Algebraic Structure (代数结构)
Chapter 1: Group Fundamentals

刘胜利

liu-sl@cs.sjtu.edu.cn
密码与信息安全实验室
计算机科学与工程系
上海交通大学

课程简介

- 课程内容：主要介绍群、环、域的主要概念及其基本性质；
- 中文参考书：韩士安，林磊，“近世代数”，科学出版社
- 英文参考书：Robert B. Ash：Abstract Algebra: The Basic Graduate Year

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题：“不能任意三等分角”，“倍立方不可能”，“化圆为方不可能”。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题：“不能任意三等分角”，“倍立方不可能”，“化圆为方不可能”。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题：“不能任意三等分角”，“倍立方不可能”，“化圆为方不可能”。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题：“不能任意三等分角”，“倍立方不可能”，“化圆为方不可能”。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题："不能任意三等分角"，"倍立方不可能"，"化圆为方不可能"。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题："不能任意三等分角"，"倍立方不可能"，"化圆为方不可能"。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

代数结构与现代科学

Galois（伽罗华），群论的鼻祖。

数学 建立了近世代数（抽象代数）这一新的学科。

- 系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 它解决了古代的尺规作图问题：“不能任意三等分角”，“倍立方不可能”，“化圆为方不可能”。

近代物理和化学

- 对正四面体的顶点用两种颜色着色，有多少种本质上不同的着色法？
- r种颜色的珠子做成有n颗珠子的项链，可做成多少种不同的项链？

计算机科学 两界图灵奖获得者的工作

- 2002年度图灵奖获得者Rivest, Shamir, Adleman所提出的RSA算法；
- 2012年度图灵奖获得者Goldwasser和Micali所提出的GM概率加密算法。

集合

- 集合：一些确定的、可以区分的事物汇聚在一起组成的一个整体，一般用大写字母表示；
- 元素：组成一个集合的每个事物称为该集合的一个元素．或简称一个元，一般用小写字母表示；
- 如果a是集合A的一个元素，就说a属于A，或者说a在A中，记作$a \in A$。若b不属于A．或者说b不在A中,记作$b \notin A$。

集合

- 集合：一些确定的、可以区分的事物汇聚在一起组成的一个整体，一般用大写字母表示；
- 元素：组成一个集合的每个事物称为该集合的一个元素．或简称一个元，一般用小写字母表示；
- 如果a是集合A的一个元素，就说a属于A，或者说a在A中，记作$a \in A$。若b不属于A．或者说b不在A中,记作$b \notin A$。

集合

- 集合：一些确定的、可以区分的事物汇聚在一起组成的一个整体，一般用大写字母表示；
- 元素：组成一个集合的每个事物称为该集合的一个元素．或简称一个元，一般用小写字母表示；
- 如果a是集合A的一个元素，就说a属于A，或者说a在A中，记作$a \in A$。若b不属于A．或者说b不在A中,记作$b \notin A$。

(1) 集合的元素可以是任何事物，也可以是另外的集合，但是集合的元素不能是该集合自身；

(2) 一个集合的各个元素是可以互相区分开的．即：元素不会重复出现；

(3) 组成一个集合的各个元素在该集合中是无次序的；

(4) 任一事物是否属于一个集合，答案是确定性的：是或否，没有第三种答案。

(1) 集合的元素可以是任何事物，也可以是另外的集合，但是集合的元素不能是该集合自身；

(2) 一个集合的各个元素是可以互相区分开的．即：元素不会重复出现；

(3) 组成一个集合的各个元素在该集合中是无次序的；

(4) 任一事物是否属于一个集合，答案是确定性的：是或否，没有第三种答案。

(1) 集合的元素可以是任何事物，也可以是另外的集合，但是集合的元素不能是该集合自身；

(2) 一个集合的各个元素是可以互相区分开的．即：元素不会重复出现；

(3) 组成一个集合的各个元素在该集合中是无次序的；

(4) 任一事物是否属于一个集合，答案是确定性的：是或否，没有第三种答案。

(1) 集合的元素可以是任何事物，也可以是另外的集合，但是集合的元素不能是该集合自身；

(2) 一个集合的各个元素是可以互相区分开的．即：元素不会重复出现；

(3) 组成一个集合的各个元素在该集合中是无次序的；

(4) 任一事物是否属于一个集合，答案是确定性的：是或否，没有第三种答案。

几个常用的集合的表示：

- $\mathbb{N}$：表示全体自然数组成的集合；
- $\mathbb{Z}$：表示全体整数组成的集合；
- $\mathbb{Q}$：表示全体有理数组成的集合；
- $\mathbb{R}$：表示全体实数组成的集合；
- $\mathbb{C}$：表示全体复数组成的集合。

几个常用的集合的表示：

- $\mathbb{N}$：表示全体自然数组成的集合；
- $\mathbb{Z}$：表示全体整数组成的集合；
- $\mathbb{Q}$：表示全体有理数组成的集合；
- $\mathbb{R}$：表示全体实数组成的集合；
- $\mathbb{C}$：表示全体复数组成的集合。

几个常用的集合的表示：

- $\mathbb{N}$：表示全体自然数组成的集合；
- $\mathbb{Z}$：表示全体整数组成的集合；
- $\mathbb{Q}$：表示全体有理数组成的集合；
- $\mathbb{R}$：表示全体实数组成的集合；
- $\mathbb{C}$：表示全体复数组成的集合。

几个常用的集合的表示：

- $\mathbb{N}$：表示全体自然数组成的集合；
- $\mathbb{Z}$：表示全体整数组成的集合；
- $\mathbb{Q}$：表示全体有理数组成的集合；
- $\mathbb{R}$：表示全体实数组成的集合；
- $\mathbb{C}$：表示全体复数组成的集合。

几个常用的集合的表示：

- $\mathbb{N}$：表示全体自然数组成的集合；
- $\mathbb{Z}$：表示全体整数组成的集合；
- $\mathbb{Q}$：表示全体有理数组成的集合；
- $\mathbb{R}$：表示全体实数组成的集合；
- $\mathbb{C}$：表示全体复数组成的集合。

集合的表示

- 外延表示法：一一列举出集合的全体元素。

  $A = \{7, 8, 9\}$

  $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$

  $B = \{a, b, \cdots, y, z\}$。

- 内涵表示法：用谓词来描述集合中元素的性质。

  $A = \{x \mid P(x)\}$

  $A = \{x \mid x\text{是整数且}6 < x < 10\}$

  $\mathbb{N} = \{x \mid x \text{ 是自然数}\}$

集合的表示

- 外延表示法：一一列举出集合的全体元素。

  $A = \{7, 8, 9\}$

  $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$

  $B = \{a, b, \cdots, y, z\}$。

- 内涵表示法：用谓词来描述集合中元素的性质。

  $A = \{x \mid P(x)\}$

  $A = \{x \mid x\text{是整数且}6 < x < 10\}$

  $\mathbb{N} = \{x \mid x \text{ 是自然数}\}$

集合的关系和特殊集合

在实数之间可以定义关系$=, <, \leq, >, \geq$。类似地，在集合之间可以定义关系$=, \subset, \subseteq, \supset, \supseteq$.

- 两个集合是相等的，当且仅当它们有相同的元素。
  - 若两个集合A和B相等，则记作$A = B$；
    $A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
  - 若A和B不相等，则记作$A \neq B$。
    $A \neq B \Leftrightarrow (\exists x)\neg(x \in A \leftrightarrow x \in B)$
- 外延公理：一个集合是由它的元素完全决定的。

集合的关系和特殊集合

在实数之间可以定义关系$=, <, \leq, >, \geq$。类似地，在集合之间可以定义关系$=, \subset, \subseteq, \supset, \supseteq$.

- 两个集合是相等的，当且仅当它们有相同的元素。
  - 若两个集合A和B相等，则记作$A = B$；
    $A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
  - 若A和B不相等，则记作$A \neq B$。
    $A \neq B \Leftrightarrow (\exists x)\neg(x \in A \leftrightarrow x \in B)$
- 外延公理：一个集合是由它的元素完全决定的。

集合的关系和特殊集合

在实数之间可以定义关系$=, <, \leq, >, \geq$。类似地，在集合之间可以定义关系$=, \subset, \subseteq, \supset, \supseteq$.

- 两个集合是相等的，当且仅当它们有相同的元素。
  - 若两个集合A和B相等，则记作$A = B$；
    $A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
  - 若A和B不相等，则记作$A \neq B$。
    $A \neq B \Leftrightarrow (\exists x)\neg(x \in A \leftrightarrow x \in B)$
- 外延公理：一个集合是由它的元素完全决定的。

集合的关系和特殊集合

在实数之间可以定义关系$=, <, \leq, >, \geq$。类似地，在集合之间可以定义关系$=, \subset, \subseteq, \supset, \supseteq$.

