20240902 MATH3301 NOTE 1[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{d}{dx}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

Today, Prof. Law mentioned after class that ideal is an attempt to generalize **Unique Factorization Theorem**.

After checking Wikipedia, I finally understood that:

(1) Ernst Eduard Kummer attempted to prove a weak version of ***Fermat's Last Theorem****, where he invented the concept "ideal number";*[2]

(2) Dirichlet refined the concept "ideal number". Instead of a number, "ideal" is a set, which is similar to the concept "subspace" in Linear Algebra.[2]

(3) While the naive generalization of ***Unique Factorization Theorem*** *fails in certain rings that "contains* $\mathbb{Z}$ *but is not as large as* $\mathbb{C}$*", ideal helps get the correct version of it.*

In light of this, this note will compare several concepts in Linear Algebra and Ring Theory. After that, it will proceed to study the concept of principal ideal and its simple applications in $\mathbb{Z}$.

2 Vector Space and Ring

Both vector space and ring are algebraic structures with two operations: addition and (scalar) multiplication.

Definition 2.1. (**Definition of Vector Space**)
Let V be a set, and $\mathbb{F}$ be a field. If:
1. A binary operation $V \times V \to V, (\mathbf{v}_1, \mathbf{v}_2) \mapsto \mathbf{v}_1 + \mathbf{v}_2$ is defined to be the vector addition on V, satisfying the following 4 axioms:
1.1. Commutative Law of Addition:

$$\forall \mathbf{v}_1, \mathbf{v}_2 \in V, \mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_2 + \mathbf{v}_1$$

1.2. Associative Law of Addition:

$$\forall \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V, (\mathbf{v}_1 + \mathbf{v}_2) + \mathbf{v}_3 = \mathbf{v}_1 + (\mathbf{v}_2 + \mathbf{v}_3)$$

1.3. Identity Element of Vector Addition:

$$\exists \mathbf{0} \in V, \forall \mathbf{v} \in V, \mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v}$$

1.4. Inverse Element of Vector Addition:

$$\forall \mathbf{v} \in V, \exists -\mathbf{v} \in V, (-\mathbf{v}) + \mathbf{v} = \mathbf{v} + (-\mathbf{v}) = \mathbf{0}$$

2. An operation $\mathbb{F} \times V \to V, (\lambda, \mathbf{v}) \mapsto \lambda \cdot \mathbf{v}$ (the symbol "$\cdot$" is usually omitted) is defined to be the scalar multiplication on V, satisfying the following 4 axioms:
2.1. Associative Law of Scalar Multiplication:

$$\forall \lambda_1, \lambda_2 \in \mathbb{F}, \forall \mathbf{v} \in V, (\lambda_1 \lambda_2)\mathbf{v} = \lambda_1(\lambda_2 \mathbf{v})$$

2.2. Identity Element of Scalar Multiplication:

$$\forall \mathbf{v} \in V, 1\mathbf{v} = \mathbf{v}$$

2.3. The Distributive Law of Scalar Multiplication over Field Addition:

$$\forall \lambda_1, \lambda_2 \in \mathbb{F}, \forall \mathbf{v} \in V, (\lambda_1 + \lambda_2)\mathbf{v} = \lambda_1 \mathbf{v} + \lambda_2 \mathbf{v}$$

2.4. The Distributive Law of Scalar Multiplication over Vector Addition:

$$\forall \lambda \in \mathbb{F}, \forall \mathbf{v}_1, \mathbf{v}_2 \in V, \lambda(\mathbf{v}_1 + \mathbf{v}_2) = \lambda \mathbf{v}_1 + \lambda \mathbf{v}_2$$

then $(V, \mathbb{R}, +, \cdot)$ is a vector space over field $\mathbb{F}$.

