↳ Subalgebraic system

- **Definition 9.10:** Let V=<S, f_1, f_2, … , f_k> be an algebraic system, and let B be a non-empty subset of S. If B is closed under all operations f_1, f_2, … , f_k, B and S share the same algebraic constants, then <B, f_1, f_2, … , f_k> is called a ***sub-algebraic system*** (or simply, a **subalgebra**) of V. Sometimes, the sub-algebraic system is simply denoted by B.
- **Example:**
  - < N,+> is a subalgebra of <Z,+>.
  - < N,+ ,0 > is also a subalgebra of <Z,+,0> (because N is closed under + and has the same algebraic constants).

- **Example:**
  - $<N-\{0\},+>$ is a subalgebra of $<Z,+>$, but not a subalgebra of $<Z,+,0>$ (because the algebraic constant **0** is not included in $N-\{0\}$).

- **Notes:**

① A subalgebra and its original algebra are the ***same type of algebraic system*** (they share the same algebraic constants, the same number of operations, and the same operational properties).

② Every algebraic system V always has ***at least one subalgebraic system***.

↳ Trivial subalgebra and proper subalgebra

- The ***largest subalgebra*** is simply V itself.
- The ***smallest subalgebra*** is the set B formed by all the algebraic constants in V, provided that B is closed under all operations in V, in this case, B constitutes the smallest subalgebra of V.
- The ***trivial subalgebras*** refer to the largest and smallest subalgebras of V.
- A ***proper subalgebra*** refers to a subalgebra B where **B** is a proper subset of S, that is, B forms a proper subalgebra of V.
- **Example:** Let $V=<Z,+,0>$, and define $nZ = \{ nz \mid z \in Z\}$, n is a natural number, then nZ is a subalgebra of V, when n = **1 or 0**, nZ is a trivial subalgebra of V, for all other n, nZ is a nontrivial proper subalgebra of V.

- **Definition 9.11:** Let $V_1=<S_1,\circ>$ and $V_2=<S_2,*>$ be algebraic systems, $\circ$ and $*$ are binary operations. The ***product algebra*** $V_1 \times V_2$ is an algebraic system with a binary operation, defined as $V_1 \times V_2 =<S, \bullet>$, where $S = S_1 \times S_2$, and for all $\forall <x_1, y_1>, <x_2, y_2> \in S_1 \times S_2$, we have $<x_1, y_1> \bullet <x_2, y_2> = <x_1 \circ x_2, y_1 * y_2>$.
- **Example:** Consider integer addition $V_1=<Z,+>$ and matrix multiplication $V_2=<M_2(R), \cdot >$,
  then $V_1 \times V_2 = < Z \times M_2(R), \circ>$,
  and for all $\forall <z_1,M_1>, <z_2,M_2> \in Z \times M_2(R)$,
  we have $<z_1,M_1> \circ <z_2,M_2> = <z_1+z_2, M_1 \cdot M_2>$.

For example: $< 5,\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}> \circ < -2,\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}> = < 3,\begin{pmatrix} 2 & -1 \\ 2 & 0 \end{pmatrix}>$

↳ The properties of product algebras

- Let $V_1=<S_1,\circ>$ and $V_2=<S_2,*>$ be algebraic systems, where $\circ$ and $*$ are binary operations. The product algebra is $V=<S_1\times S_2, \bullet>$.

(1) If $\circ$ and $*$ are **commutative**, then the operation $\bullet$ is also ***commutative***.

(2) If $\circ$ and $*$ are **associative**, then the operation $\bullet$ is also ***associative***.

(3) If $\circ$ and $*$ are **idempotent**, then the operation $\bullet$ is also ***idempotent***.