- 两个集合是相等的，当且仅当它们有相同的元素。
  - 若两个集合A和B相等，则记作$A = B$；
    $A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
  - 若A和B不相等，则记作$A \neq B$。
    $A \neq B \Leftrightarrow (\exists x)\neg(x \in A \leftrightarrow x \in B)$
- 外延公理：一个集合是由它的元素完全决定的。

- 对任意两个集合A和B，若A的每个元素都是B的元素，就称A为B的子集合(子集)，或称B包含A，或称B是A的超集合，记作$A \subseteq B$或$B \supseteq A$。
- 这个定义也可以写成

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$$

当A不是B的子集合时，即$A \subseteq B$不成立时，记作$A \not\subseteq B$。
- $\subseteq$与$\in$的区别：

$\{a, b\} \subseteq \{a, b, \{a\}\}$但$\{a, b\} \notin \{a, b, \{a\}\}$
- 对任意两个集合A和B，若$A \subseteq B$且$A \neq B$，就称A为B的真子集，或称B真包含A，或称B是A的真超集合，记作$A \subset B$或$B \subset A$。

$$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$$

- 对任意两个集合A和B，若A的每个元素都是B的元素，就称A为B的子集合(子集)，或称B包含A，或称B是A的超集合，记作$A \subseteq B$或$B \supseteq A$。
- 这个定义也可以写成

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$$

当A不是B的子集合时，即$A \subseteq B$不成立时，记作$A \nsubseteq B$。

- $\subseteq$与$\in$的区别：

$\{a, b\} \subseteq \{a, b, \{a\}\}$但$\{a, b\} \notin \{a, b, \{a\}\}$

- 对任意两个集合A和B，若$A \subseteq B$且$A \neq B$，就称A为B的真子集，或称B真包含A，或称B是A的真超集合，记作$A \subset B$或$B \subset A$。

$$A \subset B \Leftrightarrow (A \subseteq B \land A \neq B)$$

- 对任意两个集合A和B，若A的每个元素都是B的元素，就称A为B的子集合(子集)，或称B包含A，或称B是A的超集合，记作$A \subseteq B$或$B \supseteq A$。
- 这个定义也可以写成

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$$

当A不是B的子集合时，即$A \subseteq B$不成立时，记作$A \nsubseteq B$。

- $\subseteq$与$\in$的区别：

$\{a, b\} \subseteq \{a, b, \{a\}\}$但$\{a, b\} \notin \{a, b, \{a\}\}$

- 对任意两个集合A和B，若$A \subseteq B$且$A \neq B$，就称A为B的真子集，或称B真包含A，或称B是A的真超集合，记作$A \subset B$或$B \subset A$。

$$A \subset B \Leftrightarrow (A \subseteq B \land A \neq B)$$

- 对任意两个集合A和B，若A的每个元素都是B的元素，就称A为B的子集合(子集)，或称B包含A，或称B是A的超集合，记作$A \subseteq B$或$B \supseteq A$。
- 这个定义也可以写成

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$$

当A不是B的子集合时，即$A \subseteq B$不成立时，记作$A \nsubseteq B$。

- $\subseteq$与$\in$的区别：

$\{a, b\} \subseteq \{a, b, \{a\}\}$但$\{a, b\} \notin \{a, b, \{a\}\}$

- 对任意两个集合A和B，若$A \subseteq B$且$A \neq B$，就称A为B的真子集，或称B真包含A，或称B是A的真超集合，记作$A \subset B$或$B \subset A$。

$$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$$

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集.

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集.

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集。

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集.

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集.

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集.

- 不含任何元素的集合称为空集，记作$\emptyset$。

$$\emptyset = \{x \mid x \neq x\}$$

  - $(\forall x)(x \notin \emptyset)$为真；
  - 对任意的集合A，$\emptyset \subseteq A$；
  - 空集是唯一的。

- 所有事物的集合称为全集，记作E。全集的定义也可以写成

$$E = \{x \mid x = x\}$$

  - 全集的概念当于谓词逻辑的论域。
  - 对不同的问题，往往使用不同的论域，例如在研究有关实数的问题时，就以$\mathbb{R}$为全集.

集合的运算

集合的运算是由已知集合构造新集合的一种方法，是表示集合的第三种方法.

(1) 并集$A \cup B = \{x \mid x \in A \vee x \in B\}$;

(2) 交集$A \cap B = \{x \mid x \in A \wedge x \in B\}$;

(3) 差集(又称B对A的相对补集，补集)

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

集合的运算

集合的运算是由已知集合构造新集合的一种方法，是表示集合的第三种方法.

(1) 并集$A \cup B = \{x \mid x \in A \vee x \in B\}$;

(2) 交集$A \cap B = \{x \mid x \in A \wedge x \in B\}$;

(3) 差集(又称B对A的相对补集，补集)

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

集合的运算

集合的运算是由已知集合构造新集合的一种方法，是表示集合的第三种方法.

(1) 并集$A \cup B = \{x \mid x \in A \vee x \in B\}$;

(2) 交集$A \cap B = \{x \mid x \in A \wedge x \in B\}$;

(3) 差集(又称B对A的相对补集，补集)

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

集合的运算

集合的运算是由已知集合构造新集合的一种方法，是表示集合的第三种方法.

(1) 并集$A \cup B = \{x \mid x \in A \vee x \in B\}$;

(2) 交集$A \cap B = \{x \mid x \in A \wedge x \in B\}$;

(3) 差集(又称B对A的相对补集，补集)

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

(4) 余集(又称A的绝对补集)

$-A = E - A = \{x \mid x \notin A\}$,

其中E为全集．A的余集就是A对E的相对补集。

(5) 对称差$A \oplus B = (A - B) \cup (B - A)$

$= \{x \mid x \in A \overline{\vee} x \in B\}$

(4) 余集(又称A的绝对补集)

$-A = E - A = \{x \mid x \notin A\}$,

其中E为全集．A的余集就是A对E的相对补集。

(5) 对称差$A \oplus B = (A - B) \cup (B - A)$

$$= \{x \mid x \in A \overline{\vee} x \in B\}$$

广义并，广义交，幂集

- 广义并和广义交是一元运算，是对一个集合的集合A进行的运算.
- 若集合A的元素都是集合，则把A的所有元素的元素组成的集合称为A的广义并，记作$\cup A$；

$$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$$

- 把A的所有元素的公共元素组成的集合称为A的广义交，记作$\cap A$。

$$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$$

- 规定$\cup\emptyset = \emptyset$，规定$\cap\emptyset$无意义。
- 可以用广义并和广义交分别定义并集和交集

广义并，广义交，幂集

- 广义并和广义交是一元运算，是对一个集合的集合A进行的运算.
- 若集合A的元素都是集合，则把A的所有元素的元素组成的集合称为A的广义并，记作$\cup A$；

$$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$$

- 把A的所有元素的公共元素组成的集合称为A的广义交，记作$\cap A$。

$$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$$

- 规定$\cup\emptyset = \emptyset$，规定$\cap\emptyset$无意义。
- 可以用广义并和广义交分别定义并集和交集

广义并，广义交，幂集

- 广义并和广义交是一元运算，是对一个集合的集合A进行的运算.
- 若集合A的元素都是集合，则把A的所有元素的元素组成的集合称为A的广义并，记作$\cup A$；

$$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$$

- 把A的所有元素的公共元素组成的集合称为A的广义交，记作$\cap A$。

$$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$$

- 规定$\cup\emptyset = \emptyset$，规定$\cap\emptyset$无意义。
- 可以用广义并和广义交分别定义并集和交集

广义并，广义交，幂集

- 广义并和广义交是一元运算，是对一个集合的集合A进行的运算.
- 若集合A的元素都是集合，则把A的所有元素的元素组成的集合称为A的广义并，记作$\cup A$；

$$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$$

- 把A的所有元素的公共元素组成的集合称为A的广义交，记作$\cap A$。

$$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$$

- 规定$\cup\emptyset = \emptyset$，规定$\cap\emptyset$无意义。
- 可以用广义并和广义交分别定义并集和交集

广义并，广义交，幂集

- 广义并和广义交是一元运算，是对一个集合的集合A进行的运算.
- 若集合A的元素都是集合，则把A的所有元素的元素组成的集合称为A的广义并，记作$\cup A$；

$$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$$

- 把A的所有元素的公共元素组成的集合称为A的广义交，记作$\cap A$。

$$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$$

- 规定$\cup\emptyset = \emptyset$，规定$\cap\emptyset$无意义。
- 可以用广义并和广义交分别定义并集和交集

广义并，广义交，幂集

- 广义并和广义交是一元运算，是对一个集合的集合A进行的运算.
- 若集合A的元素都是集合，则把A的所有元素的元素组成的集合称为A的广义并，记作$\cup A$；

$$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$$

- 把A的所有元素的公共元素组成的集合称为A的广义交，记作$\cap A$。

$$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$$

- 规定$\cup\emptyset = \emptyset$，规定$\cap\emptyset$无意义。
- 可以用广义并和广义交分别定义并集和交集

笛卡儿积

笛卡儿积也是一种集合二元运算，两个集合的笛卡儿积是它们的元素组成的有序对的集合。

定义9.3.6:集合A和B的笛卡儿积(又称卡氏积、乘积、直积)$A\times B$定义为

$$A \times B = \{z | x \in A \quad \wedge \quad y \in B \quad \wedge \quad z = < x, y >\}$$

或简写为

$$A \times B = \{< x, y > | x \in A \quad \wedge \quad y \in B\}$$

笛卡儿积

笛卡儿积也是一种集合二元运算，两个集合的笛卡儿积是它们的元素组成的有序对的集合。

定义9.3.6:集合A和B的笛卡儿积(又称卡氏积、乘积、直积)$A \times B$定义为

$$A \times B = \{z | x \in A \quad \wedge \quad y \in B \quad \wedge \quad z =< x, y >\}$$

或简写为

$$A \times B = \{< x, y > | x \in A \quad \wedge \quad y \in B\}$$

笛卡儿积

笛卡儿积也是一种集合二元运算，两个集合的笛卡儿积是它们的元素组成的有序对的集合。

定义9.3.6:集合A和B的笛卡儿积(又称卡氏积、乘积、直积)$A \times B$定义为

$$A \times B = \{z | x \in A \quad \wedge \quad y \in B \quad \wedge \quad z =< x, y >\}$$