Definition 2.2. (**Definition of Ring**)
Let R be a set. If:
1. A binary operation $R \times R \to R, (r_1, r_1) \mapsto r_1 + r_2$ is defined to be the addition on R, satisfying the following 4 axioms:
1.1. Commutative Law of Addition:

$$\forall r_1, r_2 \in R, r_1 + r_2 = r_2 + r_1$$

1.2. Associative Law of Addition:

$$\forall r_1, r_2, r_3 \in R, (r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$$

1.3. Identity Element of Addition:

$$\exists 0 \in R, \forall r \in R, 0 + r = r + 0 = r$$

1.4. Inverse Element of Addition:

$$\forall r \in R, \exists - r \in R, (-r) + r = r + (-r) = 0$$

2. An operation $R \times R \to R, (r_1, r_2) \mapsto r_1 \cdot r_2$ (the symbol "$\cdot$" is usually omitted) is defined to be the multiplication on R, satisfying the following 2 axioms:
2.1. Associative Law of Multiplication:

$$\forall r_1, r_2, r_3 \in R, (r_1 r_2) r_3 = r_1 (r_2 r_3)$$

2.2. The Distributive Law of Multiplication over Addition:

$$\forall r_1, r_2, r_3 \in R, (r_1 + r_2) r_3 = r_1 r_3 + r_2 r_3 \text{ and } r_1 (r_2 + r_3) = r_1 r_2 + r_1 r_3$$

then $(R, +, \cdot)$ is a ring.

3 Subspace and Left Ideal

Both subspace and left ideal are smaller structure-preserving sets contained in certain algebraic structures with two operations: addition and (scalar) multiplication.

Definition 3.1. (**Definition of Subspace**)
Let V_1 be a vector space over field $\mathbb{F}$. If:
1. $\mathbf{0} \in V_2 \subseteq V_1$;
2. For all $\mathbf{v}_1, \mathbf{v}_2 \in V_2$, $\mathbf{v}_1 + \mathbf{v}_2 \in V_2$;
3. For all $\lambda \in \mathbb{F}$, for all $\mathbf{v} \in V_2$, $\lambda \mathbf{v} \in V_2$,
then V_2 is a subspace of V_1.

Proposition 3.2. Let V_1 be a vector space over field $\mathbb{F}$.
If V_2 is a subspace of V_1, then V_2 is a vector space over field $\mathbb{F}$.

Proof. We may divide our proof into ten parts.
Part 1: For all $\mathbf{v}_1, \mathbf{v}_2 \in V_2$, if we add them as vectors in V_1, then there exists a unique result $\mathbf{v}_1 + \mathbf{v}_2 \in V_2$, so we define this function as the vector addition.
Part 2: Since vector addition is commutative in V_1, it is commutative in V_2.
Part 3: Since vector addition is associative in V_1, it is associative in V_2
Part 4: There exists $\mathbf{0} \in V_2$, such that for all $\mathbf{v} \in V_2$:

$$\mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v}$$

Part 5: For all $\mathbf{v} \in V_2$, there exists $(-1)\mathbf{v} \in V_2$, such that:

$$(-1)\mathbf{v} + \mathbf{v} = (-1)\mathbf{v} + 1\mathbf{v} = [(-1) + 1]\mathbf{v} = 0\mathbf{v} = \mathbf{0}$$
$$\mathbf{v} + (-1)\mathbf{v} = 1\mathbf{v} + (-1)\mathbf{v} = [1 + (-1)]\mathbf{v} = 0\mathbf{v} = \mathbf{0}$$

Part 6: For all $\lambda \in \mathbb{F}$, for all $\mathbf{v} \in V_2$, if we multiply $\mathbf{v}$ by λ as vector in V_1, then there exists a unique result $\lambda\mathbf{v} \in V_2$, so we define this function as the scalar multiplication.
Part 7: Since the multiplication in $\mathbb{F}$ is associative with the scalar multiplication in V_1, the multiplication in $\mathbb{F}$ is associative with the scalar multiplication in V_2.
Part 8: Since the multiplicative identity element $1 \in \mathbb{F}$ is the multiplicative identity in V_1, it is the multiplicative identity in V_2.
Part 9: Since the scalar multiplication in V_1 distributes over the addition in $\mathbb{F}$, the scalar multiplication in V_2 distributes over the addition in $\mathbb{F}$.
Part 10: Since the scalar multiplication in V_1 distributes over the vector addition in V_1, the scalar multiplication in V_2 distributes over the addition in V_2.
Combine the ten parts above, we've proven that V_2 is a vector space over field $\mathbb{F}$.
Quod. Erat. Demonstrandum. □

