1 Linear Algebraic Groups.

1.1 The Zariski topology on affine $n$-space.

Let $C$ be an algebraically closed field of characteristic 0. Let $X := (X_1, \ldots, X_n)$ be $n$ indeterminates, and let $A^n := C^n$ be the affine $n$-space. Let $x := (x_1, \ldots, x_n)$ be an element of $A^n$. Let $C[X]$ be the polynomial algebra over $C$.

Since $C$ is infinite, we may identify $C[X]$ with an algebra of functions on $X$.

We define the Zariski topology on $A^n$.

A set $V \subseteq A^n$ is closed (an affine variety) if there exists a finite set $F_1, \ldots, F_r$ of polynomials in $C[X]$ such that

$$V = \{ x \in A^n : F_1(x) = \cdots = F_r(x) = 0 \}.$$ 

$V$ is closed if and only if there exists an ideal $a = (F_1, \ldots, F_r)$ with a finite basis in $C[X]$ such that

$$V = \{ x \in A^n : F(x) = 0 \}\quad \text{for all } F \in a.$$ 

**Theorem 1** (Hilbert Basis Theorem) Every ideal in $C[X]$ has a finite basis.

**Corollary 2** ($C[X]$ is Noetherian) Every ascending sequence of ideals is finite.
$V(a) :=$ the closed set of zeros of the ideal $a$ of $C[X]$.
Let $a$ be an ideal in $C[X]$.

$$V(a) = V(\sqrt{a}).$$

Let $V$ be a subset of $A^n$. Let

$$a = \{ F \in C[X] : F(x) = 0 \quad \forall x \in V \}.$$
a is a radical ideal in $C[X]$.

$I(V) := a$.
$
\overline{V} :=$ the closure of $V$.

Clearly, $I(V) = I(\overline{V})$.
$V$ and $I$ are order reversing.

$$a \subseteq b \implies V(b) \subseteq V(a)$$

$$V \subseteq W \implies I(W) \subseteq I(V)$$

Also,

$$V((1)) = \emptyset$$
$$V((0)) = \mathbb{A}^n$$
$$V(a \cap b) = V(ab) = V(a) \cup V(b)$$
$$V \left( \sum_i a_i \right) = \bigcap_i V(a_i)$$

Since $C$ is algebraically closed, we have a theorem that reduces the Zariski topology to a theory of radical ideals of a Noetherian $C$-algebra.

**Theorem 3 (Hilbert Nullstellensatz)** The mapping

$$a \mapsto V(a)$$

from the set of radical ideals in $C[X]$ to the set of closed sets in $\mathbb{A}^n$, and the mapping

$$V \mapsto I(V)$$

from the set of closed sets in $\mathbb{A}^n$ to the set radical ideals in $C[X]$ are inclusion reversing, bijective, and inverse to each other.

Therefore,

$$I(\emptyset) = (1)$$
$$I(\mathbb{A}^n) = (0)$$
$$I(V \cup W) = I(V) \cap I(W)$$
$$I \left( \bigcap_i V_i \right) = \sum_i I(V_i)$$

A topological space is *Noetherian* if every descending sequence of closed sets is finite.

2
Corollary 4 The topological space \( \mathbb{A}^n \) is Noetherian.

Since every subspace of a Noetherian space is Noetherian, every closed subset of \( \mathbb{A}^n \) is Noetherian.

Example 5 Let \( a = (XY^2 + 2Y^2, X^4 - 2X^2 + 1, 1 - Z(Y - X^2 + 1)) \subseteq C[X, Y, Z] \).

Let \((x, y, z) \in V(a)\). Then, \((x^2 - 1)^2 = 0\). Therefore, \(x = \pm 1\).

So, \(y = 0\). It follows that \(0 = 1\). So, \(V(a) = \emptyset\), and \(a = (1)\).

A topological space is reducible if it is the union of two proper closed subsets. Otherwise, it is irreducible.

Exercise 6 A Hausdorff space is irreducible if and only if it is reduced to a point.

Lemma 7 (Springer, Linear Algebraic Groups) Let \( V \) be a topological space.