或简写为

$$A \times B = \{< x, y > | x \in A \quad \wedge \quad y \in B\}$$

二元关系

对集合A和B，$A \times B$的任一子集称为A到B的一个二元关系，一般记作R。

特殊的关系：

(1) A上的恒等关系I_A定义为：

$$I_A = \{\langle x, x\rangle | x \in A\}$$

(2) A上的全域关系I_A定义为：

$$E_A = \{\langle x, y\rangle | x \in A, y \in A\} = A \times A$$

(3) $\emptyset$ 是A上的空关系

二元关系

对集合A和B，$A \times B$的任一子集称为A到B的一个二元关系，一般记作R。

特殊的关系：

(1) A上的恒等关系I_A定义为：

$$I_A = \{\langle x, x\rangle | x \in A\}$$

(2) A上的全域关系I_A定义为：

$$E_A = \{\langle x, y\rangle | x \in A, y \in A\} = A \times A$$

(3) $\emptyset$是A上的空关系

二元关系

对集合A和B，$A \times B$的任一子集称为A到B的一个二元关系，一般记作R。

特殊的关系：

(1) A上的恒等关系I_A定义为：

$$I_A = \{\langle x, x\rangle | x \in A\}$$

(2) A上的全域关系I_A定义为：

$$E_A = \{\langle x, y\rangle | x \in A, y \in A\} = A \times A$$

(3) $\emptyset$是A上的空关系

二元关系

对集合A和B，$A \times B$的任一子集称为A到B的一个二元关系，一般记作R。

特殊的关系：

(1) A上的恒等关系I_A定义为：

$$I_A = \{\langle x, x\rangle | x \in A\}$$

(2) A上的全域关系I_A定义为：

$$E_A = \{\langle x, y\rangle | x \in A, y \in A\} = A \times A$$

(3) $\emptyset$是A上的空关系

关系的性质

对A上的关系来说，主要的性质有：自反性、对称性、传递性。

- 对A上的关系R，若对任意的$x \in A$都有xRx，则称R为A上自反的关系。
- R是A上对称的 $\Leftrightarrow (\forall x)(\forall y)((x \in A \wedge y \in A \wedge xRy) \rightarrow yRx)$
- R是A上是传递的$\Leftrightarrow (\forall x)(\forall y)(\forall z)((x \in A \wedge y \in A \wedge z \in A \wedge xRy \wedge yRz) \rightarrow xRz)$

关系的性质

对A上的关系来说，主要的性质有：自反性、对称性、传递性。

- 对A上的关系R，若对任意的$x \in A$都有xRx，则称R为A上自反的关系。
- R是A上对称的
  $\Leftrightarrow (\forall x)(\forall y)((x \in A \wedge y \in A \wedge xRy) \to yRx)$
- R是A上是传递的$\Leftrightarrow (\forall x)(\forall y)(\forall z)((x \in A \wedge y \in A \wedge z \in A \wedge xRy \wedge yRz) \to xRz)$

关系的性质

对A上的关系来说，主要的性质有：自反性、对称性、传递性。

- 对A上的关系R，若对任意的$x \in A$都有xRx，则称R为A上自反的关系。
- R是A上对称的 $\Leftrightarrow (\forall x)(\forall y)((x \in A \land y \in A \land xRy) \to yRx)$
- R是A上是传递的$\Leftrightarrow (\forall x)(\forall y)(\forall z)((x \in A \land y \in A \land z \in A \land xRy \land yRz) \to xRz)$

等价关系

定义：对非空集合A上的关系R，如果R具有自反性、对称性和传递性，则称R为A上的“等价关系”。

- 在实数之间的相等关系；
- 集合之间的相等关系；
- 谓词公式之间的等值关系；
- 在非空集合A上的恒等关系I_A和全关系E_A都是等价关系。

例：在$\mathbb{Z}$中的同余关系：

$a \equiv b \mod n \Leftrightarrow n \mid (a-b)$。

定义：同余类(等价类)$\bar{a} = \{x \mid x \equiv a \mod n, \quad x \in \mathbb{Z}\}$，则

$$\bar{a} = \{kn + a | k \in \mathbb{Z}\}.$$

等价关系

定义：对非空集合A上的关系R，如果R具有自反性、对称性和传递性，则称R为A上的“等价关系”。

- 在实数之间的相等关系；
- 集合之间的相等关系；
- 谓词公式之间的等值关系；
- 在非空集合A上的恒等关系I_A和全关系E_A都是等价关系。

例：在$\mathbb{Z}$中的同余关系：

$a \equiv b \mod n \Leftrightarrow n \mid (a-b)$。

定义：同余类(等价类)$\bar{a} = \{x \mid x \equiv a \mod n, \quad x \in \mathbb{Z}\}$，则

$$\bar{a} = \{kn + a \mid k \in \mathbb{Z}\}.$$

等价关系

定义：对非空集合A上的关系R，如果R具有自反性、对称性和传递性，则称R为A上的"等价关系"。

- 在实数之间的相等关系；
- 集合之间的相等关系；
- 谓词公式之间的等值关系；
- 在非空集合A上的恒等关系I_A和全关系E_A都是等价关系。

例：在$\mathbb{Z}$中的同余关系：

$a \equiv b \mod n \Leftrightarrow n \mid (a-b)$。

定义：同余类(等价类)$\bar{a} = \{x \mid x \equiv a \mod n, \quad x \in \mathbb{Z}\}$，则

$$\bar{a} = \{kn + a \mid k \in \mathbb{Z}\}.$$

等价关系

定义：对非空集合A上的关系R，如果R具有自反性、对称性和传递性，则称R为A上的“等价关系”。

- 在实数之间的相等关系；
- 集合之间的相等关系；
- 谓词公式之间的等值关系；
- 在非空集合A上的恒等关系I_A和全关系E_A都是等价关系。

例：在$\mathbb{Z}$中的同余关系：

$a \equiv b \mod n \Leftrightarrow n \mid (a-b)$。

定义：同余类(等价类)$\bar{a} = \{x \mid x \equiv a \mod n, \quad x \in \mathbb{Z}\}$，则

$$\bar{a} = \{kn + a | k \in \mathbb{Z}\}.$$

等价关系

定义：对非空集合A上的关系R，如果R具有自反性、对称性和传递性，则称R为A上的“等价关系”。

- 在实数之间的相等关系；
- 集合之间的相等关系；
- 谓词公式之间的等值关系；
- 在非空集合A上的恒等关系I_A和全关系E_A都是等价关系。

例：在$\mathbb{Z}$中的同余关系：

$a \equiv b \mod n \Leftrightarrow n \mid (a-b)$。

定义：同余类(等价类)$\bar{a} = \{x \mid x \equiv a \mod n, \quad x \in \mathbb{Z}\}$，则

$$\bar{a} = \{kn + a | k \in \mathbb{Z}\}.$$

等价关系

定义：对非空集合A上的关系R，如果R具有自反性、对称性和传递性，则称R为A上的“等价关系”。

- 在实数之间的相等关系；
- 集合之间的相等关系；
- 谓词公式之间的等值关系；
- 在非空集合A上的恒等关系I_A和全关系E_A都是等价关系。

例：在$\mathbb{Z}$中的同余关系：

$a \equiv b \mod n \Leftrightarrow n \mid (a - b)$。

定义：同余类(等价类)$\bar{a} = \{x \mid x \equiv a \mod n, \quad x \in \mathbb{Z}\}$，则

$$\bar{a} = \{kn + a | k \in \mathbb{Z}\}.$$

商集

定义：对非空集合A上的关系R，以R的不相交的等价类为元素的集合称为A的商集，记作A/R，

$$A/R = \{y|(\exists x)(x \in A \wedge y = [x]_R)\}$$

同余关系的商集为：$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$.

划分

$A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. $A/R = \{\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6\}\}$

定义：对非空集合A，若存在集合π，满足：

(1) $(\forall x)(x \in \pi \to x \subseteq A)$,

(2) $\emptyset \notin \pi$

(3) $\cup\pi = A$

(4) $(\forall x)(\forall y)((x \in \pi \wedge y \in \pi \wedge x \neq y) \to x \cap y = \emptyset)$,

则称π为A的一个“划分”，称π中的元素为A的“划分块”.

划分

A的一个划分π，

- 是A的非空子集的集合，即$\pi \subseteq P(A)$且$\emptyset \notin \pi$.
- A的这些子集互不相交；
- A的这些子集的并集为A.

划分

A的一个划分π，

- 是A的非空子集的集合，即$\pi \subseteq P(A)$且$\emptyset \notin \pi$.
- A的这些子集互不相交；
- A的这些子集的并集为A.

划分

A的一个划分π，

- 是A的非空子集的集合，即$\pi \subseteq P(A)$且$\emptyset \notin \pi$.
- A的这些子集互不相交；
- A的这些子集的并集为A.

划分

定理：对非空集合A上的等价关系R，A的商集A/R就是A的划分，它称为由等价关系R诱导出来的A的划分，记作π_R.

上面的定理说明由A上的等价关系R可以诱导出A的一个划分．下面考虑，由A的一个划分如何诱导出A上的一个等价关系．

定理：对非空集合A的一个划分π，令A上的关系R_π为

$$R_\pi = \{\langle x, y\rangle | (\exists z)(z \in \pi \wedge x \in z \wedge y \in z)\}$$

则R_π为A上的等价关系，它称为划分π诱导出的A上的等价关系.

划分

定理：对非空集合A上的等价关系R，A的商集A/R就是A的划分，它称为由等价关系R诱导出来的A的划分，记作π_R.

上面的定理说明由A上的等价关系R可以诱导出A的一个划分．下面考虑，由A的一个划分如何诱导出A上的一个等价关系．

定理：对非空集合A的一个划分π，令A上的关系R_π为

$$R_\pi = \{\langle x, y\rangle | (\exists z)(z \in \pi \wedge x \in z \wedge y \in z)\}$$

则R_π为A上的等价关系，它称为划分π诱导出的A上的等价关系.

