..., x_n]/I$. Suppose $x_i \in k[x_1, ..., x_n]$ is mapped to a_i by the homormorphism ψ whose kernel is I. Then, $x_i - a_i$ is mapped to 0, so $x_i - a_i \in I$. Now, note that $(x_1 - a_1, ..., x_n - a_n)$ is a maximal ideal as one can easily verify and it contains I, so $I = (x_1 - a_1, ..., x_n - a_n)$. So, $(a_1, ..., a_n) \in Z(I)$. Therefore, $Z(I) \neq \emptyset$. □

The fact that every maximal ideal in the polynomial ring over n variables is of the form $(x_1 - a_1, ..., x_n - a_n)$ is a very important thing to remember. In fact, we will often use the fact that points in affine varieties correspond to maximal ideals made rigorous in the following:

Lemma 19. There is a natural bijection between a point $a \in \mathbb{A}^n$ and k-algebra homomorphisms $k[x_1, \cdots, x_n] \to k$. We say the point a corresponds to the maximal ideal defined by the kernel of this homomorphism.

Proof. Let $\phi : k[x_1, ..., x_n] \to k$ be a k-algebra homomorphism defined by $\phi(x_i) = a_i$, so $x_i - a_i \in ker(\phi)$. Now, $k[x_1, ..., x_n]/ker(\phi) \cong k$ so $ker(\phi)$ is a maximal ideal. □

We recall some definitions before moving to Hilbert's Nullstellensatz.

Definition 14. The radical of an ideal I in R is $\sqrt{I} := \{a \in R : a^n \in I, \text{for some } n \in \mathbb{Z}, n > 0\}$. It can be easily shown that $\sqrt{I}$ is an ideal itself and $I \subseteq \sqrt{I}$.

Definition 15. (Radical Ideal). The ideal I is called a radical ideal if $I = \sqrt{I}$.

We have two simple observations:

Lemma 20. For any ideal I in $k[x_1...x_n]$, $Z(I) = Z(\sqrt{I})$.

Proof. Note that $I \subseteq \sqrt{I}$ implies $Z(\sqrt{I}) \subseteq Z(I)$. Conversely, let $v \in Z(I)$ and let $f \in \sqrt{I}$. Then, $f^n \in I$ for some $n > 0$. This implies $f^n(v) = 0$ which implies $f(v) = 0$ as k has no zero divisor. Therefore, $v \in Z(\sqrt{I})$. □

Lemma 21. $\sqrt{I} \subset I(Z(I))$.

Proof. Suppose $s \in \sqrt{I}$. Then, $s^n \in I$ for some n. Now, let $v \in Z(I)$. Then, $s^n(v) = 0$ implies $s(v) = 0$, so $s \in I(Z(I))$. □

Now, we prove Hilbert's Nullstellensatz:

Theorem 22. (Hilbert's Nullstellensatz) Let I be an ideal in $k[x_1, ..., x_n]$ where k is algebraically closed. Then, $I(Z(I)) = \sqrt{I}$.

Proof. We already know $\sqrt{I} \subset I(Z(I))$. So, we only need to prove the other direction. Let $I = (f_1, ..., f_r)$ where $f_i \in k[x_1, ..., x_n]$. Suppose, $G \in I(Z(f_1, ..., f_r))$. Define $J := (f_1, ..., f_r, x_{n+1}G - 1) \subset k[x_1, ..., x_n, x_{n+1}]$. Then, $V(J) \subset \mathbb{A}^n_k$ is $\emptyset$ since G is 0 whenever all f_i are 0 and therefore, $x_{n+1}G - 1 \neq 0$ at those points.

Since $Z(J) = \emptyset$, J is not a proper ideal by Nullstellensatz version I. Therefore, $J = k[x_1, \cdots, x_{n+1}]$. So, $1 \in J$ (since J is not a proper ideal). So $1 = \sum_i a_i(x_1, ..., x_{n+1})f_i + b(x_1, .., x_{n+1})(x_{n+1}G - 1)$.

In particular, if $x_{n+1} = \frac{1}{G}$, then, $1 = \sum_i a_i f_i + b(1 - 1) = \sum_i a_i f_i$. Therefore, $G^N = G^N \sum_i a_i f_i$, so $G^N \in (I)$. Therefore, $G \in \sqrt{I}$. Therefore, $I(Z(I)) \subseteq \sqrt{I}$. □

This has a series of interesting applications.

Corollary 23. If I is a radical ideal in $k[x_1, ..., x_n]$, then $I(Z(I)) = I$. Therefore, there is a one-to-one correspondence between radical ideals and algebraic sets.

Corollary 24. For any subset $Y \subseteq \mathbb{A}^n$, $Z(I(Y)) = \bar{Y}$, the closure of Y.

Proof. We note that $Y \subseteq Z(I(Y))$ and since the latter is closed, $\bar{Y} \subseteq Z(I(Y))$. Conversely, let W be a closed set containing Y, so $W = Z(a)$ for some ideal $a \in k[x_1, \cdots, x_n]$. Then, $Y \subseteq Z(a) \implies I(Z(a)) \subseteq I(Y)$. Also $a \subseteq I(Z(a))$ so $Z(I(Y)) \subseteq Z(a) = W$, so $Z(I(Y)) \subseteq \bar{Y}$. So, $Z(I(Y)) = \bar{Y}$. □

Corollary 25. An algebraic set $Z(T)$ is irreducible if and only if $I(Z(T))$ is a prime ideal. There is a one-to-one correspondence between prime ideals and irreducible algebraic sets. The maximal ideals correspond to points.

Corollary 26. Let F be a non-constant polynomial in $k[x_1, \cdots, x_n]$ with the irreducible decomposition of F being $F = F_1^{n_1} F_2^{n_2} \cdots F_r^{n_r}$. Then, $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components and $I(V(F)) = (F_1 \cdots F_r)$. Therefore, there is a one-to-one correspondence between irreducible polynomials $F \in k[x_1, \cdots, x_n]$ (up to multiplication by a non-zero element of k) and irreducible hypersurfaces in $\mathbb{A}^n_k$.

Corollary 27. Let I be an ideal in $k[x_1, \cdots, x_n]$. Then, $V(I)$ is a finite set if and only if $k[x_1, \cdots, x_n]/I$ is a finite dimensional vector space over k. If this occurs, then, the number of points in $V(I)$ is at most $dim_k(k[x_1, \cdots, x_n]/I)$.

Proof. Let $p_1, \cdots, p_r \in V(I)$. Choose $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$ such that $f_i(p_j) = 0$ if $i \neq j$ and $f_i(p_i) = 1$ and let $\bar{f}_i$ be the residue class of f_i. Now, if $\sum_i \lambda_i \bar{f}_i = 0$ with $\lambda_i \in k$, then, $\sum_i \lambda_i f_i \in I$. Therefore, $\lambda_j = (\sum_i \lambda_i f_i)(p_j) = 0$. Therefore, $\bar{f}_i$ are linearly independent over k. So $r \leq dim_k(k[x_1, \cdots, x_n]/I)$.