1. \( S \subseteq V \) is irreducible if and only its closure is irreducible.

2. Let \( \varphi : V \to W \) be a continuous map to a topological space \( W \). If \( V \) is irreducible, so is its image \( \varphi(V) \).

3. If \( V \) is irreducible, every nonempty open subset of \( V \) is dense in \( V \).

Since a point in a topological space \( V \) is irreducible, every point is contained in a maximal irreducible subspace \( V' \) of \( V \) (Zorn’s Lemma). \( V' \) is called an irreducible component of \( V \). So, \( V \) is the union of its irreducible components. An irreducible component is closed.

Proposition 8 Let \( V \) be a nonempty closed subset of \( \mathbb{A}^n \). \( V \) is irreducible if and only if \( I(V) \) is prime.

Proof. Suppose \( V = U \cup W \), \( U, W \) proper closed subsets of \( V \).

Then, \( U, W \) are closed in \( \mathbb{A}^n \).

\[
I(V) = I(U) \cap I(W)
\]

\[
I(U) \nsubseteq I(W) \quad I(W) \nsubseteq I(U)
\]

Choose \( F \in I(U) \setminus I(W) \), and \( G \in I(W) \setminus I(U) \).

\( FG \in I(V) \). \( F \notin I(V) \) and \( G \notin I(V) \). Thus, \( I(V) \) is not prime.

We leave the converse as an exercise.

Since \((0)\) is a prime ideal in \( C[X] \), it follows that \( \mathbb{A}^n \) is irreducible.

Let \( V = V(X_1, X_2) \). Then,

\[
I(V) = (X_1) \cap (X_2).
\]

\( I(V) \) is not prime. \( V \) is the union of the coordinate axes of \( \mathbb{A}^2 \).

The point 0 in affine 1-space (the affine line) can be defined as the irreducible closed set \( V(X^2) \). The ideal \( a = (X^2) \) is not prime, but its radical \( \sqrt{a} = (X) = I(0) \) is prime.
**Remark 9** The bijective correspondence \( a \mapsto V(a) \) between radical ideals of \( \mathbb{C}[X] \) and closed subsets of \( \mathbb{A}^n \) restricts to a bijective correspondence \( p \mapsto V(p) \) between prime ideals of \( \mathbb{C}[X] \) and irreducible closed subsets of \( \mathbb{A}^n \).

**Example 10** Show that the ideal \( p = (Y - X^2, Z - XY) \) in \( \mathbb{C}[X,Y,Z] \) is prime.

Suppose \( FG \in p \). \( V(p) = \{(t, t^2, t^3) : t \in \mathbb{C}\} \) – the so-called "twisted cubic." Therefore, \( F(t, t^2, t^3)G(t, t^2, t^3) = 0 \) for all \( t \in \mathbb{C} \). Therefore, since polynomials in 1 variable have only a finite number of roots, one of the polynomials vanishes identically in \( t \). Therefore, either \( F(X,Y,Z) \) or \( G(X,Y,Z) \) is in \( p \).

Together, the Hilbert Basis Theorem (the Noetherianity of \( \mathbb{C}[X] \)), and the Hilbert Nullstellensatz (closed sets are determined by radical polynomial ideals) prove that every closed set is a finite union of distinct maximal irreducible closed subsets:

**Corollary 11** Let \( a \) be a proper radical ideal in \( \mathbb{C}[X] \). Then,

\[
a = p_1 \cap \cdots \cap p_r,
\]

where \( p_1, \ldots, p_r \) are the distinct minimal prime ideals containing \( a \).

\( p_1, \ldots, p_r \) are called the prime components of \( a \).

**Corollary 12** Let \( V \) be a non-empty closed set in \( \mathbb{A}^n \). Then,

\[
V = V_1 \cup \cdots \cup V_r,
\]

where \( V_1, \ldots, V_r \) are the distinct maximal irreducible closed subsets of \( V \).

