SI112: Advanced Geometry	Spring 2018
Lecture 12, TA Session — Apr. 9th, Monday	
Prof. Manolis	*Scribe*: Liangzu

1 Lecture 12, TA Session

1.1 Overview of This Lecture

In this TA session we will introduce the definition of *monoid, group, ring*, and *field*. Examples will be given to facilitate your understanding. Notice that the definition of ring given here is slightly different from the one given by Prof. Manolis. What's the difference?

1.2 Proof of Things

Definition 1.2.1 (binary operation)**.** A *binary operation* or *law of composition* on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a * b$, or ab in G, called the composition of a and b.

Definition 1.2.2 (monoid)**.** Suppose that S is a set and $*$ is some binary operation $S \times S \to S$, then $(S, *)$ is a *monoid* if it satisfies the following axioms.

- The binary operation is *associative*. That is,
$$(a * b) * c = a * (b * c)$$
for $a, b, c \in S$.
- There exists an element $e \in S$, called the *identity element*, such that for any element $a \in S$
$$e * a = a * e = a.$$

Example 1.2.3. $(\mathbb{N} \cup \{0\}, +)$ is a monoid.

Example 1.2.4. $(\{f : \mathbb{R}^n \to \mathbb{R}\}, \cdot)$, where $\cdot$ is such that $(f_1 \cdot f_2)(x) = f_1(x)f_2(x)$, is a monoid. What is the identity element of this monoid?

Definition 1.2.5 (group)**.** A *group* $(G, *)$ is a set G together with a law of composition $(a, b) \mapsto a * b$ that satisfies the following axioms.

- The law of composition is *associative*. That is,

$$(a * b) * c = a * (b * c)$$

  for $a, b, c \in G$.

- There exists an element $e \in G$, called the *identity element*, such that for any element $a \in G$

$$e * a = a * e = a.$$

- For each element $a \in G$, there exists an *inverse element* in G, denoted by a^{-1}, such that

$$a * a^{-1} = a^{-1} * a = e.$$

Remark 1.2.6. A group G with the property that $a * b = b * a$ for all $a, b \in G$ is called *abelian* or *commutative*. Groups not satisfying this property are said to be *nonabelian* or *non-commutative*.

Example 1.2.7. $\emptyset$ is not a group.

Example 1.2.8. The integers $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ form a group under the operation of addition.

Example 1.2.9. $(\{f : \mathbb{R}^n \to \mathbb{R}\}, \cdot)$ is a monoid, but no a group. $(\{f : \mathbb{R}^n \to \mathbb{R}/\{0\}\}, \cdot)$ is a group.

Example 1.2.10. The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a group under the binary operation of addition mod n. But if we let modular multiplication be the binary operation on $\mathbb{Z}_n$, then $\mathbb{Z}_n$ fails to be a group. The element 1 acts as a group identity since $1 \cdot k = k \cdot 1 = k$ for any $k \in \mathbb{Z}_n$. However, a multiplicative inverse for 0 does not exist since $0 \cdot k = k \cdot 0 = 0$ for every k in $\mathbb{Z}_n$.

Example 1.2.11. Let $\mathbb{M}_2(\mathbb{R})$ be the set of all 2×2 matrices and $GL_2(\mathbb{R})$ be the subset of $\mathbb{M}_2(\mathbb{R})$ consisting of invertible matrices. Then $\mathbb{M}_2(\mathbb{R})$ with matrix multiplication operation is a monoid, but not a group. $GL_2(\mathbb{R})$ is a nonabelian group (hence a monoid) under matrix multiplication, called the *general linear group*.

Exercise 1.2.12. Prove that the identity element in a group is unique.

Exercise 1.2.13. If g is any element in a group G, then the inverse of g, denoted by g^{-1}, is unique.

Exercise 1.2.14. Let G be a group. Prove that if $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Exercise 1.2.15. Let G be a group. Prove that for any $a \in G$, $(a^{-1})^{-1} = a$.

Exercise 1.2.16 (cancellation laws)**.** If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Definition 1.2.17 (subgroup)**.** Let $(G, *)$ be a group. A subset H of G is called a subgroup of G if H also forms a group under the operation $*$. More precisely, H is a subgroup of G if the restriction of $*$ to $H \times H$ is a group operation on H.

Remark 1.2.18. The subgroup $H = \{e\}$ of a group G is called the *trivial subgroup*. A subgroup that is proper subset of G is called a *proper subgroup*.