Conversely, suppose $V(I) = (p_1, \cdots, p_r)$ and so is finite. Let $p_i = (a_{1i}, \cdots, a_{1n})$ and define $f_j := \prod_{i=1}^{r}(x_j - a_{ij}), j = 1, \cdots, n$. Then, $f_j \in I(V(I))$, so for all j, $f_j^N \in I$ for some large enough $N > 0$. Now, taking I-residues, $\bar{f}_j{}^N = 0$. By expanding f_j^N, we get that $\bar{x_j}^{rN}$ is a k-linear combination of $\bar{1}, \bar{x_j}, \cdots, \bar{x_j}^{rN-1}$. So, for all s, $\bar{x_j}^s$ is a k-linear combination of $\bar{1}, \bar{x_j}, \cdots, \bar{x_j}^{rN-1}$. Therefore, the set $\{\bar{x_1}^{m_1}, \cdots, \bar{x_n}^{m_n} : m_i < rN\}$ generates $k[x_1, \cdots, x_n]/I$ as a vector space over k. □

Definition 16. Reduced Rings. A ring R is called reduced if $f^N = 0 \in R$ implies $f = 0$.

Examples:
(1) $\mathbb{A}^n$ is irreducible since it corresponds to the zero ideal in $k[x_1, \cdots, x_n]$, which is prime.

Definition 17. (Affine Curve). Let f be an irreducible polynomial in $k[x, y]$. Since $k[x, y]$ is a UFD, f generates a prime ideal in $k[x, y]$. Then, the set $Z(f)$ is irreducible. $Z(f)$ is called the *affine curve* defined by the equation $f(x, y) = 0$. If f is of degree d, we say that $Z(f)$ is an affine curve of degree d.

Definition 18. (Surface and hypersurface). If f is an irreducible polynomial in $k[x_1, \cdots, x_n]$, then we call the affine variety $V(f)$ a surface when $n = 3$ and a hypersurface when $n > 3$.

Next, we find irreducible decompositions of algebraic sets of an affine space.

2.4 Irreducible Components of Algebraic Sets

So far, we have seen polynomials and the varieties defined over them. Now, we bring in topological invariants.

Definition 19. Irreducible decomposition of a set. Let $V \in \mathbb{A}_k^n$ be an algebraic set. Then, V is reducible if $V = V_1 \cup V_2$ where V_1, V_2 are non-empty, algebraic sets in $\mathbb{A}_k^n$ i.e $V_i \neq V$ for $i = 1, 2$. If V is not irreducible, we call it reducible.

Theorem 28. The algebraic set V is irreducible if and only if $I(V)$ is prime.

Proof. Suppose, V is irreducible. Now, suppose for contradiction, $I(V)$ is not prime. Therefore, by definition of prime, there exists $f_1 f_2 \in I(V)$ such that $f_1 \notin I(V)$ and $f_2 \notin I(V)$. Now, $V = (V \cap Z(f_1)) \cup (V \cap Z(f_2))$ and $V \cap Z(f_i) \subset V, V \cap Z(f_i) \neq V$; to see this, note that for any $p \in V$ such that p is a zero of $f_1 f_2$, p has to be a root of either f_1 or f_2 since f_i belong to an integral domain, therefore, $p \in (V \cap V(f_1)) \cup (V \cap V(f_2))$ (the other direction is obvious). Then, $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ is decomposition of V which means V is not irreducible - contradiction.

Conversely, suppose $I(V)$ is prime. For contradiction, suppose V is reducible with $V = V_1 \cup V_2$, V_i non-empty. Then, consider $f_i \in I(V_i)$ such that $f_i \notin I(V)$. Clearly, $f_1 f_2 \in I(V)$, so $I(V)$ is not prime - contradiction. □

Corollary 29. The affine space $\mathbb{A}_k^n$ is irreducible if k is infinite.

Theorem 30. Let A be a non-empty collection of ideals in a Noetherian ring R. Then, A has a maximal ideal i.e an ideal I such that $I \in A$ and no other ideal in A contains I.

Proof. Given our collection of ideals, A, choose an ideal $I_0 \in A$. Then, define $A_1 = \{I \in A : I_0 \subsetneq I\}$ and $I_1 \in A_1$, $A_2 = \{I \in A : I_1 \subsetneq I\}$ and $I_2 \in A_2$ and so on. Then, the statement in the theorem is equivalent to saying that there exists positive integer n such that A_n is empty since that would mean there exists no ideal containing I_{n-1}. Suppose this is not true. Then, with $I := \cup_{n=0}^{\infty} I_n$, since R is Noetherian, therefore there exists $f_1, ..., f_m$ that generates the ideal I where each $f_i \in I_n$ for n sufficiently large. But since the generates are all in I_n, $I = I_n$ and so $I_{n'} = I_n$ for any $n' > n$ (since $I = \cup_{n=0}^{\infty} I_n$ by definition) - contradiction. □

We finally prove the main result. Note that this is pretty closely tied to the Hilbert Basis Theorem which says that every algebraic set is the intersection of a finite number of algebraic sets/hypersurfaces:

Theorem 31. Let V be an algebraic set in $\mathbb{A}_k^n$. Then, there exists unique, irreducible algebraic sets $V_1, ..., V_r$ such that $V = V_1 \cup V_2 \cdots \cup V_r$ and $V_i \subsetneq V_j$ for any $i \neq j$.

Proof. Proving this statement is equivalent to disproving that $\mathcal{F}$ is non-empty where $\mathcal{F} := \{\text{algebraic set } V \in \mathbb{A}_k^n : V \text{is not the union of finitely many irreducible algebraic sets}\}$.

Suppose, $\mathcal{F}$ is not empty. Let $V \in \mathcal{F}$ such that V is the minimal member of $\mathcal{F}$ i.e V cannot be written as the union of sets in $\mathcal{F}$.

Now, since $V \in \mathcal{F}$, V is reducible (if V is irreducible, then it is trivially the union of 1 irreducible subsets). Since V is reducible, $V = V_1 \cup V_2$ where $V_i \neq \emptyset$. Since V is the minimal member of $\mathcal{F}$, $V_i \notin \mathcal{F}$. Since $V_i \notin \mathcal{F}$, it is the union of finitely many irreducible algebraic sets, so let $V_i = V_{i1} \cup V_{i2} \cdots \cup V_{im_i}$. Then, $V = \cup_{i,j} V_{ij}$, so $V \notin \mathcal{F}$. So, we have shown that V can be written as $V = V_1 \cup \cdots \cup V_m$ where each V_i is irreducible. First, remove any V_i such that $V_i \subset V_j$. Now we prove uniqueness. Suppose $V = W_1 \cup \cdots W_m$ be another such decomposition. Then, $V_i = \cup_j (W_j \cap V_i)$. Now, $W_j \cap V_i = V_i$ since otherwise we will have found a decomposition of the irreducible set V_i. Therefore, $V_i \subset W_{j(i)}$ for some $j(i)$. Similarly, by symmetry, $W_{j(i)} \subset V_k$ for some k. But then, $V_i \subset V_k$ implies $i = k$ and so $V_i = W_{j(i)}$. Continuing this for each $i \in \{1, ..., m\}$, we get that the two decompositions are equal. □

Furthermore, we use the following terms:

Definition 20. An ideal $I \subset k[x_1, ..., x_n]$ set-theoretically defines a variety V if $V = Z(I)$. An ideal $J \subset \mathbb{A}^n$ scheme-theoretically defines a variety V if $J = I(V)$.