Definition 3.3. (**Definition of Left Ideal**)
Let R_1 be a ring. If:
1. $0 \in R_2 \subseteq R_1$;
2. For all $r_1, r_2 \in R_2$, $r_1 + r_2 \in R_2$;
3. For all $\lambda \in R_1$, for all $r \in R_2$, $\lambda r \in R_2$,
then R_2 is a left ideal of R_1.

Proposition 3.4. Let R_1 be a ring.
If R_2 is a left ideal of R_1, then R_2 is a ring.

Proof. We may divide our proof into eight parts.
Part 1: For all $r_1, r_2 \in R_2$, if we add them as elements in R_1, then there exists a unique result $r_1 + r_2 \in R_2$, so we define this function as the addition.

Part 2: Since addition is commutative in R_1, it is commutative in R_2.
Part 3: Since addition is associative in R_1, it is associative in R_2
Part 4: There exists $0 \in R_2$, such that for all $r \in R_2$:

$$0 + r = r + 0 = r$$

Part 5: For all $r \in R_2$, there exists $(-1)r \in R_2$, such that:

$$(-1)r + r = (-1)r + 1r = [(-1) + 1]r = 0r = 0$$
$$r + (-1)r = 1r + (-1)r = [1 + (-1)]r = 0r = 0$$

Part 6: For all $\lambda \in R_1$, for all $r \in R_2$, if we multiply r by λ as element in R_1, then there exists a unique result $\lambda r \in R_2$, so we define this function as the multiplication.
Part 7: Since the multiplication is associative in R_1, it is associative in R_2.
Part 8: Since the multiplication in R_1 distributes over the addition in R_1, the multiplication in R_2 distributes over the addition in R_2.
Combine the ten parts above, we've proven that R_2 is a ring.
Quod. Erat. Demonstrandum. □

4 Set-spanned Space and Set-generated Left Ideal

Both set-spanned space and set-generated ideal are smaller algebraic structures obtained by linear combinations.

Definition 4.1. (**Definition of Set-spanned Subspace**)
Let V be a vector space over field $\mathbb{F}$, and S be a nonempty subset of V.
We define the subspace spanned by S as:

$$\text{span } S = \{\Sigma_{k=1}^{m} \lambda_k \mathbf{v}_k \in V : (\lambda_k)_{k=1}^{m} \text{ in } \mathbb{F} \text{ and } (\mathbf{v}_k)_{k=1}^{m} \text{ in } S\}$$

By convention, we define span $\emptyset = \{\mathbf{0}\}$.

Proposition 4.2. Let V be a vector over field $\mathbb{F}$, and S be a nonempty subset of V. span S is a subspace of V.

Proof. We may divide our proof into three parts.
Part 1: $\mathbf{0} = \Sigma_{k=1}^{1} 0\mathbf{v} \in \text{span } S \subseteq V$, where $\mathbf{v}$ is some vector in the nonempty set S;
Part 2: For all $\mathbf{u}, \mathbf{v} \in \text{span } S$, there exist $(\lambda_k)_{k=1}^{m}, (\mu_l)_{l=1}^{n}$ in $\mathbb{F}$, there exist $(\mathbf{u}_k)_{k=1}^{m}, (\mathbf{v}_l)_{l=1}^{n}$ in S, such that $\mathbf{u} = \Sigma_{k=1}^{m} \lambda_k \mathbf{u}_k$ and $\mathbf{v} = \Sigma_{l=1}^{n} \mu_l \mathbf{v}_l$. If the two lists $(\mathbf{u}_k)_{k=1}^{m}, (\mathbf{v}_l)_{l=1}^{n}$ are distinct, then we rearrange combine them to get two identical grand lists. So we may assume that $(\mathbf{u}_k)_{k=1}^{m} = (\mathbf{v}_l)_{l=1}^{n}$. In this case:

$$\exists (\lambda_l + \mu_l)_{l=1}^{n} \text{ in } \mathbb{F}, \mathbf{u} + \mathbf{v} = \Sigma_{l=1}^{n} \lambda_l \mathbf{v}_l + \Sigma_{l=1}^{n} \mu_l \mathbf{v}_l = \Sigma_{l=1}^{n} (\lambda_l + \mu_l) \mathbf{v}_l$$