Example 1.2.19. The set $\mathbb{Z}a = \{n \in \mathbb{Z} : n = ka \text{ for some } k \text{ in } \mathbb{Z}\} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$ is a subgroup of $(\mathbb{Z}, +)$.

Example 1.2.20. It is important to realize that a subset H of a group G can be a group without being a subgroup of G. For H to be a subgroup of G it must inherit G's binary operation. The set of all 2×2 matrices $\mathbb{M}_2(\mathbb{R})$ forms a group under the operation of addition. The 2×2 general linear group $GL_2(\mathbb{R})$ is a subset of $\mathbb{M}_2(\mathbb{R})$ and is a group under matrix multiplication, but it is not a subgroup of $\mathbb{M}_2(\mathbb{R})$. If we add two invertible matrices, we do not necessarily obtain another invertible matrix. Observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

but the zero matrix is not in $GL_2(\mathbb{R})$.

Proposition 1.2.21 (identifying a subgroup, 1)**.** *A subset H of G is a subgroup if and only if it satisfies the following conditions.*

1. *The identity e of G is in H.*
2. *If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.*
3. *If $h \in H$ then $h^{-1} \in H$.*

Proof. omitted. □

Proposition 1.2.22 (identifying a subgroup, 2)**.** *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

Proof. omitted. □

Definition 1.2.23 (ring)**.** A nonempty set R is a *ring* if it has two closed binary operations, addition and multiplication, satisfying the following conditions.

1. $a + b = b + a$ for $a, b \in R$.

2. $(a + b) + c = a + (b + c)$ for $a, b, c \in R$.

3. There is an element 0 in R such that $a + 0 = a$ for all $a \in R$.

4. For every element $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0$.

5. $(ab)c = a(bc)$ for $a, b, c \in R$.

6. For $a, b, c \in R$,
$$a(b + c) = ab + ac, (a + b)c = ac + bc.$$

Remark 1.2.24. The conditions 1, 2, 3 and 4 in the above definition imply that $(R, +)$ is an abelian group; The last condition is a condition that relates addition operation and multiplication.

Remark 1.2.25. Notice that in the above definition, a ring R may not have multiplicative identity and multiplicative inverse.

If there is an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for each element $a \in R$, we say that R is a ring with *unity* or *identity*. And then the condition 5 means that R with identity is a monoid under multiplication operation.

A ring for which $ab = ba$ for all a, b in R is called a *commutative ring*.

Due to the absence of multiplicative inverses, for some nonzero and distinct elements a, b, c in a commutative ring, the equation $ab = ac \iff a(b - c) = 0$ may not imply $b = c \iff b - c = 0$. That is, the cancellation laws for multiplication operation might not hold. This motivates the following definitions.

Example 1.2.26. The continuous real-valued functions on an interval $[a, b]$ form a commutative ring.

Definition 1.2.27 (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 $b = 0$.

Definition 1.2.28 (unit)**.** A nonzero element a in a ring R with identity is called a *unit* if there exists a unique element a^{-1} such that $a^{-1}a = aa^{-1} = 1$. In other words, the unit is a nonzero element of R that has a unique multiplicative inverse.

Definition 1.2.29 (division ring)**.** A *division ring* is a ring R, with an identity, in which every nonzero element in R is a *unit*. That is, every nonzero element in a division ring has a unique multiplicative inverse.

Remark 1.2.30 (field). A commutative division ring is called a *field*. The relationship among rings, integral domains, division rings, and fields is shown in figure 1.

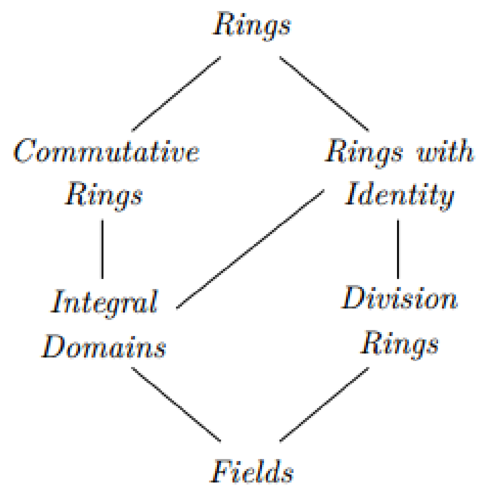

Figure 1: Types of rings

Example 1.2.31. $\mathbb{Z}$ is an integral domain, but not a field. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Example 1.2.32. We can define the product of two elements a and b in $\mathbb{Z}_n$ by $ab \pmod{n}$. For instance, in $\mathbb{Z}_{12}$, $5 \cdot 7 \equiv 11 \pmod{12}$. This product makes the abelian group $\mathbb{Z}_n$ into a ring. Certainly $\mathbb{Z}_n$ is a commutative ring; however, it may fail to be an integral domain. If we consider $3 \cdot 4 \equiv 0 \pmod{12}$ in $\mathbb{Z}_{12}$, it is easy to see that a product of two nonzero elements in the ring can be equal to zero.