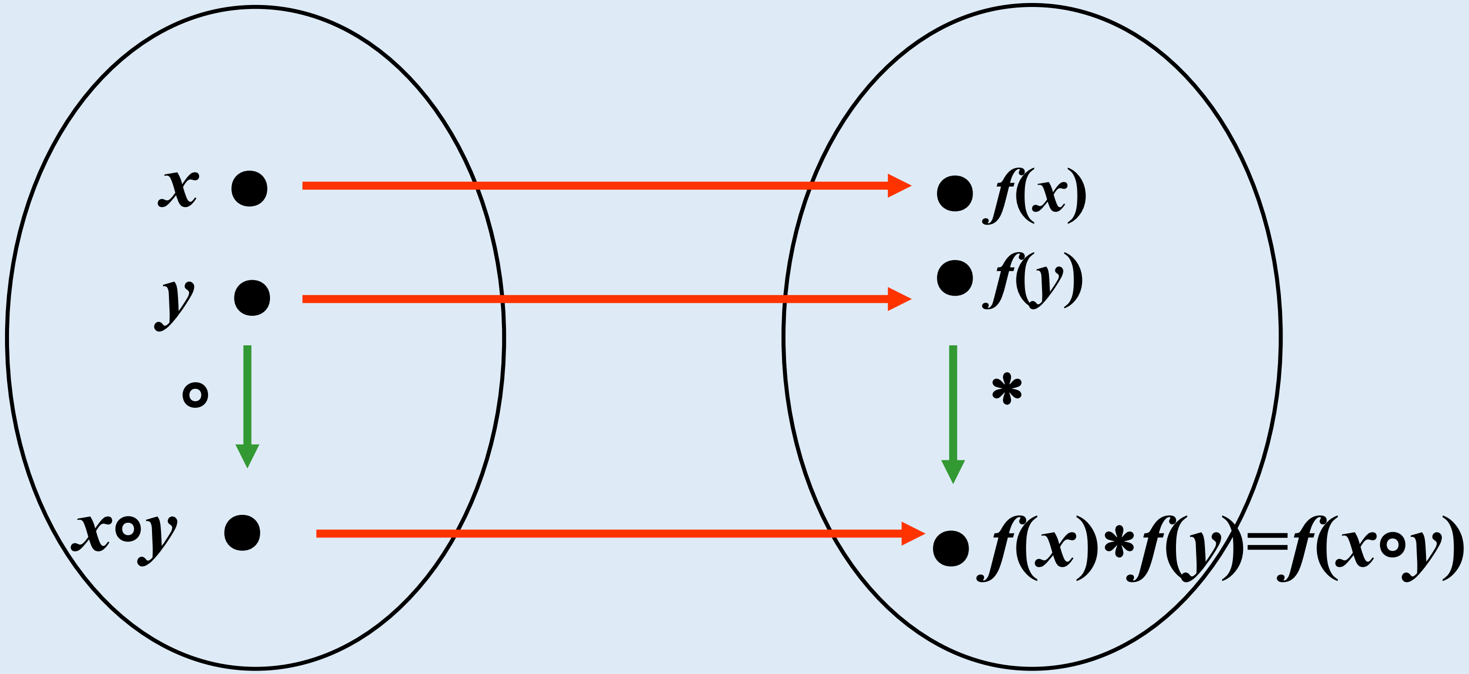
(4) If $\circ$ and $*$ have respective **identity elements** e_1 and e_2 then the operation $\bullet$ also has an ***identity elements*** $<e_1,e_2>$.

(5) If $\circ$ and $*$ have respective **zero elements** θ_1 and θ_2, then the operation $\bullet$ also has a ***zero element*** $<\theta_1, \theta_2>$.

(6) If x has an **inverse** x^{-1}, with respect to $\circ$, and y has an **inverse** y^{-1} with respect to $*$,then $\langle x,y\rangle$ has an ***inverse*** $<x^{-1},y^{-1}>$ with respect to $\bullet$.

