基礎抽象代數　群

許胖

板燒高中

January 23, 2015

大綱

定義

定義 (群)

一個代數結構 $(G, \cdot_G)$ 被稱爲**群 (Group)**，滿足以下條件：

此時 $\cdot_G$ 稱爲**群乘法**。

定義 (群)

一個代數結構 $(G, \cdot_G)$ 被稱為**群 (Group)**，滿足以下條件：

1. 有封閉律，對於所有 $a, b \in G$，$a \cdot_G b \in G$

此時 $\cdot_G$ 稱為**群乘法**。

定義 (群)

一個代數結構 $(G, \cdot_G)$ 被稱為**群 (Group)**，滿足以下條件：

1. 有封閉律，對於所有 $a, b \in G$，$a \cdot_G b \in G$
2. 有結合律，對於所有 $a, b, c \in G$，$(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$

此時 $\cdot_G$ 稱為**群乘法**。

定義 (群)

一個代數結構 $(G, \cdot_G)$ 被稱爲**群 (Group)**，滿足以下條件：

1. 有封閉律，對於所有 $a, b \in G$，$a \cdot_G b \in G$
2. 有結合律，對於所有 $a, b, c \in G$，$(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$
3. 有單位元素 $e \in G$，使得所有 $a \in G$，$e \cdot_G a = a \cdot_G e = a$

此時 $\cdot_G$ 稱爲**群乘法**。

定義

定義 (群)

一個代數結構 $(G, \cdot_G)$ 被稱爲**群 (Group)**，滿足以下條件：

1. 有封閉律，對於所有 $a, b \in G$，$a \cdot_G b \in G$
2. 有結合律，對於所有 $a, b, c \in G$，$(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$
3. 有單位元素 $e \in G$，使得所有 $a \in G$，$e \cdot_G a = a \cdot_G e = a$
4. 對於每個元素 $a \in G$ 都有反元素 $a' \in G$，使得 $a \cdot_G a' = a' \cdot_G a = e$

此時 $\cdot_G$ 稱爲**群乘法**。

群的性質 (1)

性質

若 $(G, \cdot_G)$ 爲一個群，則有以下性質：

群的性質 (1)

性質

若 $(G, \cdot_G)$ 為一個群，則有以下性質：

1. 單位元素唯一。

群的性質 (1)

性質

若 $(G, \cdot_G)$ 爲一個群，則有以下性質：

1. 單位元素唯一。
2. 對於所有 $a \in G$，其反元素唯一。

群的性質 (1)

性質

若 $(G, \cdot_G)$ 爲一個群，則有以下性質：

1. 單位元素唯一。
2. 對於所有 $a \in G$，其反元素唯一。

定義 (符號簡化)

若一個群 G 的二元運算爲群乘法 $\cdot_G$，則我們可對符號簡化：

1. 對於所有 $a, b \in G$，$a \cdot_G b$ 可寫爲 ab。
2. 對於所有 $a \in G$，其反元素記爲 a^{-1}。

群的性質 (2)

性質

若 $(G, \cdot_G)$ 爲一個群，對於所有 $a, b \in G$，則有以下性質：

註

$\left(a^{-1}\right)^{-1}$ 應理解爲「a^{-1} 的反元素」。

群的性質 (2)

性質

若 $(G, \cdot_G)$ 為一個群，對於所有 $a, b \in G$，則有以下性質：

1. $\left(a^{-1}\right)^{-1} = a$

註

$\left(a^{-1}\right)^{-1}$ 應理解為「a^{-1} 的反元素」。

群的性質 (2)

性質

若 $(G, \cdot_G)$ 為一個群，對於所有 $a, b \in G$，則有以下性質：

1. $\left(a^{-1}\right)^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

註

$\left(a^{-1}\right)^{-1}$ 應理解為「a^{-1} 的反元素」。

定義 (群連乘)

若一個群 G 的二元運算爲群乘法 $\cdot_G$，則定義群連乘 a^k，$k \in \mathbb{Z}$：

1. $k = 0$ 時，$a^k = a^0 = e$
2. $k > 0$ 時，$a^k = a \cdot_G a^{k-1} = aa^{k-1}$；$a^{-k} = (a^{-1})^k$

群連乘

定義 (群連乘)

若一個群 G 的二元運算爲群乘法 $\cdot_G$，則定義群連乘 a^k，$k \in \mathbb{Z}$：

1. $k = 0$ 時，$a^k = a^0 = e$
2. $k > 0$ 時，$a^k = a \cdot_G a^{k-1} = aa^{k-1}$；$a^{-k} = (a^{-1})^k$

推論

一個群 G 中，對所有 $a \in G$，$m, n \in \mathbb{Z}$，則

1. $a^m a^n = a^{m+n} = a^n a^m$

群連乘

定義 (群連乘)

若一個群 G 的二元運算爲群乘法 $\cdot_G$，則定義群連乘 a^k，$k \in \mathbb{Z}$：

1. $k = 0$ 時，$a^k = a^0 = e$
2. $k > 0$ 時，$a^k = a \cdot_G a^{k-1} = aa^{k-1}$；$a^{-k} = (a^{-1})^k$

推論

一個群 G 中，對所有 $a \in G$，$m, n \in \mathbb{Z}$，則

1. $a^m a^n = a^{m+n} = a^n a^m$
2. $(a^m)^n = a^{mn}$

群連乘

定義 (群連乘)