**Exercise 13** Let \( V \) be a closed subset of \( \mathbb{A}^n \).

1. An open subset \( U \) of \( V \) is dense in \( V \) if and only if \( U \cap V_i \neq \emptyset \), \( i = 1, \ldots, m \).
2. The intersection of two dense open subsets of \( V \) is nonempty.

A topological space is connected if it is not the union of two disjoint proper closed subsets. Every irreducible space is connected. Not every connected space is irreducible.

The union of the coordinate axes in \( \mathbb{A}^2 \) is connected, but is reducible, as we just saw.

By Zorn’s Lemma, every point in a topological space \( V \) is contained in a maximal connected subspace \( V' \) of \( V \). \( V' \) is called a connected component of \( V \). \( V \) is the union of its connected components. The following exercise shows that a connected component of \( V \) is closed.

**Exercise 14** 1. The closure of a connected subspace of a topological space is connected.
2. No proper nonempty subset of a connected space can be both open and closed.

3. If \( \varphi : V \to W \) is a continuous map from the connected space \( V \) into the topological space \( W \), then \( \varphi(V) \) is connected.

4. Let \( V \) be a Noetherian topological space. \( V \) is the disjoint union of finitely many connected closed subsets, its connected components. The connected components of \( V \) are both open and closed in \( V \). A connected subset of \( V \) is contained in a connected component of \( V \). If \( \varphi : V \to V \) is a continuous automorphism, \( \varphi \) permutes the connected components of \( V \).

5. A closed subset \( V \) of \( \mathbb{A}^n \) fails to be connected if and only if there exist two ideals \( a, b \) in \( C[X] \) such that \( a + b = C[X] \), and \( a \cap b = I(V) \).

For us, the most important ring associated with a closed set \( V \) is the ring of polynomial functions on \( V \). This ring is called the coordinate ring of \( V \).

\( \text{C} \left[ V \right] = C \left[ X \right] / a \), where \( a = I(V) \).

An element \( a \) in a ring \( R \) is nilpotent, if there is a positive integer \( k \) such that \( a^k = 0 \).

R is reduced if 0 is the only nilpotent element in \( R \). Since \( a \) is a radical ideal, \( C[V] \) is reduced.

Lemma 16 Let \( a \) be a radical ideal in \( C[X] \). There is a bijective mapping

\[ \varphi : V(a) \to \text{Hom}_C(C[V], C) \]

Proof. Write \( C[V] = C[\gamma] \). Let \( x \in V(a) \). Define

\[ \chi_x : C[V] \to C \]
by
\[ \chi_x(f) = f(x). \]

Clearly, \( \chi_x \in \text{Hom}_C(C[V], C) \) Note that \( \chi_x(\gamma) = x \).
Conversely, let \( \chi \in \text{Hom}_C(C[V], C) \). Set
\[ x = \chi(\gamma). \]

Then,
\[ 0 = F(\gamma), \quad F \in \mathfrak{a}. \]

Thus,
\[ 0 = \chi(F(\gamma)) = F(\chi(\gamma)). \]

Therefore,
\[ x = \chi(\gamma) \in V(\mathfrak{a}). \]

Since
\[ \chi(\gamma) = \gamma(x) = x, \]

it follows that
\[ \chi = \chi_x. \]

So, the mapping from \( V(\mathfrak{a}) \) to \( \text{Hom}_C(C[V], C) \) is surjective. It is injective, since
\[ \chi_x = \chi_y \implies x = \chi_x(\gamma) = \chi_y(\gamma) = y. \]

We call \( \chi_x \) the **evaluation homomorphism** \( (\gamma \mapsto x) \) defined by \( x \).

Let \( V \) be a closed subset of \( \mathbb{A}^n \).