- Definition of Homomorphism
- Classification of Homomorphisms
  - Monomorphism, Epimorphism, Isomorphism
  - Endomorphism
- Examples of Homomorphisms
- Properties of Epimorphism

- **Definition 9.12:** Let V_1=<S_1,∘ > and V_2=<S_2,∗> be algebraic systems, where ∘ and ∗ are binary operations. If there exists a mapping ***f*** : $S_1 \rightarrow S_2$, such that $\forall x,y \in S_1$, $f(x \circ y) = f(x) * f(y)$ then f is called a *homomorphism* from V_1 to V_2, or simply a **homomorphism**.



- **Example :** $V=\langle R^*, \cdot \rangle$, determine which of the following functions are homomorphisms of V?

(1) $f(x)=|x|$ (2) $f(x)=2x$ (3) $f(x)=x^2$

(4) $f(x)=1/x$ (5) $f(x)=-x$ (6) $f(x)=x+1$

- **Solution:** Analyze whether the function satisfies $f(x \cdot y)=f(x) \cdot f(y)$ for all x,y in the nonzero real numbers set R^* .

(1) $f(x \cdot y) = |x \cdot y| = |x| \cdot |y| = f(x) \cdot f(y)$ homomorphisms

(2) $f(x \cdot y)=2(x \cdot y) \neq f(x) \cdot f(y)=(2x) \cdot (2y)=4xy$ non-homomorphic

(3) $f(x \cdot y)=(x \cdot y)^2=f(x) \cdot f(y)=x^2 \cdot y^2$ homomorphisms

(4) $f(x \cdot y)= 1/(x \cdot y)=f(x) \cdot f(y)= 1/x \cdot 1/y$ homomorphisms

(5) $f(x \cdot y)=-(x \cdot y) \neq f(x) \cdot f(y)=(-x) \cdot (-y)=xy$ non-homomorphic

(6) $f(x \cdot y)=x \cdot y+1 \neq f(x) \cdot f(y)\ (x+1) \cdot (y+1)=xy+x+y+1$ non-homomorphic

- Let f be a *homomorphism* from $V_1=<S_1,\circ>$ to $V_2=<S_2,*>$, if f is injective (one-to-one), then f is called a *monomorphism*.
  - **Note:** f being injective (or a one-to-one mapping) means that for any $x_1,x_2\in S_1$, if $f(x_1)=f(x_2)$, then $x_1=x_2$.
- **Example:** Let $V_1 = <R^*,\cdot>$, $V_2 = <R^*,\cdot>$, and define the mapping $f:R^*\rightarrow R^*$ 为 $f(x)=x^2$. Is f a monomorphism ?
  - We need to verify the homomorphism property and injectivity.
  - **Homomorphism:** We need to check whether for all $x,y\in R^*$, the equation $f(x\cdot y)=f(x)\cdot f(y)$ holds. Since $f(x\cdot y)= (x\cdot y)^2 = f(x)\cdot f(y) = x^2\cdot y^2$, thus $f(x)=x^2$ satisfies the *homomorphism* property .
  - **Injectivity:** We need to check whether for all $x_1, x_2\in R^*$,if $f(x_1)=f(x_2)$, then $x_1=x_2$. For example, if $x_1=-1$ 、 $x_2=1$， we have $x_1^2= x_2^2=1$，but $x_1\neq x_2$， Therefore, the mapping $f(x)=x^2$ is ***not injective*** .
  - **Conclusion:** $f(x)=x^2$ is a homomorphism, but it is **not** a monomorphism.

↳ Surjective homomorphism of algebraic systems

- Let f be a homomorphism from V_1=<S_1,∘ > to V_2=<S_2,∗>, if f is surjective (onto) , then f is called an ***epimorphism***. In this case, V_2 is called the **homomorphic image** of V_1, denoted $V_1 \overset{f}{\sim} V_2$.
  - **Note**: f being surjective (or an onto mapping) means that it is covering, i.e., for every element y in S_2 , there exists some element x in S_1 such that $f(x)=y$.
- **Example:** Let $V_1 = \langle Z,+\rangle$, $V_2=\langle Z_3,+_3\rangle$ (the set of integers modulo 3 with addition modulo 3), and define the mapping f: Z → Z_3 be defined by $f(x)= x$ **mod 3.** Is f an epimorphism ?

