# 1 Lecture 14-15

## 1.1 Overview of This Lecture

The proof that $I_V$ is generated by $(I_V)_1$ is in the previous lecture note. To make things correct, $\mathbb{F}$ is assumed to be $\mathbb{R}$ or $\mathbb{C}$, which is not the case on the board.

## 1.2 Proof of Things

**Proposition 1.2.1.** *Let $V$ be a $d$-dimensional linear subspace of $\mathbb{F}^n$ and $I_V \in \mathbb{F}[x]$ the set of polynomials vanishing on $V$. Then we have $V = Z(I_V)$, where*

$$Z(I_V) = \{v \in \mathbb{F}^n : f(v) = 0, \forall f \in I_V\}.$$

*Proof.* Suppose $v \in V$, then $f(v) = 0$ for each $f \in I_V$, which means $v \in Z(I_V)$. Hence $V \subset Z(I_V)$.

On the other hand, let $v \in Z(I_V)$. Then we have $f(v) = 0$ for any $f \in I_V$. Specifically, let $u_{d+1}, \ldots, u_n$ be a basis for $V^\perp$, then for the linear forms $f_{u_{d+1}}, \ldots, f_{u_n} \in I_V$, we have

$$f_{u_{d+i}}(v) = u_{d+i}^T v = 0 \text{ for } i = 1, \ldots, n-d,$$

implying that $v \in V$. Hence $Z(I_V) \subset V$. □

**Definition 1.2.2** (addition of ideals)**.** Let $R$ be a ring and $I_1, I_2 \subset R$ be ideals. We define addition operation of ideals as follows:

$$I_1 + I_2 = \{r \in R : r = r_1 + r_2 \text{ for some } r_1 \in I_1, r_2 \in I_2\}.$$

*Remark* 1.2.3. An observation is that $I_1 + I_2$ is an ideal, as you should verify.

**Proposition 1.2.4.** *Let $I_1, I_2$ be ideals of a ring. Then $I_1 \cap I_2$ is an ideal.*

*Proof.* Immediate. □

**Proposition 1.2.5** (p)**.** *Let $I_1, I_2 \subset F[x]$ be ideals. Then $\langle I_1 \cup I_2 \rangle = I_1 + I_2$.*

*Proof.* Immediate. □

**Proposition 1.2.6.** *Let $I_1, I_2 \subset F[x]$ be ideals. Then $Z(I_1 \cup I_2) = Z(\langle I_1 \cup I_2 \rangle) = Z(I_1 + I_2)$.*

*Proof.* Immediate. □

Let $R$ be a ring and $I_1, I_2 \subset R$ be ideals. The set

$$\{r \in R : r = r_1 r_2, \text{ where } r_1 \in I_1, r_2 \in I_2\}$$

is not neccesarily an ideal of $R$. This motivates definition 1.2.7.

**Definition 1.2.7** (product of ideals)**.** Let $R$ be a ring and $I_1, I_2 \subset R$ be ideals. We define product of ideals as follows:

$$I_1 I_2 = \{r \in R : \exists l \in \mathbb{N}^+ \text{ such that } r = \Sigma_{i=1}^{l} r_i^1 r_i^2, \text{ where } r_i^1 \in I_1, r_i^2 \in I_2 \text{ for } i = 1, \ldots, l\}.$$

*Remark* 1.2.8. $I_1 I_2$ is an ideal, as you should verify.

**Proposition 1.2.9.** *Let $I_1, I_2$ be ideals of a ring $R$. Then $I_1 I_2 \subset I_1 \cap I_2$.*

*Proof.* Immediate. □

**Proposition 1.2.10.** *Let $I_1, I_2$ be ideals of the ring $\mathbb{F}[x]$. Then $Z(I_1) \cup Z(I_2) = Z(I_1 I_2)$.*

*Proof.* For each $f \in I_1 I_2$, $f = \Sigma_{i=1}^{s} h_i g_i$ for some $h_1, \ldots, h_s \in I_1, g_1 \ldots, g_s \in I_2$. Then it is easy to see that $f$ vanishes on $Z(I_1) \cup Z(I_2)$. Hence

$$I_1 I_2 \subset I_{Z(I_1) \cup Z(I_2)} \Rightarrow Z(I_1) \cup Z(I_2) \subset Z(I_1 I_2).$$

On the other hand, let $v \in Z(I_1 I_2)$. Suppose for the sake of contradiction that $v \notin Z(I_1) \cup Z(I_2)$, then there exist some $h \in I_1$ and $g \in I_2$ such that $h(v) \neq 0$ and $g(v) \neq 0$, which means that $hg(v) \neq 0$ ($\mathbb{F}$ is an integral domain). But $hg \in I_1 I_2$, contradicting to the fact $v \in Z(I_1 I_2)$. Hence $v \in Z(I_1) \cup Z(I_2)$. □

It can be easily verified that if an element $r$ is in an ideal, then for each $n \in \mathbb{N}^+$ we have that $r^n$ is in the same ideal. Conversely, we define a new set, called the radical of an ideal, as follows.