划分

定理：对非空集合A上的等价关系R，A的商集A/R就是A的划分，它称为由等价关系R诱导出来的A的划分，记作π_R.

上面的定理说明由A上的等价关系R可以诱导出A的一个划分．下面考虑，由A的一个划分如何诱导出A上的一个等价关系.

定理：对非空集合A的一个划分π，令A上的关系R_π为

$$R_\pi = \{\langle x, y\rangle | (\exists z)(z \in \pi \wedge x \in z \wedge y \in z)\}$$

则R_π为A上的等价关系，它称为划分π诱导出的A上的等价关系.

偏序关系

- 在实数之间的小于等于关系
- 在集合之间的包含关系

都具有自反性、反对称性和传递性．下面把具有这三种性质的关系称为“偏序关系”.

定义：对偏序集$\langle A,\leq\rangle$，对任意的$x,y\in A$，若有$x\leq y$或$y\leq x$，则称x和y是可比的.

定义：对偏序集$\langle A,\leq\rangle$，如果对任意的$x,y\in A$，x和y都可比，则称$\leq$为A上的“全序关系”，或称“线序关系”，并称$\langle A,\leq\rangle$为“全序集”.

定义：对偏序集$\langle A, \leq\rangle$，对任意的$x, y \in A$，若有$x \leq y$或$y \leq x$，则称x和y是可比的.

定义：对偏序集$\langle A, \leq\rangle$，如果对任意的$x, y \in A$，x和y都可比，则称$\leq$为A上的"全序关系"，或称"线序关系"，并称$\langle A, \leq\rangle$为"全序集".

定义：对偏序集$\langle A, \leq \rangle$，对任意的$x, y \in A$，若有$x \leq y$或$y \leq x$，则称x和y是可比的.

定义：对偏序集$\langle A, \leq \rangle$，如果对任意的$x, y \in A$，x和y都可比，则称$\leq$为A上的“全序关系”，或称“线序关系”，并称$\langle A, \leq \rangle$为“全序集”.

函数

定义：对于集合A到集合B的二元关系f，对任意的$\langle x, y\rangle \in R$，称$y$为$x$的象；称$x$为$y$的原象；若二元关系$f$满足：

(1) 象的存在性： 对于集合A中每一个元素x，都存在一个象y使$\langle x, y\rangle \in f$。即$(\forall x)(x \in A \rightarrow (\exists y)(y \in B \wedge \langle x, y\rangle \in f))$

(2) 象的惟一性(函数的单值性)：对于集合A中每一个元素x，都存在惟一的一个象y。

$$(\forall x)(\forall y_1)(\forall y_2)((\langle x, y_1\rangle \in f) \wedge (\langle x, y_2\rangle \in f) \rightarrow (y_1 = y_2))$$

则称f是从A到B的函数，记为$f : A \rightarrow B$ 或$y = f(x)$。

函数

定义：对于集合A到集合B的二元关系f，对任意的$\langle x, y\rangle \in R$，称$y$为$x$的象；称$x$为$y$的原象；若二元关系$f$满足：

(1) 象的存在性： 对于集合A中每一个元素x，都存在一个象y使$\langle x, y\rangle \in f$。即$(\forall x)(x \in A \to (\exists y)(y \in B \wedge \langle x, y\rangle \in f))$

(2) 象的惟一性(函数的单值性)：对于集合A中每一个元素x，都存在惟一的一个象y。

$(\forall x)(\forall y_1)(\forall y_2)((\langle x, y_1\rangle \in f) \wedge (\langle x, y_2\rangle \in f) \to (y_1 = y_2))$

则称f是从A到B的函数，记为$f : A \to B$ 或$y = f(x)$。

函数

定义：对于集合A到集合B的二元关系f，对任意的$\langle x, y\rangle \in R$，称$y$为$x$的象；称$x$为$y$的原象；若二元关系$f$满足：

(1) 象的存在性： 对于集合A中每一个元素x，都存在一个象y使$\langle x, y\rangle \in f$。即$(\forall x)(x \in A \to (\exists y)(y \in B \wedge \langle x, y\rangle \in f))$

(2) 象的惟一性(函数的单值性)：对于集合A中每一个元素x，都存在惟一的一个象y。

$$(\forall x)(\forall y_1)(\forall y_2)((\langle x, y_1\rangle \in f) \wedge (\langle x, y_2\rangle \in f) \to (y_1 = y_2))$$

则称f是从A到B的函数，记为$f : A \to B$ 或$y = f(x)$。

函数

定义：对于集合A到集合B的二元关系f，对任意的$\langle x,y\rangle \in R$，称y为x的象；称x为y的原象；若二元关系f满足：

(1) 象的存在性： 对于集合A中每一个元素x，都存在一个象y使$\langle x,y\rangle \in f$。即$(\forall x)(x \in A \to (\exists y)(y \in B \wedge \langle x,y\rangle \in f))$

(2) 象的惟一性(函数的单值性)：对于集合A中每一个元素x，都存在惟一的一个象y。

$$(\forall x)(\forall y_1)(\forall y_2)((\langle x,y_1\rangle \in f) \wedge (\langle x,y_2\rangle \in f) \to (y_1 = y_2))$$

则称f是从A到B的函数，记为$f: A \to B$ 或$y = f(x)$。

定义：设$f : A \to B$是一个函数，

(1) 若$ran(f) = B$，则称f是**满射**的，或称f是A到B上的；

- $(\forall y)(y \in B \to (\exists x)(y = f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1, x_2 \in A$，$x_1 \neq x_2$，都有$f(x_1) \neq f(x_2)$，则称f是**单射**的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是**双射**的，或一对一A到B上的.

定义：设$f: A \to B$是一个函数，

(1) 若$ran(f) = B$，则称f是**满射**的，或称f是A到B上的；

- $(\forall y)(y \in B \to (\exists x)(y = f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1, x_2 \in A$，$x_1 \neq x_2$，都有$f(x_1) \neq f(x_2)$，则称f是**单射**的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是**双射**的，或一对一A到B上的.

定义：设$f:A\rightarrow B$是一个函数，

(1) 若$ran(f)=B$，则称f是**满射**的，或称f是A到B上的；

- $(\forall y)(y\in B\rightarrow(\exists x)(y=f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1,x_2\in A$，$x_1\neq x_2$，都有$f(x_1)\neq f(x_2)$，则称f是**单射**的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1\in A\wedge x_2\in A\wedge x_1\neq x_2\rightarrow f(x_1)\neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是**双射**的，或一对一A到B上的.

定义：设$f: A \to B$是一个函数，

(1) 若$ran(f) = B$，则称f是**满射**的，或称f是A到B上的；

- $(\forall y)(y \in B \to (\exists x)(y = f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1, x_2 \in A$，$x_1 \neq x_2$，都有$f(x_1) \neq f(x_2)$，则称f是**单射**的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1 \in A \land x_2 \in A \land x_1 \neq x_2 \to f(x_1) \neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是**双射**的，或一对一A到B上的.

定义：设$f : A \to B$是一个函数，

(1) 若$ran(f) = B$，则称f是满射的，或称f是A到B上的；

- $(\forall y)(y \in B \to (\exists x)(y = f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1, x_2 \in A$，$x_1 \neq x_2$，都有$f(x_1) \neq f(x_2)$，则称f是单射的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是双射的，或一对一A到B上的.

定义：设$f: A \to B$是一个函数，

(1) 若$ran(f) = B$，则称f是**满射**的，或称f是A到B上的；

- $(\forall y)(y \in B \to (\exists x)(y = f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1, x_2 \in A$，$x_1 \neq x_2$，都有$f(x_1) \neq f(x_2)$，则称f是**单射**的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是**双射**的，或一对一A到B上的.

定义：设$f : A \to B$是一个函数，

(1) 若$ran(f) = B$，则称f是**满射**的，或称f是A到B上的；

- $(\forall y)(y \in B \to (\exists x)(y = f(x)))$
- B中任意的元素y都有原象。

(2) 若对任意的$x_1, x_2 \in A$，$x_1 \neq x_2$，都有$f(x_1) \neq f(x_2)$，则称f是**单射**的，或内射的，或一对一的；

- $(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2))$
- 对值域$ran(f)$里的任意的元素y都存在唯一的原象。

(3) 若f是满射的又是单射的，则称f是**双射**的，或一对一A到B上的.

函数是特殊的关系，所以关于关系合成与关系的逆的定理，都适用于函数．下面讨论函数的一些特殊性质．

定理 设$g:A\to B$，$f:B\to C$，则

(1) $f\circ g$是函数$f\circ g:A\to C$，

(2) 对任意的$x\in A$，有$(f\circ g)(x)=f(g(x))$

函数是特殊的关系，所以关于关系合成与关系的逆的定理，都适用于函数．下面讨论函数的一些特殊性质．

定理 设$g : A \to B$，$f : B \to C$，则

(1) $f \circ g$是函数$f \circ g : A \to C$，

(2) 对任意的$x \in A$，有$(f \circ g)(x) = f(g(x))$

函数是特殊的关系，所以关于关系合成与关系的逆的定理，都适用于函数．下面讨论函数的一些特殊性质．

定理 设$g : A \to B$，$f : B \to C$，则

(1) $f \circ g$是函数$f \circ g : A \to C$，

(2) 对任意的$x \in A$，有$(f \circ g)(x) = f(g(x))$

Groups 群

Definition 10.1 (Group 群)

A group is a nonempty set G on which is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** If a and b belong to G, then $a \cdot b$ is also in G;
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;
- **Identity:** There is an element 1 in G such that $a \cdot 1 = 1 \cdot a = a$ for all a in G;
- **Inverse:** If a is in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 10.2 (Abelian Group 可交换群/阿贝尔群)

A group $(G, \cdot)$, or G for simplicity, is abelian if the binary operation is commutative.
I.e., $a \cdot b = b \cdot a$ for all a, b in G.

