Linear Algebra to Abstract Algebra

Ji, Yong-hyeon

March 19, 2025

We cover the following topics in this note.

- Subspace; Span
- Subgroup
- TBA

Note (span). Let V be a vector space over a field $\mathbb{F}$, and let $S \subseteq V$. Recall that, for $n \in \mathbb{N}$,

$$\begin{aligned}\operatorname{span}(S) :&= \{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_n\mathbf{v}_n \mid \lambda_i \in \mathbb{F},\ \mathbf{v}_i \in S \text{ for all } i = 1,2,\ldots,n\} \\ &= \left\{ \sum_{i=1}^{n} \lambda_i\mathbf{v}_i \,\middle|\, \lambda_i \in \mathbb{F},\ \mathbf{v}_i \in S \text{ for all } 1 \le i \le n \right\}.\end{aligned}$$

(Vector) Subspace

Definition. Let V be a vector space over a field $\mathbb{F}$, and let $U \subseteq V$. We write $\boxed{U \le V}$ if V is a **(vector) subspace** of V. That is, $U \le V$ if and only if U satisfy the following conditions:

(i) $\mathbf{0}_V \in U$;

(ii) $\forall \mathbf{u}, \tilde{\mathbf{u}} \in U,\ \mathbf{u} + \tilde{\mathbf{u}} \in U$;

(iii) $\forall \mathbf{u} \in U,\ \forall \lambda \in \mathbb{F},\ \lambda\mathbf{u} \in U$.

Remark. If $S \subseteq V$, then $\operatorname{span}(S) \le V$.

Proof. We must verify that $\operatorname{span}(S)$ satisfies the three defining properties of a subspace of V:

(i) If $S = \varnothing$, by convention we define $\operatorname{span}(\varnothing) := \{\mathbf{0}_V\}$. Let $S \neq \varnothing$. Choose any $\mathbf{v} \in S (\subseteq V)$ and take $n = 1$ with the scalar $\lambda_1 = 0 \in \mathbb{F}$. Then $\mathbf{0}_V = 0 \cdot \mathbf{v} \in \operatorname{span}(S)$.

(ii) Let $\mathbf{u}, \tilde{\mathbf{u}} \in \operatorname{span}(S)$, say,

$$\mathbf{u} = \sum_{i=1}^{n} \lambda_i\mathbf{v}_i \quad \text{and} \quad \tilde{\mathbf{u}} = \sum_{j=1}^{m} \mu_j\tilde{\mathbf{v}}_j,$$

where $n, m \in \mathbb{N}$, $\lambda_i, \mu_j \in \mathbb{F}$, and $\mathbf{v}_i, \tilde{\mathbf{v}}_j \in S$ for all indices i, j. Then

$$\mathbf{u} + \tilde{\mathbf{u}} = \sum_{i=1}^{n} \lambda_i\mathbf{v}_i + \sum_{j=1}^{m} \mu_j\tilde{\mathbf{v}}_j = \overbrace{\underbrace{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_n\mathbf{v}_n}_{n \text{ terms}} + \underbrace{\mu_1\tilde{\mathbf{v}}_1 + \mu_2\tilde{\mathbf{v}}_2 + \cdots + \mu_m\tilde{\mathbf{v}}_m}_{m \text{ terms}}}^{n+m \text{ terms}} \in \operatorname{span}(S).$$

(iii) Let $\alpha \in \mathbb{F}$. Let $\mathbf{u} \in \operatorname{span}(S)$, say, $\mathbf{u} = \sum_{i=1}^{n} \lambda_i\mathbf{v}_i$, where $n \in \mathbb{N}$, $\lambda_i, \in \mathbb{F}$, and $\mathbf{v}_i \in S$ for each $1 \le i \le n$. Then

$$\alpha\mathbf{u} = \alpha\left(\sum_{i=1}^{n} \lambda_i\mathbf{v}_i\right) = \sum_{i=1}^{n} (\alpha\lambda_i)\mathbf{v}_i \in \operatorname{span}(S).$$

since $\alpha\lambda_i \in \mathbb{F}$ for all $i = 1, 2, \ldots, n$.

$\square$

Proposition. *Let V be a vector space over a field $\mathbb{F}$, and let $S \subseteq V$. Then*

(1) $S \subseteq \operatorname{span}(S) \subseteq V$.

(2) If $U \leq V$ is any subspace of V such that $S \subseteq U$, then $\operatorname{span}(S) \subseteq U$.

Proof.

(1) Let $\mathbf{s} \in S$. Then, choosing $n = 1$ and $\lambda_1 = 1 \in \mathbb{F}$, we have $\mathbf{s} = 1 \cdot \mathbf{s} \in \operatorname{span}(S)$. Each element $\mathbf{s} \in \operatorname{span}(S)$ is of the form

$$\mathbf{s} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i,$$

where $\mathbf{v}_i \in S \subseteq V$ and $\lambda_i \in \mathbb{F}$. Since V is a vector space and is closed under finite linear combinations, it follows that $\mathbf{s} \in V$.