**Definition 1.2.11** (radical of an ideal)**.** Let $I$ be an ideal of a ring $R$. Then the set

$$\sqrt{I} = \mathrm{rad}(I) = \{r \in R : \exists n \in \mathbb{N}^+ \text{such that } r^n \in I\}$$

is called *the radical of the ideal $I$*.

**Exercise 1.2.12.** Let $I$ be an ideal of a ring and $\sqrt{I}$ the radical of $I$. Show that $I \subset \sqrt{I}$.

**Definition 1.2.13** (Zariski Topology)**.** We define $Y \subset \mathbb{F}^n$ to be a closed set if there is an ideal $I$ of $\mathbb{F}[x]$ such that $Y = Z(I)$. These closed sets form a topology (indeed, this is called *Zariski Topology*).

*Remark* 1.2.14. To show that the closed sets defined in definition 1.2.13 form a topology, we need to show that

1. $\emptyset$ is closed.
2. $\mathbb{F}^n$ is closed.
3. Any union of finitely many closed sets are closed.
4. Any intersection of closed sets are closed.

The terms 1, 2, 3 are easily verified (for the term 3, you need to realize that if $Y_1, Y_2$ are closed, then there exist ideals $I_1, I_2$ such that $Y_1 \cup Y_2 = Z(I_1 I_2)$). To verify the term 4, you may want to check the proof by Ziyu in the piazza.

The definitions of *zero divisor* and *integral domain*, already given in lecture 12 (TA Session), are repeated here for your convenience.

**Definition 1.2.15** (zero divisor)**.** A nonzero element $a$ in a ring $R$ is called a *zero divisor* if there is a nonzero element $b$ in $R$ such that $ab = 0$.

**Definition 1.2.16** (integral domain)**.** A commutative ring $R$ with identity is called an *integral domain* if, for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

**Example 1.2.17** (The product of nonzero elements would be zero)**.**

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

**Example 1.2.18.** $\mathbb{F}[x]$ is an integral domain. then $pq = 0 \Rightarrow p = 0$ or $q = 0$. Also check this page.

**Proposition 1.2.19.** *Let $X_1, X_2 \subset \mathbb{F}^n$. Then $I_{X_1 \cup X_2} = I_{X_1} \cap I_{X_2}$.*

*Proof.* Immediate. □

**Definition 1.2.20** (prime ideal)**.** Let $I$ be an ideal of the ring $R$. $I$ is called *prime ideal* if $ab \in I$ where $a, b \in R$, then $a \in I$ or $b \in I$.

**Example 1.2.21.** The ring $R$ itself is an ideal in $R$ and is prime.

**Example 1.2.22** (p)**.** The set $P = \{0, 2, 4, 6, 8, 10\}$ is an ideal in $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$. This ideal is prime.

**Example 1.2.23** (p)**.** The set $4\mathbb{Z}$ of integers that are multiple of 4, i.e.,

$$4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$

is an ideal in $\mathbb{Z}$. This ideal is not prime. However, $2\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Furthermore, $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ if and only if $p$ is a prime number.

**Theorem 1.2.24.** *Let $V$ be $d$-dimensional linear subspace of $\mathbb{F}^n$. Then $I_V$ is a prime ideal.*

*Proof.* If $V = \mathbb{F}^n$, i.e., $d = n$, then $I_V = I_{\mathbb{F}^n} = \{0\}$, where $0 \in \mathbb{F}[x]$ denotes the zero polynomial in $\mathbb{F}[x]$. For any $g, h \in \mathbb{F}[x]$ such that

$$gh \in I_V \iff gh = 0,$$

we have, by example 1.2.18,

$$g = 0 \text{ or } h = 0 \iff g \in I_V \text{ or } h \in I_V.$$

This means that $I_V$ is a prime ideal.