Groups 群

Definition 10.1 (Group 群)

A group is a nonempty set G on which is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** If a and b belong to G, then $a \cdot b$ is also in G;
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;
- **Identity:** There is an element 1 in G such that $a \cdot 1 = 1 \cdot a = a$ for all a in G;
- **Inverse:** If a is in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 10.2 (Abelian Group 可交换群/阿贝尔群)

A group $(G, \cdot)$, or G for simplicity, is abelian if the binary operation is commutative.
I.e., $a \cdot b = b \cdot a$ for all a, b in G.

Groups 群

Definition 10.1 (Group 群)

A group is a nonempty set G on which is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** If a and b belong to G, then $a \cdot b$ is also in G;
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;
- **Identity:** There is an element 1 in G such that $a \cdot 1 = 1 \cdot a = a$ for all a in G;
- **Inverse:** If a is in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 10.2 (Abelian Group 可交换群/阿贝尔群)

A group $(G, \cdot)$, or G for simplicity, is abelian if the binary operation is commutative.
I.e., $a \cdot b = b \cdot a$ for all a, b in G.

Groups 群

Definition 10.1 (Group 群)

A group is a nonempty set G on which is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** If a and b belong to G, then $a \cdot b$ is also in G;
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;
- **Identity:** There is an element 1 in G such that $a \cdot 1 = 1 \cdot a = a$ for all a in G;
- **Inverse:** If a is in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 10.2 (Abelian Group 可交换群/阿贝尔群)

A group $(G, \cdot)$, or G for simplicity, is abelian if the binary operation is commutative.
I.e., $a \cdot b = b \cdot a$ for all a, b in G.

Groups 群

Definition 10.1 (Group 群)

A group is a nonempty set G on which is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** If a and b belong to G, then $a \cdot b$ is also in G;
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;
- **Identity:** There is an element 1 in G such that $a \cdot 1 = 1 \cdot a = a$ for all a in G;
- **Inverse:** If a is in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 10.2 (Abelian Group 可交换群/阿贝尔群)

A group $(G, \cdot)$, or G for simplicity, is abelian if the binary operation is commutative.
I.e., $a \cdot b = b \cdot a$ for all a, b in G.

Groups 群

Definition 10.1 (Group 群)

A group is a nonempty set G on which is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** If a and b belong to G, then $a \cdot b$ is also in G;
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;
- **Identity:** There is an element 1 in G such that $a \cdot 1 = 1 \cdot a = a$ for all a in G;
- **Inverse:** If a is in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Definition 10.2 (Abelian Group 可交换群/阿贝尔群)

A group $(G, \cdot)$, or G for simplicity, is abelian if the binary operation is commutative.
I.e., $a \cdot b = b \cdot a$ for all a, b in G.

Example 10.3

- **abelian groups:** $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{Z}_m,+)$, $(\mathbb{Z}_p^*,\times)$.
  复数域$\mathbb{C}$上的n次单位元根与复数乘法运算构成一个具有n个元素交换群U_n。

$$\begin{aligned} U_n &= \{x \mid x^n = 1, x \in \mathbb{C}\} \\ &= \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}) \mid k = 0, 1, \ldots, n-1\right\} \end{aligned}$$

- **non abelian groups:**
  - $GL_n(\mathbb{Q})$和矩阵乘法：$\mathbb{Q}$上n阶非退化矩阵与矩阵乘法。

Example 10.3

- **abelian groups:** $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{Z}_m,+)$, $(\mathbb{Z}_p^*,\times)$.
  复数域$\mathbb{C}$上的n次单位元根与复数乘法运算构成一个具有n个元素交换群U_n。

$$
\begin{aligned}
U_n &= \{x \mid x^n = 1, x \in \mathbb{C}\} \\
&= \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}) \mid k = 0, 1, \ldots, n-1\right\}
\end{aligned}
$$

- **non abelian groups:**
  - $GL_n(\mathbb{Q})$和矩阵乘法：$\mathbb{Q}$上n阶非退化矩阵与矩阵乘法。

Elementary Properties of Groups

Lemma 10.4

The identity is unique.

Proof. If 1 and $1'$ are both identity, then we have $1' = 1'1 = 1$.

Lemma 10.5

The inverse of any given element is unique.

Proof. For an element $a \in G$, if b and b' are inverses of a then

$$b = 1b = (b'a)b = b'(ab) = b'1 = b'.$$

总结：群的单位元以及任何元素的逆元具有惟一性。
$\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$。
消去律成立。

Elementary Properties of Groups

Lemma 10.4

The identity is unique.

Proof. If 1 and $1'$ are both identity, then we have $1' = 1'1 = 1$.

Lemma 10.5

The inverse of any given element is unique.

Proof. For an element $a \in G$, if b and b' are inverses of a then

$$b = 1b = (b'a)b = b'(ab) = b'1 = b'.$$

总结：群的单位元以及任何元素的逆元具有惟一性。
$\forall a, b \in G$，$(ab)^{-1} = b^{-1}a^{-1}$。
消去律成立。

Elementary Properties of Groups

Lemma 10.4

The identity is unique.

Proof. If 1 and $1'$ are both identity, then we have $1' = 1'1 = 1$.

Lemma 10.5

The inverse of any given element is unique.

Proof. For an element $a \in G$, if b and b' are inverses of a then

$$b = 1b = (b'a)b = b'(ab) = b'1 = b'.$$

总结：群的单位元以及任何元素的逆元具有惟一性。
$\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$。
消去律成立。

Elementary Properties of Groups

Lemma 10.4

The identity is unique.

Proof. If 1 and $1'$ are both identity, then we have $1' = 1'1 = 1$.

Lemma 10.5

The inverse of any given element is unique.

Proof. For an element $a \in G$, if b and b' are inverses of a then

$$b = 1b = (b'a)b = b'(ab) = b'1 = b'.$$

总结：群的单位元以及任何元素的逆元具有惟一性。
$\forall a, b \in G$，$(ab)^{-1} = b^{-1}a^{-1}$。
消去律成立。

Elementary Properties of Groups

Lemma 10.4

The identity is unique.

Proof. If 1 and $1'$ are both identity, then we have $1' = 1'1 = 1$.

Lemma 10.5

The inverse of any given element is unique.

Proof. For an element $a \in G$, if b and b' are inverses of a then

$$b = 1b = (b'a)b = b'(ab) = b'1 = b'.$$

总结：群的单位元以及任何元素的逆元具有惟一性。
$\forall a, b \in G$，$(ab)^{-1} = b^{-1}a^{-1}$。
消去律成立。

Other Definitions for Groups

Theorem 10.6

群的等价定义1：A nonempty set G on which there is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- **Closure:** *If a and b belong to G, then $a \cdot b$ is also in G;*
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all $a, b, c \in G$;*
- **Left Identity:** *There is an element 1_ℓ in G such that $1_\ell \cdot a = a$ for all a in G;*
- **Left Inverse:** *for all $a \in G$ there is an element a_ℓ^{-1} in G such that $a_\ell^{-1} \cdot a = 1_\ell$.*

Then $(G, \cdot)$ is a group.

Other Definitions for Groups

Theorem 10.6

群的等价定义1：A nonempty set G on which there is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- ***Closure:*** *If a and b belong to G, then $a \cdot b$ is also in G;*
- ***Associativity:*** *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;*
- ***Left Identity:*** *There is an element 1_ℓ in G such that $1_\ell \cdot a = a$ for all a in G;*
- ***Left Inverse:*** *for all $a \in G$ there is an element a_ℓ^{-1} in G such that $a_\ell^{-1} \cdot a = 1_\ell$.*

Then $(G, \cdot)$ is a group.

Other Definitions for Groups

Theorem 10.6

群的等价定义1：A nonempty set G on which there is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- ***Closure:*** *If a and b belong to G, then $a \cdot b$ is also in G;*
- ***Associativity:*** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all $a, b, c \in G$;*
- ***Left Identity:*** *There is an element 1_ℓ in G such that $1_\ell \cdot a = a$ for all a in G;*
- ***Left Inverse:*** *for all $a \in G$ there is an element a_ℓ^{-1} in G such that $a_\ell^{-1} \cdot a = 1_\ell$.*

Then $(G, \cdot)$ is a group.

Other Definitions for Groups

Theorem 10.6

群的等价定义1：A nonempty set G on which there is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- ***Closure:*** *If a and b belong to G, then $a \cdot b$ is also in G;*
- ***Associativity:*** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all $a, b, c \in G$;*
- ***Left Identity:*** *There is an element 1_ℓ in G such that $1_\ell \cdot a = a$ for all a in G;*
- ***Left Inverse:*** *for all $a \in G$ there is an element a_ℓ^{-1} in G such that $a_\ell^{-1} \cdot a = 1_\ell$.*

Then $(G, \cdot)$ is a group.

Other Definitions for Groups

Theorem 10.6

群的等价定义1：A nonempty set G on which there is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- ***Closure:*** *If a and b belong to G, then $a \cdot b$ is also in G;*
- ***Associativity:*** *$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$;*
- ***Left Identity:*** *There is an element 1_ℓ in G such that $1_\ell \cdot a = a$ for all a in G;*
- ***Left Inverse:*** *for all $a \in G$ there is an element a_ℓ^{-1} in G such that $a_\ell^{-1} \cdot a = 1_\ell$.*

Then $(G, \cdot)$ is a group.