Remark 1.2.33 (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 $ab = 0$. In the previous example, 3 and 4 are zero divisors in $\mathbb{Z}_{12}$.

Definition 1.2.34 (nilpotent)**.** An element x of a ring R is called *nilpotent* if there exists some positive integer n such that $x^n = 0$.

Example 1.2.35. The matrix $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ is nilpotent because $A^3 = 0$.

Proposition 1.2.36. *If x is nilpotent in a ring with identity, then $1 - x$ is a unit.*

Proof. That x is nilpotent means that there is a positive integer n such that $x^n = 0$, which implies $(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1 - x^n = 1$. Hence $1 - x$ is a unit. $\square$

1.3 Further Reading

1. wikipedia for their definition.

2. Abstract Algebra: Theory and Applications

3. Abstract Algebra wikibook

SI112: Advanced Geometry	Spring 2018
Lecture 13-14 — Apr. 10th, Tuesday	
Prof. Manolis	*Scribe*: Liangzu

2 Lecture 13-14

2.1 Overview of This Lecture

Here and in what follows, unless explicitly stated otherwise, by *ring* we mean that it is a commutative ring with identity.

Since from now on I have no Mendelson to copy, some results of theorems/definitions, etc. that I am not sure are marked by p, denoting “personal”, “Peng”, or “:p”.

2.2 Proof of Things

Definition 2.2.1 (vector space)**.** This definition might be An abelian group $(V, +)$ and an ”action” of a field F on V, i.e., $F \times V \to V$ $((c, v) \mapsto cv)$.

Definition 2.2.2 (monomial)**.** A *monomial* in $x_1, x_2, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \alpha_2, \ldots, \alpha_n$ are nonnegative integers. The *total degree* of this monomial is the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Remark 2.2.3. Notice that $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$ if and only if $\alpha_i = \beta_i$ for $i = 1, \ldots, n$.

Remark 2.2.4. We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be an n-tuple of nonnegative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

When $\alpha = (0, \cdots, 0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$ denote the total degree of the monomial x^α. Then in what follows, we will use x^α to denote $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, and x to denote $(x_1, x_2, \ldots, x_n)$ unless otherwise specified.

Definition 2.2.5 (support)**.** Suppose that $f : X \to \mathbb{R}$ is a real-valued function whose domain is an arbitrary set X. The *support* of f, written $\operatorname{supp}(f)$, is the set of points in X where f is non zero

$$\operatorname{supp}(f) = \{x \in X : f(x) \neq 0)\}.$$

If $f(x) = 0$ for all but a finite number of points x in X, then f is said to have *finite support*.

Definition 2.2.6 (polynomial over a ring)**.** A *polynomial* f in a ring R is a finite linear combination (with coefficient in R) of monomials. We write a polynomial f in the form

$$f = \Sigma_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha, a_\alpha \in R\,,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. The set of all polynomials in x with coefficients in R is denoted $R[x]$.

Remark 2.2.7. $R[x]$ is a ring (verify it), typically referred as to a *polynomial ring*.

Definition 2.2.8 (polynomial function)**.** Given $p \in R[x]$, we can define a polynomial function $f_p : R^n \to R$ (i.e., $(r_1, \ldots, r_n = r) \mapsto \Sigma_{\alpha \in \mathbb{N}^n} a_\alpha r^\alpha$). The function f_p is also called *evaluation map*.

Remark 2.2.9 (polynomial and polynomial function). We will not distinguish between polynomials and polynomial functions. Read this, and that.

Lemma 2.2.10. *If $f \in \mathbb{F}[x]$ and $f(r) = 0$ for each $r \in \mathbb{F}^n$, then we have $f = 0$. ($\mathbb{F}$ is infinite).*

Proof. Suppose inductively that $n = 1$. Since $f(r) = 0$ for each $r \in \mathbb{F}^n$ and $\mathbb{F}$ is infinite, f is a polynomial that has infinitely many roots. But a nonzero polynomial in $\mathbb{F}$ of degree m has at most m distinct roots. Hence f must be zero polynomial, i.e., $f = 0$.