A map \( \varphi : V \to W \), \( W \) a closed subset of \( \mathbb{A}^m \) is a **morphism** (of algebraic varieties) if for \( x \in V \),
\[ \varphi(x) = (f_1(x), \ldots, f_m(x)), \quad f_1, \ldots, f_m \in C[V]. \]

\( \varphi \) defines a \( C \)-algebra homomorphism
\[ \varphi^* : C[W] \to C[V], \]

defined by
\[ \varphi^*(g)(x) = g(\varphi(x)). \]

If \( C[V] = C[\gamma], \quad C[W] = C[\varsigma], \)
then
\[ \varphi^*(\varsigma) = (f_1(\gamma), \ldots, f_m(\gamma)) \in C[V]^m. \]

Call \( f_1, \ldots, f_m \) the **coordinate functions** of \( \varphi \).
Lemma 17 A morphism \( \varphi : V \to W \) of affine varieties is continuous.

**Proof.** Let \( T \) be a closed subset of \( W \). Let \( a \) be an ideal in \( C[W] \) such that \( T = V(a) \). Then,

\[
\begin{align*}
x \in \varphi^{-1}(W) & \iff \varphi(x) \in W \\
& \iff f(\varphi(x)) = 0 \ \forall f \in a \\
& \iff \varphi^*(f)(x) = 0 \ \forall f \in a.
\end{align*}
\]

So, \( \varphi^{-1}(W) = V((\varphi^*(a))). \)

If \( T \) is a closed subset of \( \mathbb{A}^p \) and

\[
V \xrightarrow{\varphi} W \xrightarrow{\psi} T,
\]

then

\[
(\psi \circ \varphi)^* = \varphi^* \circ \psi^*.
\]

Therefore, \( \varphi \) is an isomorphism of affine varieties if and only if \( \varphi^* \) is an isomorphism of \( C \)-algebras.

**Exercise 18** Let \( \varphi : V \to W \) be a morphism of affine varieties.

1. If \( V \) is irreducible (resp. connected), then the closure \( \overline{\varphi(V)} \) is irreducible (resp. connected).
2. If \( \varphi \) is an automorphism of \( V \), then \( \varphi \) permutes the irreducible (and connected) components of \( V \).
3. If \( \varphi \) is an automorphism of \( V \), and \( V' \) is a closed subset of \( V \), then \( \varphi(V) \) is a closed subset of \( V \).
4. If \( W = \overline{\varphi(V)} \), then \( \varphi^* \) is injective.
5. If \( \varphi^* \) is surjective, then \( \varphi(V) \) is a closed subset of \( W \).
6. If \( \varphi^* \) is injective, then \( \varphi(V) \) is dense in \( W \).

For proofs of the next theorem and corollary, see Springer, *Linear Algebraic Groups*, Chapter 1.

**Theorem 19** (Chevalley) Let \( B \) be a domain finitely generated over a subring \( A \), and let \( C \) be an algebraically closed field. For every \( b \neq 0 \) in \( B \), there exists \( a \neq 0 \) in \( A \) such that every homomorphism \( \alpha : A \to C \) such that \( \alpha(a) \neq 0 \) extends to a homomorphism \( \beta : B \to C \).

**Corollary 20** (Images of constructible sets are constructible)

Let \( \varphi : V \to W \) be a morphism of affine varieties. Then, \( \varphi(V) \) contains an open dense subset of \( \overline{\varphi(V)} \).
Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine varieties.

The Cartesian product $V \times W = \{(x, y) : x \in V, y \in W\}$ is an affine variety:

Let $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_m)$ be families of indeterminates.

$V \times W \subseteq \mathbb{A}^{n+m}$. If $a = I(V) \subseteq C[X]$, and $b = I(W) \subseteq C[Y]$, then

$I(V \times W) \subseteq C[X, Y]$.

$I(V \times W) = a \cdot C[X, Y] + b \cdot C[X, Y]$, the ideal in $C[X, Y]$ generated by $a \cup b$.

$C[X]$ and $C[Y]$ are linearly disjoint over $C$.

The polynomial algebra $C[X, Y]$ is canonically $C$-isomorphic to $C[T] \otimes_C C[Y]$.

$(C[X] \otimes_C C[Y]) \setminus I(V \times W)$ is canonically $C$-isomorphic to $C[X] \setminus a \otimes_C C[Y] \setminus b = C[V] \otimes_C C[W]$ (Zariski-Samuel, *Commutative Algebra*, I, Theorem 35, p. 184).