Here's a pretty straightforward result:

Theorem 32. For an affine variety X, if $f_1, ..., f_m$ scheme-theoretically define X, then $Z(I(X)) = X$

Two affine-varities can be isomorphic in the usual sense using the language of polynomial maps:

Definition 21. Isomorphic affine varieties. Two affine varieties $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ are isomorphic if there exists polynomial maps $f : V \to W$ and $g : W \to V$ such that $f \circ g = g \circ f = i_d$.

Theorem 33. Let f and g be two polynomials in $k[x, y]$ with no common factors. Then, $Z(f, g)$ is a finite set of points.

Proof. Check [1]. □

2.5 Coordinate Rings

Definition 22. (Coordinate Ring). If $Y \subseteq \mathbb{A}^n$ is an affine algebraic set, then we define the affine coordinate ring, $A(Y)$, of Y to be $k[x_1, \cdots, x_n]/I(Y)$.

Note that if Y is an affine variety, then $I(Y)$ is prime and so $A(Y)$ is an integral domain.

Definition 23. k-algebra. Let k be a field (i.e a commutative division ring). A ring R is a k-algebra if $k \subseteq Z(R) := \{x \in R : xy = yx, \forall y \in R\}$ and the identity of k is the same as the identity of R.

Note, $Z(R)$ is the center of the ring R.

Definition 24. Finitely generated k-algebra. A finitely generated k-algebra is a ring that is isomorphic to a quotient of a polynomial ring $k[x_1, ..., x_n]/I$.

Equivalently, a ring R is a finitely-generated k-algebra if R is generated as a ring by k with some finite set $r_1, ..., r_n$ of elements of R i.e $k[r_1, ..., r_n]$.

These definitions are equivalent. Suppose, R is a finitely generated k-algebra i.e $R = k[r_1, ..., r_n]$. Then, define a ring homomorphism that sends x_i to r_i. Since R is generated by r_i, this map is surjective and by quotienting over the kernel, we get the isomorphism $R \cong k[x_1, \cdots, x_n]$. Conversely, suppose $R \cong k[r_1, .., r_n]/I$. Then, let $\varphi : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/I = R$. Then, R is generated by the images of $x_1, \ldots, x_n$ under φ. Let the images be $r_1, \ldots, r_n$ and as such $R = k[r_1, \ldots, r_n]$.

Example: Any finitely generated k-algebra which is an integral domain is the affine coordinate ring of some affine variety. This is because if B is such a finitely generated k-algebra, then $B \cong k[x_1, \ldots, x_n]/I$ and then the corresponding affine variety is $Z(I)$.

2.6 Dimension of Affine Varieties

First, we define a notion of dimension on a topological space:

Definition 25. (Dimension of a topological space). Let X be a topological space. Then, the dimension of X is defined to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X.

Definition 26. (Dimension of an affine and quasi-affine variety). Let X be an affine variety or quasi-affine variety. Then, the dimension of X is defined to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. So,

$$dim(X) := \sup\{n \in \mathbb{Z} \mid \exists X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subsetneq X, X_i \text{ irreducible closed subsets of } X\}.$$

Example: $dim(\mathbb{A}^1) = 1$ as the only irreducible closed subsets of X are single points and the whole space $\mathbb{A}^1$.

Definition 27. (Height of a prime ideal). In a ring A, the height of a prime ideal I is the supremum of integers n such that there exists a chain $I_0 \subset I_1 \subset \cdots \subset I_n = I$ of distinct prime ideals.

Definition 28. (Krull Dimension of a ring A). The Krull dimension of a ring A is the supremum of the heights of all prime ideals.

Proposition 34. Let Y be an affine algebraic set. Then, the dimension of Y is equal to the dimension of its affine coordinate ring $A(Y)$.

Proof. The closed irreducible subsets of Y correspond to prime ideals of $k[x_1, .., x_n]$ containing $I(Y)$. These correspond to prime ideals of $A(Y)$. Thus, dim Y is the length of the longest chain of prime ideals of $A(Y)$, which is its Krull dimension. □

We need the following definitions to bring in some results from noetherian rings.

Definition 29. (Algebraic vs transcendental elements). Suppose L is a field extension of K (i.e. K is a subfield of L that is not equal to L). Denote this by writing L/K. An element $a \in L$ is algebraic over K if there exists a polynomial $p(x)$ in $K[x]$ s.t. $p(a) = 0$. Otherwise, we say a is transcendental over K.

Definition 30. (Algebraically independent over K). Let L/K be a field extension. Then, the set of elements of $a_1, \cdots, a_n \in L$ are algebraically independent over K if there exists no polynomial $p(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ s.t. $p(a_1, \cdots, a_n) = 0$.

Definition 31. (Transcendence degree of a field extension L/K). The transcendence degree of a field extension L/K, denoted $tr.deg(L/K)$ is the maximum number of elements in L that are algebraically independent over K.

Proposition 35. Let k be a field. Let B be an integral domain which is a finitely generated k-algebra. Then,
(1) The dimension of B is equal to the transcendence degree of the quotient field $K(B)$ (i.e. the field of fractions) of B over k.
(2) For any prime ideal I in B, we have

$$\text{height } I + \text{dim } B/I = \text{dim } B.$$

We apply this as follows:

Theorem 36. The dimension of $\mathbb{A}^n$ is n.

Proof. Dimension of $\mathbb{A}^n$ is equal to the dimension of $A(\mathbb{A}^n) = k[x_1, \cdots, x_n]$. By the previous proposition's part (a), this is equal to $tr.deg(k(x_1, ..., x_n)/k)$. This is equal to n because for the variables $x_1, ..., x_n$, if there is any polynomial $p(x_1, \cdots, x_n) = 0$, then $p = 0$. There is no larger set of elements for which this is true - if we choose $T_1, \cdots, T_n, T_{n+1}$, then we can define the polynomial $p(T_1, \cdots, T_n, T_{n+1}) = f(T_1, \cdots, T_n) - T_{n+1}$ where $f(T_1, \cdots, T_n) = T_{n+1}$ and then p is 0 at $(T_1, \cdots, T_n, T_{n+1})$. □

Proposition 37. If Y is a quasi-affine variety, then dim $Y =$ dim $\bar{Y}$.