Now assume that the lemma is true for $n - 1$. Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $f(r) = 0$ for each $r \in \mathbb{F}^n$. By collecting the various powers of x_n, we can write f in the form

$$f(x) = f(x_1, x_2, \ldots, x_n) = \Sigma_{i=0}^{N} g_i(x_1, x_2, \ldots, x_{n-1}) x_n^i,$$

where $g_i \in \mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$.

If we fix $(a_1, a_2, \ldots, a_{n-1}) \in \mathbb{F}^{n-1}$, we get a polynomial $f(a_1, a_2, \ldots, a_{n-1}, x_n) \in \mathbb{F}[x_n]$. By the hypothesis on f, this vanishes for every $a_n \in \mathbb{F}[x_n]$. It follows from the case $n = 1$ that $f(a_1, a_2, \ldots, a_{n-1}, x_n)$ is a zero polynomial in $\mathbb{F}[x_n]$. That is, the coefficients of $f(a_1, a_2, \ldots, a_{n-1}, x_n)$ are zero. Hence $g_i(a_1, a_2, \ldots, a_{n-1}) = 0$ for all i. Since $(a_1, a_2, \ldots, a_{n-1})$ is arbitrarily chosen in $\mathbb{F}^{n-1}$, the inductive assumption then implies that each g_i is the zero polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_{n-1}]$. This forces f to be the zero polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_n]$ and completes the proof of the lemma. $\square$

Example 2.2.11 (p, geometric algebra)**.** Let $f(x_1, x_2) = x_1^2 + x_2^2 - 1 \in \mathbb{R}[x_1, x_2]$ be a polynomial. It is clear that the solution of $f(x_1, x_2) = 0$, when "plotted", is a unit circle on the plane, where the unit circle is merely a set of points in $\mathbb{R}^2$. In this way we can study the property of the solution through geometry. More generally, let $I \subset \mathbb{F}[x]$, where $\mathbb{F}$ is a field, be a set of polynomials. Then we define a set $Z(I)$, called "Zero Set", in the following way.

$$Z(I) = \{v \in \mathbb{F}^n : f(v) = 0, \forall f \in I\}. \tag{2.2.1}$$

It can be seen that $Z(I)$ is merely a set of points in $\mathbb{F}^n$. In this way we can study the zero solution of the polynomials in the set I from $Z(I)$. The connection between I and $Z(I)$ remains to be discussed.

Example 2.2.12 (p, algebraic geometry)**.** **Conversely**, given a set of points $V \subset \mathbb{F}^n$ as a geometric object. Can we study it in an algebraic way, for example, by studying the solution of a specific set of polynomials? Let's start from the simplest example. Now we have a set V containing only one point $(0,0) \in \mathbb{R}^2$ (hence $V \subset \mathbb{R}^2$). Is there any polynomial $f(x_1, x_2) \in \mathbb{R}[x_1, x_2]$ satisfying $f(0,0) = 0$? there are obviously many of them. Indeed, all polynomials whose constant term is 0 satisfy $f(0,0) = 0$. The qualified polynomials will form a set, say $I_{\{(0,0)\}}$. You may want to understand the property of $(0,0)$ by studying $I_V = I_{\{(0,0)\}}$, but I will not. This example is too trivial to be interesting. More generally, let $V \subset \mathbb{F}^n$ be a set of points. Then we define a set I_V as follows:

$$I_V = \{f \in \mathbb{F}[x] : f(v) = 0, \forall v \in V\}. \tag{2.2.2}$$

In this way we can study the geometric object V by study the property of I_V, which is an algebraic object. However, the connection between V and I_V remains to be discussed. The set I_V and the connection between V and I_V might be a recurring theme of this course.

Definition 2.2.13 (ideal)**.** A subset $I \subset R$, where R is a ring, is an ideal if it satisfies

- $0 \in I$.
- If $f, g \in I$, then $f + g \in I$ (i.e., closed under addition).
- If $f \in I$ and $h \in R$, then $hj \in I$.

Exercise 2.2.14. Prove that I_V defined as in (2.2.2) is a ideal. Indeed, I_V is called *vanishing ideal.*

Definition 2.2.15. Let R be a ring and $r_1, r_2, \ldots, r_n \in R$. Then we set

$$\langle r_1, r_2, \ldots, r_n \rangle = \{\Sigma_{i=1}^n h_i r_i : h_1, h_2, \ldots, h_n \in R\}.$$

Exercise 2.2.16 (ideal generated by some elements)**.** A crucial observation is that $\langle r_1, r_2, \ldots, r_n \rangle$ is an ideal of R (prove it). We will call $\langle r_1, r_2, \ldots, r_n \rangle$ is the *ideal generated by* $r_1, r_2, \ldots, r_n$.