So, the coordinate ring of $V \times W$ is $C[V] \otimes_C C[W]$. If $f \in C[V], g \in C[W]$, then, for $(x, y) \in V \times W$, $(f \otimes g)(x, y) = f(x)g(y)$.

Suppose $V$ and $W$ are irreducible. Then, $C[V]$ and $C[W]$ are integral domains. Since $C$ is algebraically closed, $C[V] \otimes_C C[W]$ is an integral domain. Therefore, $V \times W$ is irreducible.

**Example 21**

$$V = V(X_1^2 + X_2^2 - 1) \subseteq \mathbb{A}^2$$

$$W = V(Y_1) \subseteq \mathbb{A}^2$$

$$V \times W = V(X_1^2 + X_2^2 - 1, Y_1) \subseteq \mathbb{A}^4$$

$$C[V] = C[\gamma_1, \gamma_2], \gamma_1^2 + \gamma_2^2 = 1$$

$$C[W] = C[\varsigma_2]$$

$$C[V \times W] = C[\gamma_1, \gamma_2, \varsigma_2], \gamma_1^2 + \gamma_2^2 = 1$$

$$= C[\gamma_1, \gamma_2] \otimes_C C[\varsigma_2].$$

1.2 **The closed subgroups of $GL(n)$.**

The set $M(n)$ of $n \times n$ matrices with entries in $C = \text{affine } n^2$-space.

$c = (c_{ij}) = \text{the point } (a_{11}, \ldots, a_{1n}, \ldots, a_{n1}, \ldots, a_{nn})$.

$$GL(n) = \{c \in M(n) : \det c \neq 0\}.$$
$GL(n)$ is a dense open subset of $M(n)$. Identify it with the closed subset $V$ of $\mathbb{A}^{n^2+1}$ defined by the equation

$$X_{n^2+1}\det X = 1.$$ 

With this identification, the coordinate ring of $GL(n)$ is $C[X, \frac{1}{\det X}]$. $C[X, \frac{1}{\det X}]$ is the localization of $C[X]$ by the multiplicative set $M$ of non-negative powers of $\det X$.

$C[X, \frac{1}{\det X}]$ is an integral domain. $C[X]$ is a subring of $C[X, \frac{1}{\det X}]$. The closed subsets of $GL(n)$ are in bijective correspondence with the radical ideals of $C[X]$ are the defining ideals of closed subsets of $GL(n)$.

**Proposition 22** A radical ideal $a$ is the defining ideal of a closed subset of $GL(n)$ if and only if no prime component of $a$ contains $\det X$.

The proof is in the appendix to this section.

**Example 23** $a = (X_{11}^2 - X_{11}, X_{11} - X_{22}, X_{11} - X_{12}, X_{11} - X_{21})$ is not the defining ideal of a closed subset of $GL(n)$.

$V(a)$ has two components $V_1, V_2$, where $V_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \right\}, a \neq 0$, $V_2 = \left\{ \begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix} \right\}, b, c \in C$. $a = (X_{11}X_{22} - 1, X_{12}, X_{21}) \cap (X_{11}, X_{12})$. The second prime component contains $\det X$.

Let $V$ be a closed subset of $GL(n)$, and let $C[\gamma, \frac{1}{\det \gamma}]$ be its coordinate ring. We have the short exact sequence:

$$0 \rightarrow a \rightarrow C\left[ X, \frac{1}{\det X} \right] \xrightarrow{\phi} C[\gamma, \frac{1}{\det \gamma}] \rightarrow 0,$$

$$\varphi(X) = \gamma, \quad \varphi\left( \frac{1}{\det X} \right) = \frac{1}{\det \gamma}.$$

A subgroup $G$ of $GL(n)$ that is also a closed subset is called a closed subgroup (linear algebraic group). $GL(1)$ is denoted by $\mathbb{G}_m$.

A subgroup $G$ of $\mathbb{G}_m$ is closed if and only if there is a polynomial $F$ in $C[X]$, $X$ an indeterminate, such that $G = V(F)$. $G$ is the finite set of roots of a polynomial in 1 indeterminate.