Theorem 38. Let A be a noetherian ring and let $f \in A$ be an element which is not a zero divisor nor a unit. Then, every minimal prime ideal p containing f has height 1.

Proposition 39. A noetherian integral domain A is a unique factorization domain if and only if every prime ideal of height 1 is principal.

Lastly, we have

Proposition 40. A variety Y in $\mathbb{A}^n$ has dimension $n - 1$ if and only if it is the zero set $Z(f)$ of a single nonconstant irreducible polynomial in $k[x_1, \cdots, x_n]$.

3 Projective Varieties

Definition 32. (Projective n-space). Let k be an algebraically closed field. The projective n-space over k, denoted $\mathbb{P}^n_k$ or $\mathbb{P}^n$, is the set of equivalence classes of $n+1$-tuples $a_0, \cdots, a_n$ of elements of k, not all zero, under the equivalence relation given by $(a_0, \cdots, a_n) \sim (\lambda a_0, \cdots, \lambda a_n)$ for all non-zero $\lambda \in k$.

An element of $\mathbb{P}^n$ is called a point. If P is a point, then any $(n+1)$-tuple $(a_0, \cdots, a_n)$ in the equivalence class of P is called a set of homogenous coordinates for P.

We will require a few constructions from algebra now.

Definition 33. (Graded Ring). A graded ring is a ring S with the decomposition $S = \oplus_{d \geq 0} S_d$ of S into a direct sum of *abelian groups* S_d such that for any $d, e \geq 0$, $S_d \cdot S_e \subseteq S_{d+e}$.

Definition 34. (Homogenous element of degree d or forms of degree d). An element of S_d in a graded ring $S = \oplus_{d \geq 0} S_d$ is called a homogenous element of degree d.

Any element of S can be written, uniquely, as a finite sum of homogenous elements.

Definition 35. (Homogenous ideals). An ideal $I \subseteq S$ is called a homogenous ideal if $I = \oplus_{d \geq 0}(I \cap S_d)$.

Proposition 41. An ideal I is homogenous if and only if it can be generated by homogenous elements

Proof. Let I be a homogenous ideal i.e. $I = \oplus_{d \geq 0}(I \cap S_d)$. Then, consider $f \in I$, which we can write as $f = f_0 + f_1 + f_2 + \cdots$ where each f_i is a homogenous element. Then, the ideal I is generated by these homogenous elements that constitute each element of I. Conversely, suppose I is generated by homogenous elements $f_1, f_2, \cdots$. Then, clearly any arbitrary element of I can be written as $a_1 f_1 + a_2 f_2 + \cdots$ where $a_i \in S$. Write each a_i as a sum of homogenous elements and we see that $I = \oplus_{d \geq 0}(I \cap S_d)$. □

Proposition 42. The sum, product, intersection and radical of homogenous ideals are homogenous.

Proposition 43. A homogenous ideal I is prime if, for any two *homogenous elements* f, g s.t. $fg \in I$, we have that $f \in I$ or $g \in I$.

Now, we come back to the polynomial ring. For a polynomial ring $S := k[x_1, \cdots, x_n]$, we can construct it as a graded ring by letting S_d be the set of all linear combinations of monomials (or forms) of degree d in $x_0, \cdots, x_n$.

Why do we care about homogenous polynomials? If f is a homogenous polynomial of degree d, then $f(\lambda a_0, \cdots, \lambda a_n) = \lambda^d f(a_0, \cdots, a_n)$. This means whether the polynomial is 0 or not depends only on the *equivalence class of* $(a_0, \cdots, a_n)$. Therefore, f defines a function from $\mathbb{P}^n$ to $\{0, 1\}$ by $f(P) = 0$ if $f(a_0, \cdots, a_n) = 0$ and $f(P) = 1$ if $f(a_0, \cdots, a_n) \neq 0$.

Definition 36. (Zero set of a set of homogenous polynomials). The zeros of a homoygenous polynomial is $Z(f) = \{P \in \mathbb{P}^n | f(P) = 0\}$. If T is any set of homogenous elements of $k[x_1, \cdots, x_n]$, we define the zero set of T to be $Z(T) = \{P \in \mathbb{P}^n | f(P) = 0, \forall f \in T\}$.

If I is a homogenous ideal of $k[x_1, \cdots, x_n]$, we define $Z(I) = Z(T)$ where T is the set of all homogenous elements in I. Since $k[x_1, \cdots, x_n]$ is a Noetherian ring, any set of homogenous elements T has a finite subset $f_1, \cdots, f_r$ such that $Z(T) = Z(f_1, \cdots, f_r)$.

Definition 37. (Algebraic Set). A subset Y of $\mathbb{P}^n$ is an algebraic set if there exists a set T of homogenous elements of $k[x_1, \cdots, x_n]$ such that $Y = Z(T)$.

In particular, if f is a *linear homogenous polynomial,* then $Z(f)$ is called a hyperplane.

Once again, we have that the union of finitely many algebraic sets is an algebraic set, intersection of any family of algebraic sets is an algebraic set, the empty set and all of $\mathbb{P}^n$ are algebraic sets.

Definition 38. (Zariski topology on $\mathbb{P}^n$). The Zariski topology on $\mathbb{P}^n$ is defined by letting the closed sets be algebraic sets in $\mathbb{P}^n$.

Definition 39. (Projective algebraic variety and quasi-projective variety). A projective algebraic variety is an irreducible algebraic set in $\mathbb{P}^n$. An open subset of a projective variety is called a quasi-projective variety.

Definition 40. (Homogenous ideal). If Y is any subset of $\mathbb{P}^n$, we define the homogenous ideal of Y in $k[x_1, \cdots, x_n]$, denoted $I(Y)$, to be the ideal *generated by*

$$\{f \in S | f \text{ is homogenous and } f(P) = 0, \forall P \in Y\}.$$

Definition 41. (Homogenous coordinate ring). If Y is an algebraic set, we define the homogenous coordinate ring of Y is (with $I(Y)$ the homogenous ideal of Y)

$$S(Y) = k[x_1, \cdots, x_n]/I(Y).$$

Definition 42. (H_i and U_i). We denote the zero set of x_i to be H_i for $i = 0, ..., n$. We define the open set $U_I := \mathbb{P}^n - H_i$ i.e.

$$U_i := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n | x_i \neq 0\}.$$

Open cover of $\mathbb{P}^n$: We now have an open cover of $\mathbb{P}^n$ by the open sets U_i, for $i = 0, \cdots, n$.