- *Homomorphism*: We need to check whether for all $x,y \in Z$, $f(x+y)=f(x) +_3 f(y)$. Since $f(x+y)=(x+y) \bmod 3$, $f(x) +_3 f(y)=(x \bmod 3 + y \bmod 3) \bmod 3$, by the distributive property of modular arithmetic, we have $f(x+y)=f(x) +_3 f(y)$, Therefore $f(x)= x \bmod 3$ satisfies the homomorphism property.
- *Surjectivity*: For each element y *in* Z_3, does there exist some x *in* Z_3 such that $f(x)=y$. Since every element in Z_3 (0, 1, 2) can be obtained by taking modulo 3 of some integer, f is surjective. That is, f is an epimorphism.
- *Conclusion*: $f(x)= x \bmod 3$ is a **homomorphism** and is indeed an **epimorphism**.
- **Note**: Since x_1 and x_2 having the same remainder under $f(x)= x \bmod 3$ does not imply that $x_1 = x_2$, f is not injective, that is, f is *not a monomorphism*.

- Let f be a homomorphism from V_1=<S_1,∘ > to V_2=<S_2,∗>, if f is bijective, then f is called an ***isomorphism*** from V_1 to V_2 denoted as $V_1 \cong V_2$.

- **Note**: f being bijective (or a one-to-one and onto mapping) means that f is both injective (one-to-one) and surjective (onto). The existence of an isomorphism between two algebraic systems means that their algebraic structures are equivalent.

- **Example:** Let $V_1=\langle R,+\rangle$, $V_2=\langle R,+\rangle$, f: R→R be defined by $f(x)=2x$. Is the mapping f an isomorphism from V_1 to V_2?
  - we need to verify two conditions: the mapping is a homomorphism, and it is bijective.

↳ Isomorphism of algebraic systems(e.g.)

- **Homomorphism:** $f(x+y)=2(x+y)=2x+2y=f(x)+f(y)$, which shows that f is a homomorphism.
- **Bijectivity :**
  - **Injectivity:** If $f(x_1)=f(x_2)$, **then** $2x_1 = 2x_2$, which leads to $x_1 = x_2$, showing that f is injective.
  - **Surjectivity:** For every real number $y \in \mathbf{R}$, there exists $x=y/2$, such that $f(x)=2 \cdot y/2=y$ showing that f is surjective.
  - Since f is both injective and surjective, it is bijective.
- **Conclusion:**

  $f(x)=2x$ is an *isomorphism* from $V1$ to $V2$, and it preserves the properties of the addition operation (closure, commutativity, associativity, identity element, and inverse element).

↳ Endomorphisms and automorphisms of algebraic systems

- A homomorphism f:S→S from an algebraic V=⟨S,∘⟩ to itself is called an ***endomorphism***. That is, for all x,y∈S we have $f(x∘y)=f(x)∘f(y)$.
- A ***zero homomorphism*** maps every input element to the zero element in the target algebraic structure.
- An ***automorphism*** refers to a homomorphism f:S→S of the algebraic system V=⟨S,∘⟩ that is both injective and surjective, indicating that the system is structurally equivalent to itself.
- A ***monomorphic endomorphism*** (or **injective endomorphism**) is a special type of endomorphism that is also injective.

- **Example: let V=<Z,+>, $\forall a \in$Z, f_a : Z→Z, $f_a(x)=ax$** . Prove that f_a is an endomorphism of V.
  - Since $\forall x,y \in$Z, we have: $f_a(x+y) = a(x+y) = ax+ay = f_a(x)+f_a(y)$.
  - When $a = 0$, f_0 is called the *zero homomorphism*, when $a=\pm 1$, f_a is called an ***automorphism***.
  - For all other values of a, f_a is an *injective endomorphism* (monomorphic endomorphism).