The proper subgroups of $\mathbb{G}_m$ are finite groups: the groups of $m^{th}$ roots of unity.

Other examples:

1. The special linear group $SL(n) = \{ c \in GL(n) : \det c = 1 \}$. 


2. The upper triangular group $T(n) = \{ c \in GL(n) : c_{ij} = 0, \ i > j \}$.

3. The upper triangular unipotent group $U(n) = \{ c \in T(n) : c_{ii} = 1, i = 1, \ldots, n \}$.

4. The diagonal group $D(n) = \{ c \in GL(n) : c_{ij} = 0, i \neq j \}$.

5. The orthogonal group $O(n) = \{ c \in GL(n) : c^t c = I_n \}$, where $I_n$ is the $n \times n$ identity matrix.

6. The special orthogonal group $SO(n) = O(n) \cap SL(n)$.

7. A closed subgroup of $GL(n)$ is the symplectic group $SP(2n) = \{ c \in GL(2n) : c^t j c = I_{2n} \}$, where

$$j = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$ 

These are some of the so-called classical groups. A more prosaic closed subgroup of $GL(n)$ is

$$G = \{ c \in GL(n) : \exists p \in \mathbb{N} : (\det c)^p = 1 \}.$$

2 Appendix: The defining ideal in $C[X]$ of a closed subset of $GL(n)$.

We want to prove the following proposition:

**Proposition 24** A radical ideal $a$ in $C[X]$ is the defining ideal of a closed subset of $GL(n)$ if and only if no prime component of $a$ contains $\det X$.

An ideal $a$ of $C[X]$ is contracted if there is an ideal $b$ of $C[X, \frac{1}{\det X}]$ with $a = b \cap C[X]$.

If $a$ is an ideal of $C[X]$, $a^e = C[X, \frac{1}{\det X}] \cdot a$ is called the extension of $a$. Let $a$ be an ideal and $G$ be an element of $C[X]$. $G$ is prime to $a$ if for any $F \in C[X]$,

$$FG \in a \implies F \in a.$$ 

Note that $G$ is prime to $a$ if and only if every positive power of $G$ is prime to $a$.

**Lemma 25** $a$ is contracted if and only if $\det X$ is prime to $a$.

**Proof.** If $a = b \cap C[X], b$ an ideal of $C \left[ X, \frac{1}{\det X} \right]$, then

$$\det X \cdot F \in a, \quad F \in C[X] \implies F \in b \cap C[X] = a.$$ 

Suppose $\det X$ is prime to $a$. Let $F \in a^e \cap C[X]$. Then,

$$F = \sum_{j=1}^{p} H_i F_i, \quad H_i \in C \left[ X, \frac{1}{\det X} \right], \quad F_i \in a, \quad i = 1, \ldots, p.$$ 

10
There exists a nonnegative integer $k$ such that $G_i = \det X^k \cdot H_i \in C[X], i = 1, \ldots, p$. Thus,

$$\det X^k F = \sum_{j=1}^{p} G_i F_i \in a.$$ 

It follows that $F \in a$.

$$\det X \prod_{q \neq p} F_q \in a.$$ 

Suppose $\prod_{q \neq p} F_q$ is in $a$. Then, $\prod_{q \neq p} F_q \in p$. Therefore, for some $q \neq p$, $F_q \in p$. Thus, $a$ is not contracted. \[\blacksquare\]

**Proposition 26** (Zariski-Samuel, Commutative Algebra, Vol. I, Theorem 15, p. 223) The maps $b \mapsto b \cap C[X]$ from the set of all ideals in $C[X, \frac{1}{\det X}]$ to the set of contracted ideals in $C[X],$

and

$$a \mapsto a^e = C \left[ X, \frac{1}{\det X} \right] \cdot a$$

from the set of contracted ideals in $C[X]$ to the set of ideals in $C[X, \frac{1}{\det X}]$, are inclusion preserving, bijective and inverse to one another, and preserve the ideal-theoretic operations of forming intersections and radicals.