Map to affine n-space. We now define the map $\varphi_i : U_i \to \mathbb{A}^n$ such that if $P = (a_0, ..., a_n) \in U_i$, then $\varphi_i(P) = Q$ where Q is the point with affine coordinates

$$\left(\frac{a_0}{a_i}, \cdots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \cdots, \frac{a_n}{a_i}\right).$$

Proposition 44. The map $\varphi_i : U_i \to \mathbb{A}^n$ is a homeomorphism of U_i with its induced topology to $\mathbb{A}^n$ with its Zariski topology.

Proof. One can easily check that φ is bijective. We now show that the map takes closed sets to closed sets. Consider φ_0. We define the map $\alpha : S^h \to k[y_1, \cdots, y_n]$ where S^h is the set of homogenous elements of $k[x_0, \cdots, x_n]$ and the map $\beta : k[y_1, \cdots, y_n] \to S^h$. Let $f \in S^h$, then $\alpha(f) = f(1, y_1, \cdots, y_n)$. On the other hand, for $g \in k[y_1, \cdots, y_n]$ of degree e, we let $\beta(g) = x_0^e g(x_1/x_0, \cdots, x_n/x_0)$. Let $Y \subseteq U$ be a closed subset. Let $\bar{Y}$ be the closure in $\mathbb{P}^n$. Since this is a closed set, this is an algebraic set and so $\bar{Y} = Z(T)$ for some $T \subseteq S^h$. Define $T' := \alpha(T)$. One can check that $\varphi(Y) = Z(T')$. Conversely, let W be a closed subset of $\mathbb{A}^n$. Then, $W = Z(T')$ for some subset T' of $k[y_1, \cdots, y_n]$ and $\varphi^{-1}(W) = Z(\beta(T')) \cap U$. Thus, φ and φ^{-1} are both closed maps, so φ is a homeomorphism. □

Corollary 45. If Y is a projective (respectively, quasi-projective) variety, then Y is covered by the open sets $Y \cap U_i$, $i = 0, \cdots, n$ which are homeomorphic to affine (respectively, quasi-affine) varieties via the mapping φ_i defined above.

4 Ring Theory Revision

All the material here is from Dummit and Foote's "Abstract Algebra". Detailed proofs of the theorems can be found in the text.

4.1 Rings

Definition: Rings. A ring R is a set with binary operations $\times$ and $+$ such that
(1) $(R, +)$ is an abelian group (i.e has identity, inverses and associativity).
(2) $\times$ is associatve i.e $(a \times b) \times c = a \times (b \times c)$
(3) distributive laws hold in R i.e $\forall a, b, c \in R$, we have $(a+b)\cdot c = a\cdot c + b\cdot c$ and $a\cdot(b+c) = a\cdot b + a\cdot c$.

Note: Rings that are commutative under multiplication are called **commutative rings**.

Example: Ring without identity The set of even integers $2\mathbb{Z}$ since 1 is not even.

Example: Ring of functions. For X a non-empty set and A any ring, the set of functions $f : X \to A$ forms a ring R with operations $(f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x)$. R is commutative if and only if A is commutative. R has identity 1 if and only if A has 1.

Example: Some other easy rings. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings. $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity 1.

Example: Trivial and Zero ring. Any abelian group is a trivial ring with the operation $x \cdot y = 0$ for any $x, y \in R$.

Definition: Division Ring. A ring R with identity $1 \neq 0$ such that every $x \in R$ has a multiplicative inverse $x^{-1} \in R$ with $xx^{-1} = x^{-1}x = 1$ is a division ring.

Definition: Field. A field is a commutative division ring.

Proposition: Immediate properties of rings For any ring R:
(1) $0x = x0 = 0, \forall x \in R$
(2) $(-x)y = x(-y) = -(xy), \forall x, y \in R$
(3) $(-x)(-y) = xy, \forall x, y \in R$
(4) if $\exists 1 \in R$, then 1 is unique and $-x = (-1)x, \forall x \in R$.

Proposition: A finite division ring is a field.

Definition: Zero divisor. Let R be a ring. Let $x \neq 0$. Then, x is a zero divisor if $\exists y \in R, y \neq 0$ such that $xy = 0$ or $yx = 0$.

Definition: Unit. Let R be a ring with identity 1. Then, $x \in R$ is called a unit if there exists $y \in R$ such that $xy = yx = 1$.
$R^\times$ is the set of units in ring R. $(R^\times, \times)$ is a group under multiplication called the group of units.

Example of zero divisor: Let $x \neq 0$ be an integer and suppose x is relatively prime to $n \in \mathbb{Z}$. Then, x is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.

Lemma: If $x \in R$ is a zero divisor then x is not a unit. If $x \in R$ is a unit, then x is not a zero divisor.

Corollary: Fields have no zero divisors.

Example: zero divisor. Let $x \neq 0, x \in \mathbb{Z}$ and suppose x is relatively prime to $n \in \mathbb{Z}$. Then, $\bar{x}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.

4.2 Integral Domains and Subrings

Definition: Integral Domain. A commutative ring with identity $1 \neq 0$ such that it has no zero divisor.

Proposition: Cancellation laws hold in integral domains. Let $a, b, c \in R$ such that a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$. In other words, if a, b, c are elements in an integral domain, then, $ab = ac \implies a = 0$ or $b = c$.

Proposition: Any finite integral domain is a field.

Proof. Let R be a finite integral domain. Let $a \in R$ s.t. $a \neq 0$. We find a multiplicative inverse for a. Consider the map $\varphi(x) = ax$ for all $x \in R$. This map is injective by the previous proposition. Since R is finite and the map is injective, this map must also be surjective. Thus, there exists x such that $ax = 1$. □

Definition: Subring. A subring of the ring R is a subgroup of R that is closed under multiplication i.e $S \neq \emptyset$ is closed under addition, for each $x \in S$, there exists an additive inverse in S, $0 \in S$ and S is closed under multiplication.

Definition: Polynomial Rings. Let R be a commutative ring with identity 1. Let x be an indeterminate. Then, $R[x]$ is the ring of polynomials $\sum_{i=1}^{n} a_i x^i, n \geq 0, a_i \in R$. If $a_n \neq 0$, degree of the polynomial is n. Monic polynomials are those with $a_n = 1$. $R \subset R[x]$ is the set of constant polynomials. $R[x]$ is itself a commutative ring with identity (where 1 is the same identity as in R).

Note: if S is a subring of R, then $S[x]$ is a subring of $R[x]$.

Proposition: immediate properties of polynomial rings. Let R be an integral domain. Let $p(x), q(x)$ be non-zero elements of $R[x]$. Then,
(1) degree $p(x)q(x)$ = degree $p(x)$+ degree $q(x)$.
(2) the units of $R[x]$ are the same as the units of R
(3) $R[x]$ is an integral domain.

Definition: Ring homomorphisms. Let R and S be rings. A ring homomorphism $f : R \to S$ is a map such that $f(x + y) = f(x) + f(y), f(xy) = f(x)f(y), \forall x, y \in R$. A bijective ring homomorphism is called an **isomorphism** and we say $R \cong S$.