- **Example:** Let V_1=<Q,+>, V_2=<Q*,·>, where Q*=Q–{0} is the set of nonzero rational numbers. Define f : Q→Q*, $f(x)=e^x$.
  Determine the type of homomorphism that $f(x)$ defines from V_1 to V_2 .
- **Solution:**
  - f is a *homomorphism* from V_1 to V_2, because $\forall x,y \in$ Q, have $f(x+y)=e^{x+y}=e^x \cdot e^y=f(x) \cdot f(y)$.
  - f is a *monomorphism* because for $\forall x,y \in$ Q , If $f(x_1)=f(x_2)= e^{x1}=e^{x2}$, which implies $x_1=x_2$, f is ***injective***.
  - However, for any $y \in Q*$, e^x cannot reach every nonzero rational number (for example, negative numbers), so $f(x)=e^x$ is ***not surjective***.

- **Example:** Let $V=<Z_n,\oplus>$, $f_p:Z_n\to Z_n$, $f_p(x)$ = (xp) mod n, p = 0, 1, … , $n-1$. Analyze the properties of f_p.

① *Homomorphism*: $\forall x, y\in Z_n$, $f_p(x\oplus y)=((x\oplus y)p)$ mod n = (xp) mod $n \oplus (yp)$ mod $n = f_p(x) \oplus f_p(y)$.

② f_p is an *endomorphism*. Both the input and output of f_p are Z_n , and it satisfies the homomorphism property.

③ If *p and n are coprime*, then f_p is *injective* (**Monomorphism**). For example, when n=6 *and* p=3(which are not coprime), we have $f_p(1)=(1\cdot 3)$ *mod* 6 =3, but $x_1=1 \neq x_2=3$, so it is not injective.

- **Example:** Let V=<Z_n,⊕>, f_p:$Z_n \rightarrow Z_n$, $f_p(x)$ = (xp) mod n, p = 0, 1, … , n–1. Analyze the properties of f_p.

④ **Surjectivity (*Epimorphism*):** If ***p* and *n* are coprime**, then f_p is surjective. For example, with ***n*=6** and ***p*=3** (not coprime), in Z_6 , for y=0, there is ***x*=0,2,4**,for ***y*=3**, there is ***x*=1,3,5**,but for ***y*=1,2,4,5**, no ***x*** satisfies $f_p(x)=y$.

⑤ **Zero Homomorphism:** If ***p*=0**, then $f_p(x) = (x \cdot 0) \bmod n = 0$, which means it maps all inputs to zero. Therefore, f_p is the ***zero homomorphism***.

⑥ **Automorphism:** If ***p* and *n* are coprime**, f_p satisfies both injectivity and surjectivity (bijectivity), so f_p is an ***automorphism***.

↳ Properties of epimorphism between Algebraic Systems

- Let V_1 and V_2 be algebraic systems, and let $f : V_1 \rightarrow V_2$, be a **surjective (onto) homomorphism**. Then:

  (1) If the operation $\circ$ in V_1 is commutative (associative, idempotent), then the corresponding operation $\circ'$ in V_2 is also ***commutative*** (associative, idempotent).

  (2) If $\circ$ is distributive over $*$ in V_1 , then the corresponding $\circ'$ is ***distributive*** over $*'$ in V_2 .

  (3) If $\circ$ and $*$ are absorbent (absorption law holds) in V_1 , then the corresponding $\circ'$ and $*'$ are also ***absorbent*** in V_2 .

  (4) If $\circ$ in V_1 has an identity element e_1 (or a zero element θ_1), then $f(e_1)$) (or $f(\theta_1)$) is the ***identity (or zero) element*** for the corresponding operation $\circ'$ in V_2 .

  (5) If the inverse of x under $\circ$ in V_1 is x^{-1}, then the ***inverse*** of $f(x)$ under the corresponding $\circ'$ in V_2 is $f(x^{-1})$.