(2) Let $U \leq V$ and $S \subseteq U$. Let $\mathbf{s} \in \operatorname{span}(S)$. Then, there exist $n \in \mathbb{N}$, scalars $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{F}$, and vectors $\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_n \in S \subseteq V$ such that

$$\mathbf{s} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \in \operatorname{span}(S).$$

Since

- $S \subseteq U$, i.e., $\mathbf{v}_i \in S \subseteq U$ for each $i = 1, 2, \ldots, n$, and
- $U \leq V$, i.e., $\mathbf{u} + \tilde{\mathbf{u}} \in U$ and $\alpha \mathbf{u} \in U$ for any $\mathbf{u}, \tilde{\mathbf{u}} \in U,\ \alpha \in \mathbb{F}$,

it follows that

$$\forall i \in \{1, 2, \ldots, n\},\ \lambda_i \mathbf{v}_i \in U \quad \text{and} \quad \mathbf{s} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \in U.$$

$\square$

Proposition. *Let V be a vector space over a field $\mathbb{F}$, and let $S \subseteq V$. Let $\mathcal{U} := \{U \leq V : S \subseteq U\}$. Then*

$$\operatorname{span}(S) = \bigcap_{U \in \mathcal{U}} U.$$

In other words, $\operatorname{span}(S)$ *is the smallest subspace of V containing S.*

Proof. We want to show that $\operatorname{span}(S) = \bigcap_{U \in \mathcal{U}} U$.

($\subseteq$) Let $\mathbf{u} \in \operatorname{span}(S)$. By definition, there exists $n \in \mathbb{N}$, scalars $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{F}$, and vectors $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in S$ such that

$$\mathbf{u} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i.$$

Let $U \in \mathcal{U}$ be arbitrary. Since $S \subseteq U$ and $U \leq V$, it is closed under finite linear combinations:

$$\sum_{i=1}^{n} \lambda_i \mathbf{v}_i \in U.$$

Since $\forall U \in \mathcal{U},\ \mathbf{u} \in U \Leftrightarrow \mathbf{u} \in \bigcap_{U \in \mathcal{U}} U$, we obtain

$$\mathbf{u} = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \in \bigcap_{U \in \mathcal{U}} U.$$

($\supseteq$) Since $S \subseteq \operatorname{span}(S)$ and $\operatorname{span}(S) \leq V$, we know $\operatorname{span}(S) \in \mathcal{U}$. Let $\mathbf{u} \in \bigcap_{U \in \mathcal{U}} U$. Then

$$\mathbf{u} \in \bigcap_{U \in \mathcal{U}} U \iff \forall U \in \mathcal{U},\ \mathbf{u} \in U \implies \mathbf{u} \in \operatorname{span}(S).$$

Hence, we conclude that $\operatorname{span}(S) = \bigcap_{U \in \mathcal{U}} U$. $\square$

Subgroup

Definition. Let G be a group. Let $H \subseteq G$. We say that H is a **subgroup** of G, denoted by $H \leq G$, if and only if H is itself a group (with the operation inherited from G).

Example.

- $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
- $(\mathbb{Q}^{\times}, \times) \leq (\mathbb{R}^{\times}, \times)$.

Subgroup Test

Proposition. *Let G be a group, and let $H \subseteq G$ with $H \neq \varnothing$.*

(1) (2-step Test)

$$H \leq G \iff \left(x, y \in H \implies xy \in H,\ x^{-1} \in H\right)$$

(2) (1-step Test)

$$H \leq G \iff \left(x, y \in H \implies xy^{-1} \in H\right)$$

Proof. We want to show that

$$\underbrace{H \leq G}_{\text{(a)}} \iff \underbrace{\left(x, y \in H \implies xy \in H,\ x^{-1} \in H\right)}_{\text{(b)}} \iff \underbrace{\left(x, y \in H \implies xy^{-1} \in H\right)}_{\text{(c)}}$$

((a) $\Rightarrow$ (b)) Let $H \leq G$. Let $x, y \in H$. Since every subgroup is closed under the group operation and taking inverses, we have

$$xy \in H \quad \text{and} \quad x^{-1} \in H.$$

((b) $\Rightarrow$ (c)) Let $x, y \in H$. Suppose that $xy \in H$ and $x^{-1} \in H$. Clearly, $xy^{-1} \in H$.

((c) $\Rightarrow$ (a)) Let $x, y \in H$. Suppose that

$$xy^{-1} \in H.$$

Since $H \neq \varnothing$, $\exists a \in H$, and so

$$aa^{-1} \in H \implies e \in H.$$

Since $x \in H$ and $e \in H$, we have

$$ex^{-1} \in H \implies x^{-1} \in H.$$

Then, since $x, y \in H$ and $y^{-1} \in H$, we obtain

$$x(y^{-1})^{-1} \in H \implies xy \in H,$$

i.e., H is closed under binary operation on G.

□

Subgroup Generated by S

Definition. Let G be a group, and let $S \subseteq G$. The **subgroup of G generated by S**, denoted by $\langle S \rangle$, is defined as:

$$\langle S \rangle := \bigcap \{H \leq G : S \subseteq H\} = \bigcap_{S \subseteq H \leq G} H.$$

Exercise. Let G be a group, and let $S \subseteq G$. Show that $\langle S \rangle$ is the unique smallest subgroup of G containing S.

Sol. TBA $\square$

Exercise. Let G be a group, and let $S \subseteq G$. Let $H_i \leq G$ for each $i \in I$. Show that

$$\bigcap_{i \in I} H_i \leq G.$$

Sol. TBA $\square$

Proposition. *Let* $(G, +)$ *be an abelian group with identity* 0_G*, and let* $x, y \in G$*. Then*

(1) $\langle x \rangle = \{nx : n \in \mathbb{Z}\}$

(2) $\langle x, y \rangle = \left\{nx + my : n, m \in \mathbb{Z}\right\}$

Proof. TBA $\square$

References

[1] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 18. 선형대수학에서 추상대수학으로 (a) 선형결합의 추상화" YouTube Video, 24:25. Published October 15, 2019. URL: https://www.youtube.com/watch?v=zg63xXZYNM8&t=598s.

[2] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 19. 선형대수학에서 추상대수학으로 (b) 대수적 구조를 보존하는 함수 algebraic homomorphisms" YouTube Video, 25:21. Published October 16, 2019. URL: https://www.youtube.com/watch?v=9TtGaY5C0lg&t=187s.