Lemma: Let $f : R \to S$ be a ring homomorphism. Then, $Im(f)$ be a subring of S and $ker(f)$ is a subring of R.

Examples of subrings: $\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of $\mathbb{R}$. $2\mathbb{Z}$ and $n\mathbb{Z}$ are subrings of $\mathbb{Z}$.

4.3 Ideals

Definition: Ideals. Let R be a ring, let $r \in R$ and let I be a subset of R. Then, $rI := \{rx : x \in I\}$. $Ir := \{xr : x \in I\}$. A subset I of R is a left ideal of R if I is a subring of R and $rI \subseteq I, \forall r \in R$. A subset I of R is a right ideal of R if I is a subring of R and $Ir \subseteq I, \forall r \in R$. If I is both a left and right ideal, it is called an ideal of R.

Definition (Quotient ring of R by an ideal). Let I be an ideal of the ring R. Then, R/I is the quotient ring of R by I. The elements of this quotient ring are of the form $r + I$ for $r \in R$ and $r + I = s + I$ if $r - s \in I$.

Proposition: Quotient ring is a ring. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations $(r+I)+(s+I) = (r+s)+I, (r+I)(s+I) = (rs + I), \forall r, s \in R$. Conversely, if I is any subgroup of R such that these two operations are well-defined, then I is an ideal of R.

Proposition: Isomorphism Theorems for Rings.
(1) (First Isomorphism Theorem for Rings) If $\psi : R \to S$ is a ring homomorphism, then $ker(\psi)$ is an ideal of R, $Im(\psi)$ is a subring of S and $R/ker(\psi) \cong \psi(R)$.
(2) If I is an ideal of R, then the map $R \to R/I$ defined by $r \to r + I$ is a surjective ring homomorphism with kernel I. This is the natural projection of R onto R/I. Every ideal is the kernel of a ring homomorphism and vice-versa.
(3) (Second Isomorphism Theorem for Rings) Let A be a subring and B be an ideal of the ring R. Then, $A + B = \{a + b | a \in A, b \in B\}$ is a subring of R and $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.
(4) (Third Isomorphism Theorem for Rings) Let I and J be ideals of the ring R with $I \subseteq J$. Then,

J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
(5) (Lattice/Fourth Isomorphism Theorem for Rings) Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion-preserving bijection between the set of subrings of R that contain I and the set of subrings of R/I (in other words, if $A \subseteq B$ and both contain I, then $A/I \subseteq B/I$ + if $J \subseteq K$ are ideals containing I, then $J/I \subseteq K/I$). Also, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Definition: Proper ideal. An ideal I is proper if $I \neq R$.

Example: R and $\{0\}$ are ideals of R. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any $n \in \mathbb{Z}$.

Definition (Ideals generated by a set). Let R be a ring with identity 1. Let A be a subset of R. Let (A) be the smallest ideal of R containing A. Then,
(1) (A) is the smallest ideal of R containing A, called the ideal generated by A:

$$(A) = \cap_{\text{(I is an ideal, A} \subseteq \text{I)}} I$$

.
(2) Define $RA = \{\sum_i r_i a_i : r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$. Define RA and RAR similarly. We say RA is the left ideal generated by A, AR is the right ideal generated by A and RAR is the ideal generated by A. **If R is commutative,** $RA = AR = RAR = (A)$**.**
(3) Principle ideals are ideals generated by a single element.
(4) A finitely general ideal is an ideal generated by a finite set.

Proposition (conditions for proper ideal and fields): Let I be an ideal of R, where R is a ring with identity 1. (1) $I = R$ if and only if I contains a unit. (2) If R is commutative, then R is a field if and only if its only ideals are the zero ideal $\{0\}$ and R.

Corollary: If R is a field, then any non-zero ring homomorphism from R into another ring is an injection.

4.4 Maximal Ideals

Definition: Maximal Ideals Let R be a ring with identity $1 \in R$. An ideal M in R is called a maximal ideal if $M \neq R$ and the only ideals containing M are M and R.

Proposition: In a ring with identity 1, every proper ideal is contained in a maximal ideal.

Sketch of proof: Suppose I is a proper ideal. Let S be the set of proper ideals containing I(S is clearly non-empty and has partial order by inclusion). Let C be a chain in S and let J be the union of all ideals in C. Show that J is an ideal - $0 \in J$ and elements are closed under subtraction and left/ring multiplication by elements of R. Then, show that J is a proper ideal since otherwise $1 \in J$

and therefore, 1 *is in at least one of the ideals in* C *making that ideal not proper. Then, each chain has an upper bound in* S*. Use Zorn's lemma to conclude* S *has a maximal element which is our maximal proper ideal containing* I

Proposition: Let R be a commutative ring with identity 1. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Sketch of proof: ideal M *is maximal iff there are no ideals* I *st* $M \subset I \subset R$*. By lattice isomorphism, ideals of* R *containing* M *correspond bijectively with the ideals of* R/M*, so* M *is maximal if and only if the only ideals of* R/M *are 0 and* R/M*. But by a proposition above,* R/M *is a field iff the only ideals are* 0 *and* R/M*.*

4.5 Prime Ideals

Definition: Prime ideal. Suppose R is a commutative ring with identity 1. An ideal P is called a prime ideal if $P \neq R$ and whenever $xy \in P$, we have $x \in P$ and/or $y \in P$.

Proposition: Suppose R is commutative with identity $1 \neq 0$. Then, the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof: P *is a prime ideal if and only if* $\bar{R} \neq \bar{0}$ *(since* $P \neq R$*) and* $\bar{a}\bar{b} = \bar{a}\bar{b} = 0$ *implies either* $\bar{a} = 0$ *or* $\bar{b} = 0$ *which is if and only if* R/P *is an integral domain.*

Proposition: Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: M *is maximal implies* R/M *is a field and a field is an integral domain so* M *must be prime.*

Example: The ideal (x) is a prime ideal in $\mathbb{Z}[x]$ since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

4.6 Rings of Fractions and Fields of Fractions

Let R be a commutative ring. We want to show that R is a subring of a larger ring Q in which every non-zero element of R that is not a zero divisor is a unit in Q.

First, we define the equivalence relation $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. Define addition and multiplication of fractions as is normally done with rational numbers.

Definition: Let R be a commutative ring and let D be a non-empty subset of R such that $0 \notin D$, D contains no zero divisors and D is closed under multiplication. Then, there exists a commutative ring Q, denoted $Q = D^{-1}R$, with $1 \in Q$ such that Q contains R as a subring and every element of

D is a unit in Q. This ring Q has the following properties:
(1) every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$.
(2) If $D = R - \{0\}$, then Q is a field. We call Q the field of fractions or the quotient field of R.
(3) The ring Q is the smallest ring containing R in which all elements of D are units. In other words, let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism s.t. $\varphi(d)$ is a unit in S for all $d \in D$. Then, there is an injective ring homomorphism $\phi : Q \to S$ s.t. $\phi|_R = \varphi$.