Other Definitions for Groups

Theorem 10.6

群的等价定义1：A nonempty set G on which there is defined a binary operation $(a, b) \mapsto a \cdot b$ satisfying the following properties:

- ***Closure:*** *If a and b belong to G, then $a \cdot b$ is also in G;*
- ***Associativity:*** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all $a, b, c \in G$;*
- ***Left Identity:*** *There is an element 1_ℓ in G such that $1_\ell \cdot a = a$ for all a in G;*
- ***Left Inverse:*** *for all $a \in G$ there is an element a_ℓ^{-1} in G such that $a_\ell^{-1} \cdot a = 1_\ell$.*

Then $(G, \cdot)$ is a group.

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 对于任意$a,b\in G$，方程$ax=b$和$ya=b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 左消去律：对于任意$a,a_i,a_j\in G$，如果$a\cdot a_i=a\cdot a_j$，则有$a_i=a_j$。
- 右消去律：对于任意$a,a_i,a_j\in G$，如果$a_i\cdot a=a_j\cdot a$，则有$a_i=a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- ***Closure:*** 任意$a,b\in G$有$a\cdot b\in G$；
- ***Associativity:*** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 对于任意$a,b\in G$，方程$ax=b$和$ya=b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- ***Closure:*** 任意$a,b\in G$有$a\cdot b\in G$；
- ***Associativity:*** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 左消去律：对于任意$a,a_i,a_j\in G$，如果$a\cdot a_i=a\cdot a_j$，则有$a_i=a_j$。
- 右消去律：对于任意$a,a_i,a_j\in G$，如果$a_i\cdot a=a_j\cdot a$，则有$a_i=a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 对于任意$a,b\in G$，方程$ax=b$和$ya=b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 左消去律：对于任意$a,a_i,a_j\in G$，如果$a\cdot a_i=a\cdot a_j$，则有$a_i=a_j$。
- 右消去律：对于任意$a,a_i,a_j\in G$，如果$a_i\cdot a=a_j\cdot a$，则有$a_i=a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- ***Closure:*** 任意$a,b \in G$有$a \cdot b \in G$；
- ***Associativity:*** 对于任意的$a,b,c \in G$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$；
- 对于任意$a,b \in G$，方程$ax = b$和$ya = b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- ***Closure:*** 任意$a,b \in G$有$a \cdot b \in G$；
- ***Associativity:*** 对于任意的$a,b,c \in G$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$；
- 左消去律：对于任意$a,a_i,a_j \in G$，如果$a \cdot a_i = a \cdot a_j$，则有$a_i = a_j$。
- 右消去律：对于任意$a,a_i,a_j \in G$，如果$a_i \cdot a = a_j \cdot a$，则有$a_i = a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 对于任意$a,b\in G$，方程$ax=b$和$ya=b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 左消去律：对于任意$a,a_i,a_j\in G$，如果$a\cdot a_i=a\cdot a_j$，则有$a_i=a_j$。
- 右消去律：对于任意$a,a_i,a_j\in G$，如果$a_i\cdot a=a_j\cdot a$，则有$a_i=a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 对于任意$a,b\in G$，方程$ax=b$和$ya=b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 左消去律：对于任意$a,a_i,a_j\in G$，如果$a\cdot a_i=a\cdot a_j$，则有$a_i=a_j$。
- 右消去律：对于任意$a,a_i,a_j\in G$，如果$a_i\cdot a=a_j\cdot a$，则有$a_i=a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 对于任意$a,b\in G$，方程$ax=b$和$ya=b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a,b\in G$有$a\cdot b\in G$；
- **Associativity:** 对于任意的$a,b,c\in G$，有$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；
- 左消去律：对于任意$a,a_i,a_j\in G$，如果$a\cdot a_i=a\cdot a_j$，则有$a_i=a_j$。
- 右消去律：对于任意$a,a_i,a_j\in G$，如果$a_i\cdot a=a_j\cdot a$，则有$a_i=a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a, b \in G$有$a \cdot b \in G$；
- **Associativity:** 对于任意的$a, b, c \in G$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$；
- 对于任意$a, b \in G$，方程$ax = b$和$ya = b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G,\cdot)$是群的充分必要条件是：

- **Closure:** 任意$a, b \in G$有$a \cdot b \in G$；
- **Associativity:** 对于任意的$a, b, c \in G$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$；
- 左消去律：对于任意$a, a_i, a_j \in G$，如果$a \cdot a_i = a \cdot a_j$，则有$a_i = a_j$。
- 右消去律：对于任意$a, a_i, a_j \in G$，如果$a_i \cdot a = a_j \cdot a$，则有$a_i = a_j$。

Other Definitions for Groups

Theorem 10.7

群的等价定义2：设G是一个非空集合，则$(G, \cdot)$是群的充分必要条件是：

- **Closure:** 任意$a, b \in G$有$a \cdot b \in G$；
- **Associativity:** 对于任意的$a, b, c \in G$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$；
- 对于任意$a, b \in G$，方程$ax = b$和$ya = b$在中有解。

Theorem 10.8

有限群的等价定义：设G是一个有限非空集合，则$(G, \cdot)$是群的充分必要条件是：

- **Closure:** 任意$a, b \in G$有$a \cdot b \in G$；
- **Associativity:** 对于任意的$a, b, c \in G$，有$a \cdot (b \cdot c) = (a \cdot b) \cdot c$；
- 左消去律：对于任意$a, a_i, a_j \in G$，如果$a \cdot a_i = a \cdot a_j$，则有$a_i = a_j$。
- 右消去律：对于任意$a, a_i, a_j \in G$，如果$a_i \cdot a = a_j \cdot a$，则有$a_i = a_j$。

设G是一个无限非空集合，即使二元运算“$\circ$”满足“封闭性”，“结合律”，“左消去律”，“右消去律”，$(G, \circ)$也不一定是群。例如:

- $(\mathbb{N}, +)$不是群；$(\mathbb{Z}^*, \cdot)$不是群；$(\mathbb{Z}^+, \cdot)$不是群；

原因：$f_a : G \to G; f_a : a_i \mapsto a \circ a_i (a_i \circ a)$可能不是双射，导致上述的证明不能使用。

Lemma 10.9

Let a and b be elements of G, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = b1b^{-1} = bb^{-1} = 1$.

Lemma 10.10

Let $a \in G$. Then $a^{m+n} = a^m a^n$ and $a^{mn} = (a^m)^n$ for all integers m and n.

设G是一个无限非空集合，即使二元运算“$\circ$”满足“封闭性”，“结合律”, “左消去律”, “右消去律”，$(G, \circ)$也不一定是群。例如:

- $(\mathbb{N}, +)$不是群；$(\mathbb{Z}^*, \cdot)$不是群；$(\mathbb{Z}^+, \cdot)$不是群；

原因：$f_a : G \to G; f_a : a_i \mapsto a \circ a_i (a_i \circ a)$可能不是双射，导致上述的证明不能使用。

Lemma 10.9

Let a and b be elements of G, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = b1b^{-1} = bb^{-1} = 1$.

Lemma 10.10

Let $a \in G$. Then $a^{m+n} = a^m a^n$ and $a^{mn} = (a^m)^n$ for all integers m and n.

设G是一个无限非空集合，即使二元运算"$\circ$"满足"封闭性"，"结合律","左消去律","右消去律"，$(G,\circ)$也不一定是群。例如:

- $(\mathbb{N},+)$不是群；$(\mathbb{Z}^*,\cdot)$不是群；$(\mathbb{Z}^+,\cdot)$不是群；

原因：$f_a : G \to G; f_a : a_i \mapsto a \circ a_i (a_i \circ a)$可能不是双射，导致上述的证明不能使用。

Lemma 10.9

Let a and b be elements of G, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = b1b^{-1} = bb^{-1} = 1$.

Lemma 10.10

Let $a \in G$. Then $a^{m+n} = a^m a^n$ and $a^{mn} = (a^m)^n$ for all integers m and n.

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- ⇔(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- ⇔ $\forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- $\Leftrightarrow$(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- $\Leftrightarrow \forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- $\Leftrightarrow$(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- $\Leftrightarrow \forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- $\Leftrightarrow$(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- $\Leftrightarrow \forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- $\Leftrightarrow$(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- $\Leftrightarrow \forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- $\Leftrightarrow$(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- $\Leftrightarrow \forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Subgroups

Definition 10.11 (subgroup)

- A subgroup H of a group G is a nonempty subset of G that forms a group under the binary operation of G.
- Equivalently, H is a nonempty subset of G such that if a and b belong to H, so does ab^{-1}.
- A subgroup H of G is said to be proper if $H \neq G$.
- If H is a subgroup of G, we denote $H \leq G$. If H is a proper subgroup, we denote $H < G$.

群H是群G的子群的两个等价定义：

- $\Leftrightarrow$(1) $HH \subseteq H$；(2) $H^{-1} \subseteq H$；
- $\Leftrightarrow \forall a, b \in H, ab^{-1} \in H$。

群G中必存在两个子群：$\{1\}$和G，这两个群称为平凡子群。

Examples of Subgroups

例：设$M_n(\mathbb{R})$表示实数域上的n阶方阵集合，$GL_n(\mathbb{R})$表示所有n阶可逆矩阵构成的乘法群，则

$$SL_n(\mathbb{R}) := \{A \mid \det(A) = 1, A \in M_n(\mathbb{R})\}$$

是$GL_n(\mathbb{R})$的一个子群。

例：设G为群，定义

$$C(G) := \{g \mid gx = xg, x \in G\}.$$

则$C(G)$是G的子群。

例：$n\mathbb{Z} \leq \mathbb{Z}$ for $n \in \mathbb{N}$.