Definition 2.2.17 (ideal generated by a subset)**.** An ideal I in a ring R is said to be generated by a subset T of the ring R if for each $\alpha \in I$, there is $s \in \mathbb{N}^+$ such that $\alpha = r_1t_1 + \cdots + r_st_s$ for some $t_1, \ldots, t_s \in T, r_1, \ldots, r_s \in R$.

Definition 2.2.18 (p, linear form)**.** $f_c \in \mathbb{F}[x]$ is called a *linear form with coefficient* $c \in \mathbb{F}^n$ if

$$f_c(x) = c^T x = c_1x_1 + \cdots + c_nx_n$$

for some $c \in \mathbb{F}^n$.

Remark 2.2.19 (p). If $f_c(x) = c^T x$, or f_c, is a linear form and the coefficient c is irrelevant, we use $f(x)$, or f, instead of $f_c(x)$ to the denote linear form $c^T x$ for convenience.

Lemma 2.2.20. $(\mathbb{F}[x])_1$*, the set of linear forms of* $\mathbb{F}[x]$*, is a vector space over* $\mathbb{F}$*.*

Proof. Let $\alpha_1, \alpha_2 \in \mathbb{F}$ and let $f_{c_1}, f_{c_2} \in (\mathbb{F}[x])_1$. Then

$$\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x) = \alpha_1 c_1^T x + \alpha_2 c_2^T x = (\alpha_1 c_1 + \alpha_2 c_2)^T x = f_{\alpha_1 c_1 + \alpha_2 c_2}(x) \in (\mathbb{F}[x])_1.$$

This proves that $(\mathbb{F}[x])_1$ is a vector space. □

Lemma 2.2.21. $c_1, c_2, \ldots, c_s \in \mathbb{F}^n$ *is linearly independent if and only if* $f_{c_1}, f_{c_2}, \ldots, f_{c_s} \in (\mathbb{F}[x])_1$ *is linearly independent.*

Proof. Suppose $f_{c_1}, f_{c_2}, \ldots, f_{c_s}$ is linearly independent, and let $\alpha_1 c_1 + \cdots + \alpha_s c_s = 0$. Then for each $r \in \mathbb{F}^n$,

$$\alpha_1 f_{c_1}(r) + \cdots + \alpha_s f_{c_s}(r) = \alpha_1 c_1^T r + \cdots + \alpha_s c_s^T r = (\alpha_1 c_1 + \cdots + \alpha_s c_s)^T r = 0\,,$$

which implies that $\alpha_i = 0$ for $i = 1, \ldots, s$ and thus that $f_{c_1}, f_{c_2}, \ldots, f_{c_s}$ is linearly independent.

On the other hand, suppose $c_1, c_2, \ldots, c_s$ is linearly independent, and let

$$\alpha_1 f_{c_1}(r) + \cdots + \alpha_s f_{c_s}(r) = \alpha_1 c_1^T r + \cdots + \alpha_s c_s^T r = 0\,,$$

for each $r \in \mathbb{F}^n$. Then we have

$$\alpha_1 f_{c_1}(e_i) + \cdots + \alpha_s f_{c_s}(e_i) = \alpha_1 c_1^T e_i + \cdots + \alpha_s c_s^T e_i = 0, \text{ for } i = 1, \ldots, n\,,$$

where $e_1, e_2, \ldots, e_n$ is the standard basis for $\mathbb{F}^n$. These n equations imply that

$$\alpha_1 c_1 + \cdots + \alpha_s c_s = 0\,.$$

□

Proposition 2.2.22. $(\mathbb{F}[x])_1$ *is a n-dimensional vector space over $\mathbb{F}$.*

Proof. We have proved that $(\mathbb{F}[x])_1$ is a vector space in lemma 2.2.20. It remains to be shown that the dimension of $(\mathbb{F}[x])_1$ is n. It suffices to show that $c_1, c_2, \ldots, c_s \in \mathbb{F}^n$ is linearly independent if and only if $f_{c_1}, f_{c_2}, \ldots, f_{c_s} \in (\mathbb{F}[x])_1$ is linearly independent (why? think about their dimensions), which has been proved in lemma 2.2.21. □

Definition 2.2.23 (p, vanishing at a point)**.** Let $f : X \to Y$ be a function and $x \in X$ be a point. f is said to vanish at the point x if $f(x) = 0$.