4.7 Euclidean Domains and Discrete Valuation Rings

Definition (Norm/Positive Norm). Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm on the integral domain R. If $N(a) > 0$ for all $a \neq 0$, then N is called a positive norm.

Definition (Euclidean Domains). An integral domain R is called a Euclidean Domain (or possess a Division Algorithm) if there exists a norm N on R such that for any two elements $a, b \in R$ with $b \neq 0$, there exists elements $q, r \in R$ s.t.

$$a = bq + r$$

with $r = 0$ or $N(r) < N(b)$. We call q the quotient and r the remainder.

Examples of Euclidean domains:
(1) All fields are trivial examples of Euclidean Domains.
(2) $\mathbb{Z}$ is a Euclidean Domain with $N(a) = |a|$.
(3) If F is a field, then the polynomial ring $F[x]$ is a Euclidean domain with norm $N(p(x)) = deg(p(x))$.

Proposition: Every ideal in a Euclidean domain is a principal ideal. So, Euclidean domains are principal ideal domains.

Proof. If $I = 0$, we are done. Let $d \in I$ s.t. $N(d) \leq N(x)$ for all $x \in I$. Then, $(d) \subseteq I$. Consider any $a \in I$, where $a = qd + r$ (here, $r = 0$ or $N(r) \leq N(d)$). Then, $r = a - qd \in I$. By minimality of norm of d, $r = 0$, so $a = qd \in (d)$. So $I \subseteq (d)$. □

Examples:
(1) Every ideal in $\mathbb{Z}$ is a principal ideal.

Definition (Discrete Valuation): Let K be a field. A discrete valuation on K is a function

$$v : K^\times \to \mathbb{Z}$$

such that (1) $v(ab) = v(a) + v(b)$ (2) v is surjective and (3) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.

Definition (Valuation Ring): The valuation ring of v is

$$\{x \in K^\times | v(x) \geq 0\} \cup \{0\}.$$

Definition(Discrete Valuation Ring). An integral domain R is a discrete valuation ring if there exists a valuation v on its field of fractions such that R is the valuation ring of v.

Note: **A discrete valuation ring is a Euclidean Domain** with the norm $N(0) = 0$ and $N = v$ on non-zero elements.

4.8 Principal Ideal Domains

Definition: Principal Ideal Domain (PID). A PID is an integral domain in which every ideal is principal.

Example: $\mathbb{Z}$ is a PID.

Proposition: Let R be a PID and let $a, b \in R$ such that $a \neq 0$, $b \neq 0$. Let d be a generator for the principal ideal generated by a and b. Then,
(1) d is the greatest common divisor of a and b.
(2) d can be written as an R-linear combination of a and b i.e. there exists $x, y \in R$ such that $d = ax + by$ and
(3) d is unique up to multiplication by a unit of R.

Proposition: Every non-zero prime ideal in a PID is a maximal ideal.

Proof. Let (p) be a prime ideal in a PID. Let $I = (m)$ contain (p). We want to show $I = (p)$ or $I = R$. Since $(p) \subset (m) = I$, $p = rm$ for some $r \in R$. Now, (p) is prime, so either $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(p) = (m) = 1$. If $r \in (p)$, write $r = ps$ so $p = rm = psm$. So $sm = 1$ so m is a unit and $I = R$. □

Corollary: If R is any commutative ring such that the polynomial ring $R[x]$ is a PID or a Euclidean domain, then R is necessarily a field.

Proof. Suppose, $R[x]$ is a PID. Now, R is a subring of $R[x]$, then R must be an integral domain. The ideal (x) is a non-zero prime ideal in $R[x]$ as $R[x]/(x) \cong R$. Then, (x) is a maximal ideal by previous proposition, so R is a field. □

4.9 Irreducible elements and Prime elements

Definition: Irreducible, prime and associate. Let R be an integral domain.
(1) Let $x \in R$ such that x is not a unit. Then x is irreducible in R if $x = ab$ where $a, b \in R$ implies either a or b is a unit in R.
(2) A non-zero element $x \in R$ is called a prime in R if the ideal (x) generated by x is a prime ideal. Equivalently, $x \neq 0$ is a prime if it is not a unit and whenever x divides $ab \in R$, either x divides a or x divides b.
(3) Two elements x and y of R are associate if $x = uy$ for some unit $u \in R$.

Proposition: In an integral domain, a prime element is always irreducible.

Proof. Suppose (p) is a non-zero prime ideal and $p = ab$. Then, $ab \in (p)$ implies either $a \in (p)$ or $b \in (p)$. Assume the former WLOG. Then, $a = pr$ for some $r \in R$. Now, $p = ab = prb$ so $rb = 1$ so b is a unit. Thus, p is irreducible. □

Proposition: prime = irreducible in PID. In a PID, a non-zero element x is a prime if and only if it is irreducible.

Proof. We already know prime implies irreducible, so we show the converse. Suppose M is an ideal containing (p). Then, $M = (m)$ is a principal ideal and since $p \in (m)$, $p = rm$ for some r. Since p is irreducible, either r or m is a unit. So, either $(p) = (m)$ or $(m) = (1)$. Thus, the only ideals containing (p) are (p) or (1). So (p) is a maximal ideal. We know maximal ideals are prime ideals, so p is a prime. □

4.10 Unique Factorization Domain

Definition: Unique factorization domain (UFD) A unique factorization domain is an integral domain R in which every non-zero $x \in R$ which is not a unit has the following properties:
(1) x is a finite product of irreducible p_i (not necessarily distinct) of R; $x = p_1 \cdots p_r$
(2) The decomposition is unique up to associates i.e $x = q_1 \cdots q_m$ is another decomposition, then $m = r$ and after renumpering p_i is associate to q_i for all i.

Example: **A field F is a UFD since every element is a unit.**

Example: **When R is a UFD, R[x] is also a UFD.**

Proposition: prime = irreducible in UFD. In a UFD, a non-zero element x is a prime if and only if it is irreducible.

Proof. Let R be a UFD. We need to show irreducible implies prime. Suppose $p \in R$ is irreducible and suppose $p|ab$ for some $a, b \in R$. Then, $ab = pc$ for some c. Write a and b as their irreducible decomposition. Then p must be associate to some irreducible either in the decomposition of a or b - assume the former WLOG. Then, $a = (up)p_2 \cdots p_n$ where u is a unit. Then, p divides a and so p is a prime. □

Proposition: Let $a, b \in R$ be non-zero and let R be a UFD. Suppose, $a = up_1^{e_1} \cdots p_n^{e_n}$ and $b = vp_1^{f_1} \cdots p_n^{f_n}$ are their prime factorizations for a and b with u, v units. Here the primes p_i are distinct and $e_i, f_i \geq 0$ for all i. Then, $d = p_1^{\min e_1, f_1} \cdots p_n^{\min e_n, f_n}$ is the greatest common divisor of a and b.