Examples of Subgroups

例：设$M_n(\mathbb{R})$表示实数域上的n阶方阵集合，$GL_n(\mathbb{R})$表示所有n阶可逆矩阵构成的乘法群，则

$$SL_n(\mathbb{R}) := \{A \mid \det(A) = 1, A \in M_n(\mathbb{R})\}$$

是$GL_n(\mathbb{R})$的一个子群。

例：设G为群，定义

$$C(G) := \{g \mid gx = xg, x \in G\}.$$

则$C(G)$是G的子群。

例：$n\mathbb{Z} \leq \mathbb{Z}$ for $n \in \mathbb{N}$.

Examples of Subgroups

例：设$M_n(\mathbb{R})$表示实数域上的n阶方阵集合，$GL_n(\mathbb{R})$表示所有n阶可逆矩阵构成的乘法群，则

$$SL_n(\mathbb{R}) := \{A \mid \det(A) = 1, A \in M_n(\mathbb{R})\}$$

是$GL_n(\mathbb{R})$的一个子群。

例：设G为群，定义

$$C(G) := \{g \mid gx = xg, x \in G\}.$$

则$C(G)$是G的子群。

例：$n\mathbb{Z} \leq \mathbb{Z}$ for $n \in \mathbb{N}$.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！

  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群!
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群!
- 两个子群的交$H_1 \cap H_2$一定是子群!

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

子群

- 两个子群的并$H_1 \cup H_2$不一定是子群！
  证明：设$h_1 \in H_1 \setminus H_2$，$h_2 \in H_2 \setminus H_1$，则$h_1 h_2 \notin H_1 \cup H_2$，故$H_1 \cup H_2$不是子群！
- 两个子群的交$H_1 \cap H_2$一定是子群！

Lemma 10.12

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

- **Proof: Closure:** if $a, b \in H \cap K$ then $ab \in H$ and $ab \in K$, and therefore $ab \in H \cap K$.
- **Identity:** $1 \in H \cap K$.
- **Inverse:** if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, thus $a^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G, as required.

Definition 10.13 (isomorphic 同构)

The groups $(G_1, \cdot)$ and $(G_2, \circ)$ are said to be isomorphic if there is a bijection $f : G_1 \mapsto G_2$ such that $f(a \cdot b) = f(a) \circ f(b)$.
Isomorphic groups are essentially the same and differ only notationally.

Example. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$;

Example. $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$;

Fact 10.14

- *Let $(G_1, \cdot) \cong (G_2, \circ)$ with isomorphic bijection $f : G_1 \mapsto G_2$, then $f(e_1) = e_2$, and $f(a^{-1}) = f(a)^{-1}$.*

Definition 10.13 (isomorphic 同构)

The groups $(G_1, \cdot)$ and $(G_2, \circ)$ are said to be isomorphic if there is a bijection $f : G_1 \mapsto G_2$ such that $f(a \cdot b) = f(a) \circ f(b)$.
Isomorphic groups are essentially the same and differ only notationally.

Example. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$;

Example. $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$;

Fact 10.14

- *Let $(G_1, \cdot) \cong (G_2, \circ)$ with isomorphic bijection $f : G_1 \mapsto G_2$, then $f(e_1) = e_2$, and $f(a^{-1}) = f(a)^{-1}$.*

Definition 10.13 (isomorphic 同构)

The groups $(G_1, \cdot)$ and $(G_2, \circ)$ are said to be isomorphic if there is a bijection $f : G_1 \mapsto G_2$ such that $f(a \cdot b) = f(a) \circ f(b)$.
Isomorphic groups are essentially the same and differ only notationally.

Example. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$;

Example. $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$;

Fact 10.14

- *Let* $(G_1, \cdot) \cong (G_2, \circ)$ *with isomorphic bijection* $f : G_1 \mapsto G_2$, *then* $f(e_1) = e_2$, *and* $f(a^{-1}) = f(a)^{-1}$.

Definition 10.13 (isomorphic 同构)

The groups $(G_1, \cdot)$ and $(G_2, \circ)$ are said to be isomorphic if there is a bijection $f : G_1 \mapsto G_2$ such that $f(a \cdot b) = f(a) \circ f(b)$.
Isomorphic groups are essentially the same and differ only notationally.

Example. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$;

Example. $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$;

Fact 10.14

- *Let* $(G_1, \cdot) \cong (G_2, \circ)$ *with isomorphic bijection* $f : G_1 \mapsto G_2$, *then* $f(e_1) = e_2$, *and* $f(a^{-1}) = f(a)^{-1}$.

Definition 10.13 (isomorphic 同构)

The groups $(G_1, \cdot)$ and $(G_2, \circ)$ are said to be isomorphic if there is a bijection $f : G_1 \mapsto G_2$ such that $f(a \cdot b) = f(a) \circ f(b)$.
Isomorphic groups are essentially the same and differ only notationally.

Example. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$;

Example. $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$;

Fact 10.14

- *Let* $(G_1, \cdot) \cong (G_2, \circ)$ *with isomorphic bijection* $f : G_1 \mapsto G_2$*, then* $f(e_1) = e_2$*, and* $f(a^{-1}) = f(a)^{-1}$.

Definition 10.13 (isomorphic 同构)

The groups $(G_1, \cdot)$ and $(G_2, \circ)$ are said to be isomorphic if there is a bijection $f : G_1 \mapsto G_2$ such that $f(a \cdot b) = f(a) \circ f(b)$.
Isomorphic groups are essentially the same and differ only notationally.

Example. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$;

Example. $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$;

Fact 10.14

- *Let $(G_1, \cdot) \cong (G_2, \circ)$ with isomorphic bijection $f : G_1 \mapsto G_2$, then $f(e_1) = e_2$, and $f(a^{-1}) = f(a)^{-1}$.*

群中的集合所生成的子群

Definition 10.15

A是群G的非空集合。$<A>=\bigcap_{i\in I}H_i$，其中$H_i, i\in I$, 是群G中含A的所有子群。则称$<A>$是集合A生成的子群，称A为$<A>$的生成元集。

- **subgroup generated by** A If A is any non-empty subset of a group G, the subgroup generated by A is the smallest subgroup containing A, often denoted by $<A>$. 非空集合A在群G中生成的子群$<A>$是G中所有包含A的最小的群。
- 若$H=<A>$，则称集合A是群H的生成元集。
- $<A>=\{x_1x_2\cdots x_n \mid n\in\mathbb{N}, x_i\in A\cup A^{-1}\}$。

群中的集合所生成的子群

Definition 10.15

A是群G的非空集合。$< A >= \bigcap_{i \in I} H_i$，其中$H_i, i \in I$, 是群$G$中含$A$的所有子群。则称$< A >$是集合$A$生成的子群，称$A$为$< A >$的生成元集。

- **subgroup generated by A** If A is any non-empty subset of a group G, the subgroup generated by A is the smallest subgroup containing A, often denoted by $< A >$. 非空集合A在群G中生成的子群$< A >$是G中所有包含A的最小的群。
- 若$H =< A >$，则称集合A是群H的生成元集。
- $< A >= \{x_1 x_2 \cdots x_n | n \in \mathbb{N}, x_i \in A \cup A^{-1}\}$。

群中的集合所生成的子群

Definition 10.15

A是群G的非空集合。$< A >= \bigcap_{i\in I} H_i$，其中$H_i, i \in I$, 是群$G$中含$A$的所有子群。则称$< A >$是集合$A$生成的子群，称$A$为$< A >$的生成元集。

- **subgroup generated by A** If A is any non-empty subset of a group G, the subgroup generated by A is the smallest subgroup containing A, often denoted by $< A >$. 非空集合A在群G中生成的子群$< A >$是G中所有包含A的最小的群。
- 若$H =< A >$，则称集合A是群H的生成元集。
- $< A >= \{x_1 x_2 \cdots x_n | n \in \mathbb{N}, x_i \in A \cup A^{-1}\}$。

群中的集合所生成的子群

Definition 10.15

A是群G的非空集合。$< A >= \bigcap_{i\in I} H_i$，其中$H_i, i \in I$, 是群$G$中含$A$的所有子群。则称$< A >$是集合$A$生成的子群，称$A$为$< A >$的生成元集。

- **subgroup generated by** A If A is any non-empty subset of a group G, the subgroup generated by A is the smallest subgroup containing A, often denoted by $< A >$. 非空集合A在群G中生成的子群$< A >$是G中所有包含A的最小的群。
- 若$H =< A >$，则称集合A是群H的生成元集。
- $< A >= \{x_1 x_2 \cdots x_n | n \in \mathbb{N}, x_i \in A \cup A^{-1}\}$。

如果$A = \{a\}$，则$< a >= \{a^r \mid r \in \mathbb{Z}\}$。

如果$A = \{a, b\}$且$ab = ba$，则$< a, b >= \{a^m b^n \mid m, n \in \mathbb{Z}\}$。

如果$A = \{a\}$，则$< a >= \{a^r \mid r \in \mathbb{Z}\}$。

如果$A = \{a, b\}$且$ab = ba$，则$< a, b >= \{a^m b^n \mid m, n \in \mathbb{Z}\}$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H =< a >$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H = < a >$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H =< a >$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H = < a >$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H =< a >$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H =< a >$。

Lemma 10.16

Let $a \in G$. Then the set of all elements of G that are of the form a^n for some integer n is a subgroup of G.

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$

- **Closure:** if $a^m, a^n \in H$, then $a^m a^n = a^{m+n} \in H$.
- **Identity:** $1 = a^0 \in H$.
- **Inverse:** $(a^n)^{-1} = a^{-n} \in H$ for all integers n.

Thus H is a subgroup of G, as required.