Definition 2.2.24 (p, vanishing on a set)**.** Let $f : X \to Y$ be a function and I be a subset of X. f is said to vanish on the set I if f vanishes at every point of the set X, i.e., $f(x) = 0$ for each $x \in X$.

Next, we will establish some simple facts. Proving them requires basis linear algebra, which you are supposed to be familiar with.

Fact 2.2.25 (p)**.** *If $f_1, f_2, \ldots, f_s \in \mathbb{F}[x]$ vanish at a point $x \in \mathbb{F}^n$, then their linear combination*

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_s f_s,$$

where $\alpha_i \in \mathbb{F}$ for $i = 1, 2, \ldots, s$, also vanishes at the point x.

Fact 2.2.26 (p)**.** *If a linear form $f \in (\mathbb{F}[x])_1$ vanishes on a set $S \subset \mathbb{F}^n$, then f also vanishes on the set*

$$span(S) = \{\Sigma_{i\in I} k_i s_i : k_i \in \mathbb{F}, s_i \in S\}.$$

Fact 2.2.27 (p)**.** *If $f_1, f_2, \ldots, f_s \in (\mathbb{F}[x])_1$ vanish on a set $S \subset \mathbb{F}^n$, then their linear combination*

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_s f_s,$$

where $\alpha_i \in \mathbb{F}$ for $i = 1, 2, \ldots, s$, vanishes on the set $span(S) = \{\Sigma_{i\in I} k_i s_i : k_i \in \mathbb{F}, s_i \in S\}$ (and of course S).

Definition 2.2.28. Let V be a d-dimensional linear subspace of $\mathbb{F}^n$. $(I_V)_1$ be the set of linear forms that vanish on V. That is, $(I_V)_1 = \{f \in I_V : f \text{ is a linear form}\}$.

Proposition 2.2.29. $(I_V)_1$ *is a vector space over $\mathbb{F}$.*

Proof. Let $\alpha_1, \alpha_2 \in \mathbb{F}$ and $f_{c_1}, f_{c_2} \in (I_V)_1$. Then $\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x) = f_{\alpha_1 c_1 + \alpha_2 c_2}(x)$. It is obvious that $f_{\alpha_1 c_1 + \alpha_2 c_2}$ is a linear form and $\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x)$ vanishes on V, hence $\alpha_1 f_{c_1}(x) + \alpha_2 f_{c_2}(x) \in (I_V)_1$. □

Remark 2.2.30. Let V be a d-dimensional linear subspace of $\mathbb{F}^n$. We've proved that $(\mathbb{F}[x])_1$ and $(I_V)_1$ is vector space. Hence $(I_V)_1$ is a subspace of $(\mathbb{F}[x]_1)$. It is then natural to ask what is the dimension of the subspace $(I_V)_1$. It turns out that $\dim(I_V)_1 = n - d$, as proved in the following theorem.

Theorem 2.2.31. *Let V be a d-dimensional linear subspace of $\mathbb{F}^n$. Then $(I_V)_1$ is an $\mathbb{F}$-subspace of $(\mathbb{F}[x])_1$ of dimension $n - d$, and I_V is the ideal generated by $(I_V)_1$. Hence, if $f_{b_1}, \dots, f_{b_{n-d}}$ is a basis for $(I_v)_1$ then $I_v = \langle f_{b_1}, \dots, f_{b_{n-d}} \rangle$.*

Proof. It is trivial when $V = \mathbb{F}^n$.

Assume V is a proper subset of $\mathbb{F}^n$. Let $v_1, v_2, \dots, v_d \in \mathbb{F}^n$ be an orthogonal basis for V and $u_{d+1}, u_{d+2}, \dots, u_n \in \mathbb{F}^n$ an orthogonal basis for $V^\perp$, where $V^\perp$ is the orthogonal complement of V. Hence v's and u's form an orthogonal basis for $\mathbb{F}^n$, say

$$B = [v_1, v_2, \dots, v_d, u_{d+1}, u_{d+2}, \dots, u_n]\,, \tag{2.2.3}$$

and we have $B^T B = I$.

We've proved that $(I_V)_1$ is a vector space. Hence $(I_V)_1$ is a subspace of $\mathbb{F}^n$. It remains to be shown that 1. the dimension of $(I_V)_1$ is $n - d$, and that 2. I_V is the ideal generated by $(I_V)_1$.