Proposition: Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

4.11 Polynomial Rings

Definition (Polynomial Ring). $R[x]$ consists of formal sums $a_n x^n + \cdots + a_1 x + a_0$, where $a_i \in R$ and $n \geq 0$. If $a_n \geq 0$, then the degree of the polynomial is n. A monic polynomial is one where $a_n = 1$.

We already saw the following before:

Proposition 1: Let R be an integral domain. Then:
(a) $deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$ given $p(x), q(x)$ are non-zero.
(b) The units of $R[x]$ are the units of R.
(c) $R[x]$ is an integral domain.

Proposition 2: Quotient of polynomial ring. Let I be an ideal of the ring R. Then, $R[x]/I[x] \cong (R/I)[x]$. In particular, if I is a prime ideal of R, then $I[x]$ is a prime ideal of $R[x]$.

Proof. Consider map $\varphi : R[x] \to (R/I)[x]$ by taking each coefficient mod *I*; this is easily seen to be a ring homomorphism. Then, $ker(\varphi) = I[x]$ proves first part. For the second, since I is prime, R/I is integral domain (by previous proposition) so $(R/I)[x]$ is an integral domain and so $I[x]$ is a prime ideal of $R[x]$. □

Note: It is *not* true that if I is a maximal ideal of R, then $I[x]$ is a maximal ideal of $R[x]$. However, if I is maximal in R, then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

Definition: Polynomial ring of more than one variables. The polynomial ring in the variables $x_1, \cdots, x_n$ with coefficients in R denoted by $R[x_1, \cdots, x_n]$ is defined inductively by $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$.

A polynomial in a polynomial ring of more than one variable is a finite sum of elements of the form $ax_1^{d_1} \cdots x_n^{d_n}$ where $a \in R, d_i \geq 0$ which are called the monomial terms. For a monomial term, if $a = 1$, we call it a monic term. A monomial term of this form is of degree $d = d_1 + \cdots + d_n$ and the n-tuple $(d_1, \cdots, d_n)$ is the multidegree of the term.

If f is a non-zero polynomial in n variables, the sum of all monomial terms in f of degree k is called the homogenous component of f of degree k. If f has degree d, then f may be written uniquely as the sum $f_0 + \cdots + f_d$ where f_k is the homogenous component of f of degree k.

4.12 Polynomial Rings over Fields

Theorem 3: Polynomial rings that are Euclidean Domains. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. If $a(x), b(x)$ are two polynomials in $F[x]$ with $b(x) \neq 0$, then there are unique polynomials $q(x), r(x) \in F[x]$ such that $a(x) = q(x)b(x) + r(x)$ with $r(x) = 0$ or $degree\ \mathrm{r}(x) < degree\ \mathrm{b}(x)$.

Sketch of proof: Use induction. Let $deg(a(x)) = n, deg(b(x)) = m$. If $a(x) = 0$, then $q(x) = r(x) = 0$. If $n < m$, let $q(x) = 0, r(x) = a(x)$. So let $n \geq m$. Construct $q(x)$ - if $a(x) = \sum_{i=0}^{n} a_i x^i, b(x) = \sum_{i=0}^{m} b_i x^i$. Define $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ designed to subtract leading term from $a(x)$. By inductive hypothesis, $a'(x) = q'(x)b(x) + r(x)$. With $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$. To prove uniqueness, assume there is another decomposition with $q_1(x), r_1(x)$ and leverage the fact that degree of $f(x)g(x)$ is the sum of degree $f(x)$ and degree $g(x)$.

Corollary 4: If F is a field, then $F[x]$ is a Principal Ideal Domain (PID) and a Unique Factorization Domain (UFD).

Now we look at polynomial rings that UFDs.

Proposition 5: Gauss's Lemma. Let R be a UFD with a field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some non-constant polynomials $A(x), B(x) \in F[x]$, then there are non-zero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Sketch of proof for R a field: Let $p(x) = A(x)B(x)$ where on RHS, coefficients are in F. Multiply both sides by a common denominator for all coefficients to get $dp(x) = a'(x)b'(x)$ where on RHS we have elements in R[x], $d \neq 0 \in R$. If d is unit, we are done with $a(x) = d^{-1}a'(x)b'(x)$. Check Dummit and Foote for the proof in the case where d is not a unit.

Corollary: Let R be a UFD. Let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic poynomial that is irreducible in

$R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof: By Gauss's Lemma, if $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$. Conversely, suppose the gcd of coefficients of $p(x)$ is 1. If p is reducible with $p(x) = a(x)b(x)$, then neither $a(x)$ nor $b(x)$ are constant polynomials - this factorization also shows $p(x)$ is reducible in $F[x]$.

Theorem: R is a UFD if and only if $R[x]$ is a UFD.

Corollary: If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

4.13 Irreducibility Criteria

Now we look at **irreducible criteria** of polynomials.

We will require the following throughout the AG notes:

Proposition: Let R be a field. The prime ideals of $R[y]$ are the zero ideal (0), the ideals $(f(y))$ where f is irreducible.

Proof: Given R is a field, $R[x]$ is a PID. If (f) is a prime ideal in $R[x]$, then f is prime which means f is irreducible.

Proposition: Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in R i.e there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proof: If $p(x)$ has a factor of degree 1, then since F is a field, we may assume the factor is of the form $(x - a), a \in F$. Then, $p(a) = 0$. Conversely, if $p(a) = 0$, then by division algorithm in $F[x]$ - theorem 3 in this section - $p(x) = q(x)(x - a) + r$ where r is constant and since $p(a) = 0, r = 0$ so $(x - a)$ is a factor.

Proposition: A polynomial of degree two or three over a field F is reducible if and only if has a root in F.

Proposition: Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in its lowest term (i.e r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$ i.e $r|a_0$ and $s|a_n$. In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

The following are very important results:

Proposition: Let I be a proper ideal in the integer domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proof: Suppose p(x) cannot be factored in (R/I)[x] but p(x) is reducible in R[x] so $p(x) = a(x)b(x)$ *where both a(x) and b(x) are monic, nonconstant in R[x]. But then reducing the coefficients modulo I gives a factorization in (R/I)[x] - contradiction.*

Proposition: Einsenstein's Criterion. Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial in $R[x]$ ($n \geq 1$). Suppose $a_{n-1}, a_n, \cdots, a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

Proposition: The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials in $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition: Let $g(x)$ be a nonconstant element of $F[x]$ and let $g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$ be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then, we have the following isomorphism of things:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k})$$

Proposition: I the polynomial $f(x)$ has roots $a_1, ..., a_k \in F$ (not necessarily distinct), then $f(x)$ has $(x - a_1) \cdots (x - a_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in R, even counted with multiplicity.