So $\mathbf{u}+\mathbf{v} \in \text{span } S$.
Part 3: For all $\lambda \in \mathbb{F}$, for all $\mathbf{v} \in \text{span } S$, there exists $(\mu_k)_{k=1}^m$ in $\mathbb{F}$, there exists $(\mathbf{v}_k)_{k=1}^m$ in S, such that $\mathbf{v} = \Sigma_{k=1}^m \mu_k \mathbf{v}_k$. In this case:

$$\exists (\lambda\mu_k)_{k=1}^m \text{ in } \mathbb{F}, \lambda\mathbf{v} = \Sigma_{k=1}^m (\lambda\mu_k)\mathbf{v}_k$$

So $\lambda\mathbf{v} \in \text{span } S$.
Combine the two parts above, we've proven that span S is a subspace of V.
Quod. Erat. Demonstrandum. □

Definition 4.3. (**Definition of Set-generated Left Ideal**)
Let R be a ring, and S be a subset of R.
We define the left ideal generated by S as:

$$\text{gen } S = \{\Sigma_{k=1}^m \lambda_k r_k \in R : (\lambda_k)_{k=1}^m \in R \text{ and } (r_k)_{k=1}^m \text{ in } S\}$$

Proposition 4.4. Let R be a ring, and S be a nonempty subset of R.
gen S is a left ideal of R.

Proof. We may divide our proof into three parts.
Part 1: $0 = \Sigma_{k=1}^1 0r \in \text{gen } S \subseteq R$, where r is some element in the nonempty set S;
Part 2: For all $r, s \in \text{gen } S$, there exist $(\lambda_k)_{k=1}^m, (\mu_l)_{l=1}^n$ in R, there exist $(r_k)_{k=1}^m, (s_l)_{l=1}^n$ in S, such that $r = \Sigma_{k=1}^m \lambda_k r_k$ and $s = \Sigma_{l=1}^n \mu_l s_l$. If the two lists $(r_k)_{k=1}^m, (s_l)_{l=1}^n$ are distinct, then we rearrange combine them to get two identical grand lists. So we may assume that $(r_k)_{k=1}^m = (s_l)_{l=1}^n$. In this case:

$$\exists (\lambda_k + \mu_k)_{k=1}^m \text{ in } R, r+s = \Sigma_{k=1}^m \lambda_k r_k + \Sigma_{k=1}^m \mu_k s_k = \Sigma_{k=1}^m (\lambda_k + \mu_k) r_k$$

So $r+s \in \text{gen } S$.
Part 3: For all $\lambda \in R$, for all $r \in \text{gen } S$, there exists $(\mu_k)_{k=1}^m$ in R, there exists $(r_k)_{k=1}^m$ in S, such that $r = \Sigma_{k=1}^m \mu_k r_k$. In this case:

$$\exists (\lambda\mu_k)_{k=1}^m \text{ in } R, \lambda r = \Sigma_{k=1}^m (\lambda\mu_k) r_k$$

So $\lambda r \in \text{gen } S$.
Combine the two parts above, we've proven that gen S is a left ideal of V.
Quod. Erat. Demonstrandum. □

5 Principal Left Ideal

We want to generate left ideal by fewer elements.

Definition 5.1. (**Definition of Principal Left Ideal**)
Let R be a ring, and r be an element of R. If a left ideal J of R is generated by $\{r\}$, then J is a principal ideal with generator r.

As a consequence of **Euclid Algorithm**, we can simplify the left ideals of $\mathbb{Z}$

Proposition 5.2. Every left ideal J of $\mathbb{Z}$ is principal.