1. To prove $\dim(I_V)_1 = n - d$, It is enough to do the following: (a) find $n - d$ linearly independent linear forms in $(I_V)_1$, which implies that $\dim(I_V)_1 \geq n - d$; (b) Prove that for arbitrary $n - d + 1$ linear forms in $(I_V)_1$, they are linearly dependent.

   (a) By the definition of orthogonal complement, we have

   $$u_{d+i}^T v_j = 0, \forall i = 1, \dots, n - d, \forall j = 1, \dots, d\,. \tag{2.2.4}$$

   It is obvious from (2.2.4) that the linear forms $f_{u_{d+1}}, f_{u_{d+2}}, \dots, f_{u_n}$ vanish on the set $\{v_1, v_2, \dots, v_d\}$. By the fact 2.2.26, $f_{u_{d+1}}, f_{u_{d+2}}, \dots, f_{u_n}$ vanish on the set $span(\{v_1, v_2, \dots, v_d\}) = V$. Hence we have

   $$f_{u_{d+1}}, f_{u_{d+2}}, \dots, f_{u_n} \in (I_V)_1\,.$$

   In addition, that A is invertible means that $u_{d+1}, u_{d+2}, \dots, u_n$ is linearly independent, which further implies, by lemma 2.2.21, that $f_{u_{d+1}}, f_{u_{d+2}}, \dots, f_{u_n}$ is linearly independent.

   (b) Let $f_{c_d}, f_{c_{d+1}}, \dots, f_{c_n} \in (I_V)_1$, where $c_i \in \mathbb{F}^n$ for $i = d, \dots, n$. Suppose for the sake of contradiction that $f_{c_d}, f_{c_{d+1}}, \dots, f_{c_n}$ is linearly independent. Then by lemma

2.2.21, $c_d, c_{d+1}, \ldots, c_n$ is linearly independent. But $f_{c_d}, f_{c_{d+1}}, \ldots, f_{c_n} \in (I_V)_1$ and thus they vanish on $V = span(\{v_1, v_2, \ldots, v_d\})$, which means that

$$c_d, c_{d+1}, \ldots, c_n \in V^\perp,$$

contradicting the fact that $\dim V^\perp = n - \dim V = n - d$.

2. We know from the proof above that the linear forms $f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n}$ is a basis for $(I_V)_1$. To prove I_V is the ideal generated by $(I_V)_1$, it suffices to show, according to definition 2.2.17, that (a) $\langle f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n} \rangle \subset I_V$ and that (b) for each $p \in I_V$, we have

$$p = b_{d+1} f_{u_{d+1}} + b_{d+2} f_{u_{d+2}} + \cdots + b_n f_{u_n} , \tag{2.2.5}$$

for some $b_{d+1}, b_{d+2}, \ldots b_n \in \mathbb{F}[x]$.

(a) Note that We can not use fact 2.2.25 or fact 2.2.27 to prove it (why?).

Let $f_a \in (I_V)_1$. Hence there exists $p_{d+1}, \ldots, p_n \in \mathbb{F}[x]$ such that

$$f_a = p_{d+1} f_{u_{d+1}} + p_{d+2} f_{u_{d+2}} + \cdots + p_n f_{u_n}.$$

It follows that for any $x \in V$, we have

$$f_a(x) = p_{d+1}(x) f_{u_{d+1}}(x) + p_{d+2}(x) f_{u_{d+2}}(x) + \cdots + p_n(x) f_{u_n}(x) = 0,$$

which means that $f_a \in I_V$. Hence $\langle f_{u_{d+1}}, f_{u_{d+2}}, \ldots, f_{u_n} \rangle \subset I_V$.

(b) Let $p \in I_V$. Then for each $x \in \mathbb{F}^n$, there exists a $q \in \mathbb{F}[x]$ such that $q(B^T x) = p(x)$, where B is defined in (2.2.3) (why such a q exists? there is also a $q_* \in \mathbb{F}[x]$ such that $q^*(Bx) = p(x)$, why do we use q (or B^T) instead of q^* (or B)?). Then

$$p(x) = q(B^T x) = q(v_1^T x, \ldots, v_d^T x, u_{d+1}^T x, \ldots, u_n^T x).$$

As in 2.2.10, we can split $q(v_1^T x, \ldots, v_d^T x, u_{d+1}^T x, \ldots, u_n^T x)$ into two parts, one containing the terms including $u_{d+1}^T x, \ldots, u_n^T x$, which can be represented as