Now we begin to consider the case that $V$ is a proper subset of $\mathbb{F}^n$, i.e., $d < n$. Let $v_1, v_2, \ldots, v_d \in \mathbb{F}^n$ be an orthonormal basis for $V$ and $u_{d+1}, u_{d+2}, \ldots, u_n \in \mathbb{F}^n$ an orthogonal basis for $V^\perp$, where $V^\perp$ is the orthogonal complement of $V$. Hence $v$'s and $u$'s form an orthonormal basis for $\mathbb{F}^n$, say

$$B = [v_1, v_2, \ldots, v_d, u_{d+1}, u_{d+2}, \ldots, u_n], \tag{1.2.1}$$

and we have $B^T B = I$. Also let $B_V = [v_1, v_2, \ldots, v_d] \in \mathbb{F}^{n \times d}$, $B_{V^\perp} = [u_{d+1}, u_{d+2}, \ldots, u_n] \in \mathbb{F}^{n \times (n-d)}$.

For any $g, h \in \mathbb{F}[x]$ such that $gh \in I_V$, there exist $p, q \in \mathbb{F}[x]$ such that for each $r \in \mathbb{F}^n$, we have $p(B^T r) = g(r), q(B^T r) = h(r)$. Hence

$$\begin{aligned} gh(r) &= g(r)h(r) \\ &= p(B^T r)q(B^T r) \\ &= p(v_1^T r, \ldots, v_d^T r, u_{d+1}^T r, \ldots, u_n^T r)q(v_1^T r, \ldots, v_d^T r, u_{d+1}^T r, \ldots, u_n^T r) \\ &= (p'(v_1^T r, \ldots, v_d^T r) + \Sigma_{i=1}^{n-d}(u_{d+i}^T r)p_i(r))(q'(v_1^T r, \ldots, v_d^T r) + \Sigma_{i=1}^{n-d}(u_{d+i}^T r)q_i(r)), \end{aligned} \tag{1.2.2}$$

where $p', q' \in \mathbb{F}[x_1, x_2, \ldots, x_d]$ and $p_i, q_i \in \mathbb{F}[x]$ for $i = 1, 2, \ldots n - d$. Since $gh$ vanishes on $V$, we have that $p'(v_1^T w, \ldots, v_d^T w)q'(v_1^T w, \ldots, v_d^T w) = 0$ for each $w \in V$.

For any $\alpha \in \mathbb{F}^d$, let $z = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_d v_d \in V$. Then we have

$$\begin{aligned} p'(\alpha)q'(\alpha) &= p'(\alpha_1, \ldots, \alpha_d)q'(\alpha_1, \ldots, \alpha_d) \\ &= p'(v_1^T z, \ldots, v_d^T z)q'(v_1^T z, \ldots, v_d^T z) \\ &= 0. \end{aligned} \tag{1.2.3}$$

This means $p'q' = 0$, and thus by example 1.2.18, we have

$$\begin{aligned} & p' = 0 \text{ or } q' = 0 \\ \Rightarrow & g(r) = \Sigma_{i=1}^{n-d}(u_{d+i}^T r)p_i(r) \text{ or } h(r) = \Sigma_{i=1}^{n-d}(u_{d+i}^T r)q_i(r) \text{ for any } r \in \mathbb{F}^n \\ \Rightarrow & g \in I_V \text{ or } h \in I_V. \end{aligned} \tag{1.2.4}$$

This proves that $I_V$ is a prime ideal. □

**Proposition 1.2.25.** *Let $I_1, I_2$ be ideals in $\mathbb{F}[x]$ and $I_1 \subset I_2$. Then we have $Z(I_2) \subset Z_(I_1)$.*

*Proof.* Immediate. □

We discussed problem 3 in the quiz, its geometry, and its applications in data clustering. Have a look at this paper for further information.

**Theorem 1.2.26.** *Let $X \subset \mathbb{F}^n$ and $I_X \subset \mathbb{F}[x]$ the vanishing ideal on $X$. Then $Z(I_X) = \overline{X}$, where $\overline{X}$ is the closure of $X$.*

*Proof.* Obviously $\overline{X} \subset Z(I_X)$ since $X \subset Z(I_X)$ and $Z(I_X)$ is closed. Let $\overline{X} = Z(J)$, where $J \in \mathbb{F}[x]$ is an ideal. Hence $J \subset I_{\overline{X}}$. Then we have

$$X \subset \overline{X} \Rightarrow J \subset I_{\overline{X}} \subset I_X \Rightarrow Z(I_X) \subset Z(J) \Rightarrow Z(I_X) \subset \overline{X}.$$

□

Review the final picture for a preview of the next week (radical, Hilbert Basis Theorem, Hilbert's Nullstellensatz, etc.)

## 1.3 Further Reading