Proof. We may divide our proof into two cases.
Case 1: In this case, $J = \{0\}$.
This left ideal is generated by $\{0\}$, so it is principal with generator 0.
Case 2: In this case, $J \neq \{0\}$.
We further divide this case into three steps.
Step 1: In this step, we construct $J_{>0} = \{b' \in J : b' > 0\}$ and find its minimum.
Any nonzero left ideal J contains at least one nonzero element b'. If $b' \in J$ happens to be negative, then we multiply $-1 \in R$ to make it positive, so $J_{>0}$ is nonempty. In addition, $J_{>0}$ has lower bound 0. According to **Well-ordering Principle**, $J_{>0}$ a unique minimum b.
Step 2: In this step, we prove that gen $\{b\} \subseteq J$.
For all $a \in$ gen $\{b\}$, there exists $q \in \mathbb{Z}$, such that $a = qb$, which implies $a \in J$.
Step 3: In this step, we prove that $J \subseteq$ gen $\{b\}$.
Assume to the contrary that some $a \in J$ is not an element of gen $\{b\}$, according to **Euclid's Algorithm**, there exists a unique pair of integers (q, r) with $0 < r < q$, such that $a = qb + r$. This implies $r = a + (-q)b \in J$, which is a contradiction as b should be the minimum positive integer in J. Hence, J is principal with generator b.
The three steps above show that J has is principal with generator b in this case.
Combine the two cases above, we've proven the statement.
Quod. Erat. Demonstrandum. □

Interestingly, this simplification characterizes greatest common divisor.

Definition 5.3. (**Definition of Divisible Relation and Common Divisor**)
Let a, b be integers.
If there exists integer q, such that $a = qb$, then b divides a;
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer.
If b divides all integer in A, then b is a common divisor of A.

Definition 5.4. (**Definition of Greatest Common Divisor**)
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer. If:
1. b is a common divisor of A;
2. All common divisor b' of A divides b,
then b is a greatest common divisor of A.

Proposition 5.5. Let A be a nonempty subset of $\mathbb{Z}$. For all integer b, b is a generator of gen A if and only if it is a greatest common divisor of A.

Proof. We may divide our proof into two directions.
"only if" direction: Assume that b is a generator of gen A.
We may further divide this direction into two steps.
Step 1: In this step, we prove that b is a common divisor of A.
For all $a \in A$, $a = \Sigma_{k=1}^{1} 1a \in \text{gen } A = \text{gen } \{b\}$, so there exists $q \in \mathbb{Z}$, such that $a = qb$, which implies b divides a and the whole set A. Hence, b is a common divisor of A.
Step 2: In this step, we prove that any common divisor b' of A divides b.
Since $b \in \text{gen } \{b\} = \text{gen } A$, there exists $(\lambda_k)_{k=1}^{m}$ in R, there exists $(a_k)_{k=1}^{m}$ in A, such that $b = \Sigma_{k=1}^{m} \lambda_k a_k$. Each a_k is divisible by b', so $a_k = q_k b'$ for some integer q_k. This implies $b = (\Sigma_{k=1}^{m} \lambda_k q_k) b'$, so b' divides b.
The two steps above show that b is a greatest common divisor of A.
Combine the two directions together, we've proven the statement.
"if" direction: Assume that b is a greatest common divisor of A.
According to **Proposition 5.2.**, gen A always has a generator, namely, b'.
According to **"only if" direction**, b' is also a greatest common divisor of A.
Since both b and b' are greatest common divisors of A, they differ by a factor ± 1. Since b' is a generator of A, $b = \pm b'$ is also a generator of A.
Combine the two directions above, we've proven the biconditional.
Quod. Erat. Demonstrandum. □

References

[1] H. Ren, "Template for math notes," 2021.

[2] Wikipedia contributors, "Ideal (ring theory) — Wikipedia, the free encyclopedia," 2024, [Online; accessed 2-September-2024]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Ideal_(ring_theory)&oldid=1243068127