$$\Sigma_{i=1}^{n-d} (u_{d+i}^T x) q_i(x), \text{ where } q_i \in \mathbb{F}[x] \text{ for } i = 1, \ldots, n-d\,,$$

and the other not containing them, which can be represented as

$$q'(v_1^T x, \ldots, v_d^T x)\,.$$

Hence

$$p(x) = \Sigma_{i=1}^{n-d} (u_{d+i}^T x) q_i(x) + q'(v_1^T x, \ldots, v_d^T x)\,,$$

where $q_i \in \mathbb{F}[x]$ for $i = 1, \ldots, n-d$. If suffices to show that $q' = 0$, by which we will have $p = \Sigma_{i=1}^{n-d} q_i f_{u_{d+i}}$ and we can set $b_{d+i} = q_i$ for $i = 1, \ldots, n-d$ to obtain (2.2.5), completing the proof.

We will use the hypothesis $p \in I_V$ to prove $q' = 0$. For each $r \in V$, we have $p(r) = 0$. Since $\Sigma_{i=1}^{n-d} q_i f_{u_{d+i}}$ vanishes on V, $(\Sigma_{i=1}^{n-d} q_i f_{u_{d+i}})(r) = 0$. This implies $q'(v_1^T r, \ldots, v_d^T r) = 0$. Recall that $v_1, v_2, \ldots, v_d$ is a basis for V, there exist unique $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{F}$ such that $r = \Sigma_{i=1}^{d} \alpha_i v_i$. Hence $q'(\alpha_1, \alpha_2, \ldots, \alpha_d) = 0$. This holds for each $r \in V$, but this is not, though close to, what we want.

We desire to prove that for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathbb{F}^d$, $q'(\alpha) = 0$. But for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathbb{F}^d$, there exists a unique $r \in V$ such that $\Sigma_{i=1}^{d} \alpha_i v_i$. $p'(r) = 0$ implying $p'(\alpha) = 0$, by lemma 2.2.10, $p' = 0$. We finished the proof.

□

Remark 2.2.32 (subspaces and ideals). A subspace V of $\mathbb{F}^n$ and its ideal I_V are connected deeply. They both have to be closed under addition and multiplication, except that, for V, we multiply by scalars, whereas for an ideal, we multiply by polynomials. Further, notice that the ideal generated by polynomials $f_1, f_2, \ldots, f_s$ is similar to the span of vectors $v_1, v_2, \ldots, v_s$.

Exercise 2.2.33. Describe the connection between $(I_V)_1$ and orthogonal complement.

Definition 2.2.34 (p, projective variety)**.** $X \subset \mathbb{F}^n$ is called a *projective variety*, if for each $x \in X$, $span(\{x, 0\}) \subset X$.

Remark 2.2.35. Let $X \subset \mathbb{F}^n$ be a projective variety and $I_X \subset \mathbb{F}[x]$ vanish on X. Then for each $x \in X$, $\lambda \in \mathbb{F}$, and $f \in I_X$, we have $f(\lambda x) = f(x) = 0$.

Proposition 2.2.36. $\mathbb{F}[x]$ *is a* $\mathbb{Z}^+$*-graded ring. That is,* $\mathbb{F}[x]$ *can be written as the direct sum of* $(\mathbb{F}[x])_i, i \in \mathbb{N}$, *i.e.,* $\mathbb{F}[x] = \oplus_{i \in \mathbb{N}} (\mathbb{F}[x])_i$, *where* $(\mathbb{F}[x])_i$ *is the set of all homogeneous polynomials of degree* i*, and is a vector space over* $\mathbb{F}$ *of dimension* $\binom{i+n-1}{n-1}$.

Proof. ...... □

Example 2.2.37. The basis of $(\mathbb{F}[x])_2$, where $\mathbb{F}[x] = \mathbb{F}[x_1, x_2, x_3]$, is $x_1^2, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2$. Its dimension is 6.

Question 2.2.38. I_X is an $\mathbb{F}$-subspace of $\mathbb{F}[x]$. Can we write I_X as a direct sum of $(I_X)_i, i \in \mathbb{N}$, i.e., $I_X = \oplus_{i \in \mathbb{N}} (I_X)_i$? (This is true if X is a projective variety).

2.3 Further Reading

1. for review linear algebra, read relevant chapters on this book and that book.
2. formal polynomials: 1, 2.
3. chapter 1 of this book: Ideals, Varieties, and Algorithms, very excellent.
4. not-so-useful notes here