若一個群 G 的二元運算爲群乘法 $\cdot_G$，則定義群連乘 a^k，$k \in \mathbb{Z}$：

1. $k = 0$ 時，$a^k = a^0 = e$
2. $k > 0$ 時，$a^k = a \cdot_G a^{k-1} = aa^{k-1}$；$a^{-k} = (a^{-1})^k$

推論

一個群 G 中，對所有 $a \in G$，$m, n \in \mathbb{Z}$，則

1. $a^m a^n = a^{m+n} = a^n a^m$
2. $(a^m)^n = a^{mn}$
3. $(a^m)^{-1} = a^{-m}$

群的消去律

性質

若 $(G, \cdot_G)$ 為一個群，則 G 滿足消去律。即對於所有 $a, b, c \in G$，若

1. $ab = ac$，則 $b = c$
2. $ba = ca$，則 $b = c$

群的消去律

性質

若 $(G, \cdot_G)$ 爲一個群，則 G 滿足消去律。即對於所有 $a, b, c \in G$，若

1. $ab = ac$，則 $b = c$
2. $ba = ca$，則 $b = c$

定理

若 $(G, \cdot_G)$ 爲一個群，則對於任意 $a, b \in G$，x, y 是未知數，$ax = b$ 和 $ya = b$ 存在唯一解。

阿貝爾群

定義 (阿貝爾群)

一個群 $(G, \cdot_G)$，若對所有 $a, b \in G$ 都滿足 $ab = ba$，則 G 稱爲**阿貝爾群 (Abelian group)**，又稱**交換群**。

範例

$(\mathbb{Z}, +)$ 是一個交換群，$(\mathbb{M}_{n\times n}(\mathbb{R}), \cdot)$ 就不是，反例：

阿貝爾群

定義 (阿貝爾群)

一個群 $(G, \cdot_G)$，若對所有 $a, b \in G$ 都滿足 $ab = ba$，則 G 稱為**阿貝爾群 (Abelian group)**，又稱交換群。

範例

$(\mathbb{Z}, +)$ 是一個交換群，$(\mathbb{M}_{n\times n}(\mathbb{R}), \cdot)$ 就不是，反例：

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = BA$$

定義 (半群和單半群)

一個代數結構 $(G, \cdot_G)$ 若滿足 *1* 和 *2*，則 G 稱爲**半群 (Semigroup)**。若 $(G, \cdot_G)$ 滿足 *1*、*2*、*3*，則 G 稱爲**單半群 (Monoid)**。

半群、有限群

定義 (半群和單半群)

一個代數結構 $(G, \cdot_G)$ 若滿足 *1* 和 *2*，則 G 稱爲**半群 (Semigroup)**。若 $(G, \cdot_G)$ 滿足 *1*、*2*、*3*，則 G 稱爲**單半群 (Monoid)**。

定義 (有限群)

一個群 $(G, \cdot_G)$ 若 $|G| < \infty$，則 G 稱爲**有限群 (Finite group)**。

定義 (子群)

一個群 $(G, \cdot_G)$ 上，若 $(H, \cdot_H)$ 是一個群且 $H \subseteq G$、$H \neq \emptyset$，則 $(H, \cdot_H)$ 被稱爲 G 的子群 **(Subgroup)**。

定義 (子群)

一個群 $(G, \cdot_G)$ 上，若 $(H, \cdot_H)$ 是一個群且 $H \subseteq G$、$H \neq \emptyset$，則 $(H, \cdot_H)$ 被稱爲 G 的子群 **(Subgroup)**。

註

$\cdot_G$ 和 $\cdot_H$ 要是相同的。

子群簡化 (1)

引理 (實用版子群)

一個群 $(G, \cdot_G)$ 上有一個非空子集 H，H 滿足以下條件

1. 對於任意 $a, b \in H$，$ab \in H$
2. 對於任意 $a \in H$，存在 $a^{-1} \in H$

若且唯若 $(H, \cdot_H)$ 是一個子群。

子群簡化 (1)

引理 (實用版子群)

一個群 $(G, \cdot_G)$ 上有一個非空子集 H，H 滿足以下條件

1. 對於任意 $a, b \in H$，$ab \in H$
2. 對於任意 $a \in H$，存在 $a^{-1} \in H$

若且唯若 $(H, \cdot_H)$ 是一個子群。

註

事實上這兩個規則就是驗證 1 和 4。

子群簡化 (2)

引理 (精簡版子群)

一個群 $(G, \cdot_G)$ 上有一個非空子集 H，對於任意 $a, b \in H$，$ab^{-1} \in H$ 若且唯若 $(H, \cdot_H)$ 是一個子群。

子群簡化 (2)

引理 (精簡版子群)

一個群 $(G, \cdot_G)$ 上有一個非空子集 H，對於任意 $a, b \in H$，$ab^{-1} \in H$ 若且唯若 $(H, \cdot_H)$ 是一個子群。

性質

一個群 $(G, \cdot_G)$ 上若有兩個子群 H_1、H_2，則 $H_1 \cap H_2$ 是 G 的子群。

有限群

定理 (有限子群)

一個有限群 $(G, \cdot_G)$ 上有一個非空子集 H，對於任意 $a, b \in H$，$ab \in H$ 若且唯若 $(H, \cdot_H)$ 是一個子群。