$H = \{a^n : n \in \mathbb{Z}\}$是由一个元素$a$生成的子群，即$H = < a >$。

Cyclic Groups

Definition 10.17 (cyclic group)

- A group G is cyclic if G is generated by a single element: $G =< a >$.
- A finite cyclic group generated by a is necessarily abelian, and can be writen as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$.

命题：如果G是一个循环群，则G必有下列形状：

1. $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{N}\}$.
2. $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$，其中$a^n = 1$，而$a^s = a^t, 0 \le s, t \le n-1$，当且仅当$s = t$。

- A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.
- If G is an infinite cyclic group generated by a, then $G \cong \mathbb{Z}$.

Cyclic Groups

Definition 10.17 (cyclic group)

- A group G is cyclic if G is generated by a single element: $G =< a >$.
- A finite cyclic group generated by a is necessarily abelian, and can be writen as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$.

命题：如果G是一个循环群，则G必有下列形状：

1. $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{N}\}$.
2. $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$，其中$a^n = 1$，而$a^s = a^t, 0 \leq s, t \leq n-1$，当且仅当$s = t$。

- A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.
- If G is an infinite cyclic group generated by a, then $G \cong \mathbb{Z}$.

Cyclic Groups

Definition 10.17 (cyclic group)

- A group G is cyclic if G is generated by a single element: $G =< a >$.
- A finite cyclic group generated by a is necessarily abelian, and can be writen as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$.

命题：如果G是一个循环群，则G必有下列形状：

1. $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{N}\}$.
2. $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$，其中$a^n = 1$，而$a^s = a^t, 0 \leq s, t \leq n-1$，当且仅当$s = t$。

- A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.
- If G is an infinite cyclic group generated by a, then $G \cong \mathbb{Z}$.

Cyclic Groups

Definition 10.17 (cyclic group)

- A group G is cyclic if G is generated by a single element: $G =< a >$.
- A finite cyclic group generated by a is necessarily abelian, and can be writen as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$.

命题：如果G是一个循环群，则G必有下列形状：

1. $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{N}\}$.
2. $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$，其中$a^n = 1$，而$a^s = a^t, 0 \leq s, t \leq n-1$，当且仅当$s = t$。

- A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.
- If G is an infinite cyclic group generated by a, then $G \cong \mathbb{Z}$.

Cyclic Groups

Definition 10.17 (cyclic group)

- A group G is cyclic if G is generated by a single element: $G =< a >$.
- A finite cyclic group generated by a is necessarily abelian, and can be writen as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$.

命题：如果G是一个循环群，则G必有下列形状：

1. $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{N}\}$.
2. $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$，其中$a^n = 1$，而$a^s = a^t, 0 \leq s, t \leq n-1$，当且仅当$s = t$。

- A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.
- If G is an infinite cyclic group generated by a, then $G \cong \mathbb{Z}$.

Cyclic Groups

Definition 10.17 (cyclic group)

- A group G is cyclic if G is generated by a single element: $G =< a >$.
- A finite cyclic group generated by a is necessarily abelian, and can be writen as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$.

命题：如果G是一个循环群，则G必有下列形状：

1. $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{N}\}$.
2. $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$，其中$a^n = 1$，而$a^s = a^t, 0 \leq s, t \leq n-1$，当且仅当$s = t$。

- A finite cyclic group with n elements is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n.
- If G is an infinite cyclic group generated by a, then $G \cong \mathbb{Z}$.

循环群和非循环群举例：

- The group $(\mathbb{Z},+)$ is a cyclic group, generated by 1.
- Let n be a positive integer. Then $(\mathbb{Z}_n,+)$ is a cyclic group of order n.
- *Klein 4-group:* $K_4=\{1,a,b,c\}$, with the multiplication table

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

这是阶数最小的非循环群！

Order of an element, Order of a group

Definition 10.18 (order of an element)

The order of an element in a group G (notation $|a|$) is the least positive integer n such that $a^n = 1$.

- if no such integer exists, the order of a is infinite.
- if $|a| = n$, then the cyclic subgroup $< a >$ has n elements.

Definition 10.19 (order of group)

The order of the group G, denoted by $|G|$, is the number of elements.

Lemma 10.20

1. 如果ord$(g) = t$，且$g^m = 1$，则$t|m$；
2. 如果ord$(g) = t$，则ord$(g^s) = t/\gcd(t, s)$；ord(g^s)=ord$(g^{\gcd(t,s)})$
3. 如果ord$(g) = t$，且$\gcd(t, s) = 1$，则ord$(g^s) = t$；
4. ord(g)=ord(g^{-1})；

Order of an element, Order of a group

Definition 10.18 (order of an element)

The order of an element in a group G (notation $|a|$) is the least positive integer n such that $a^n = 1$.

- if no such integer exists, the order of a is infinite.
- if $|a| = n$, then the cyclic subgroup $< a >$ has n elements.

Definition 10.19 (order of group)

The order of the group G, denoted by $|G|$, is the number of elements.

Lemma 10.20

1. 如果ord$(g) = t$，且$g^m = 1$，则$t|m$；
2. 如果ord$(g) = t$，则ord$(g^s) = t/\gcd(t,s)$；ord(g^s)=ord$(g^{\gcd(t,s)})$
3. 如果ord$(g) = t$，且$\gcd(t,s) = 1$，则ord$(g^s) = t$；
4. ord(g)=ord(g^{-1})；

Order of an element, Order of a group

Definition 10.18 (order of an element)

The order of an element in a group G (notation $|a|$) is the least positive integer n such that $a^n = 1$.

- if no such integer exists, the order of a is infinite.
- if $|a| = n$, then the cyclic subgroup $< a >$ has n elements.

Definition 10.19 (order of group)

The order of the group G, denoted by $|G|$, is the number of elements.

Lemma 10.20

1. 如果ord$(g) = t$，且$g^m = 1$，则$t|m$；
2. 如果ord$(g) = t$，则ord$(g^s) = t/\gcd(t, s)$；ord(g^s)=ord$(g^{\gcd(t,s)})$
3. 如果ord$(g) = t$，且$\gcd(t, s) = 1$，则ord$(g^s) = t$；
4. ord(g)=ord(g^{-1})；

循环群

Theorem 10.21 (循环群的性质)

Subgroups of a cyclic group is also cyclic.

Theorem 10.22 (循环群的性质)

Let $G =< a >$.

- *if $|G| = \infty$, the only generator of G is a and a^{-1}. All subgroups of G is*

$$\{< a^d > \mid d = 0, 1, 2, \cdots\}$$

- *if $|G| = n$, then there are $\phi(n)$ generators, and a^r is one of generator iff $\gcd(n, r) = 1$. All subgroups of G is*

$$\{< a^d > \mid 0 \leq d \leq n-1, d|n\}.$$

循环群

Theorem 10.21 (循环群的性质)

Subgroups of a cyclic group is also cyclic.

Theorem 10.22 (循环群的性质)

Let $G =< a >$.

- *if* $|G| = \infty$, *the only generator of* G *is* a *and* a^{-1}. *All subgroups of* G *is*

$$\{< a^d > \mid d = 0, 1, 2, \cdots\}$$

- *if* $|G| = n$, *then there are* $\phi(n)$ *generators, and* a^r *is one of generator iff* $\gcd(n, r) = 1$. *All subgroups of* G *is*

$$\{< a^d > \mid 0 \leq d \leq n - 1, d|n\}.$$

循环群

Theorem 10.21 (循环群的性质)

Subgroups of a cyclic group is also cyclic.

Theorem 10.22 (循环群的性质)

Let $G =< a >$.

- *if* $|G| = \infty$, *the only generator of* G *is* a *and* a^{-1}. *All subgroups of* G *is*

$$\{< a^d > \ | d = 0, 1, 2, \cdots\}$$

- *if* $|G| = n$, *then there are* $\phi(n)$ *generators, and* a^r *is one of generator iff* $\gcd(n, r) = 1$. *All subgroups of* G *is*

$$\{< a^d > \ | 0 \leq d \leq n-1, d|n\}.$$

平面的运动群

Definition 11.1 (非空集合上的可逆变换)

设M是一个非空集合，M上的可逆变换指M到自身的一一对应（即双射）。

Definition 11.2 (平面的运动)

平面P的一个运动是指平面P的一个保距变换。

Theorem 11.3 (平面运动的几何形式，M. Chasles)

平面的运动有且仅有下列三种：

1. *沿任一给定向量的平移；*
2. *以任意点为中心的旋转；*
3. *绕某一直线作翻折后再沿该直线上的一个向量作一平移（包括作纯翻折）。*

平面的运动群

Definition 11.1 (非空集合上的可逆变换)

设M是一个非空集合，M上的可逆变换指M到自身的一一对应（即双射）。

Definition 11.2 (平面的运动)

平面P的一个运动是指平面P的一个保距变换。

Theorem 11.3 (平面运动的几何形式，M. Chasles)

平面的运动有且仅有下列三种：

1. *沿任一给定向量的平移；*
2. *以任意点为中心的旋转；*
3. *绕某一直线作翻折后再沿该直线上的一个向量作一平移（包括作纯翻折）。*

平面的运动群

Definition 11.1 (非空集合上的可逆变换)

设M是一个非空集合，M上的可逆变换指M到自身的一一对应（即双射）。

Definition 11.2 (平面的运动)

平面P的一个运动是指平面P的一个保距变换。

Theorem 11.3 (平面运动的几何形式，M. Chasles)

平面的运动有且仅有下列三种：

1. *沿任一给定向量的平移；*
2. *以任意点为中心的旋转；*
3. *绕某一直线作翻折后再沿该直线上的一个向量作一平移（包括作纯翻折）。*

变换群

Definition 11.4 (变换群)

设M是一个非空集合，$T(M)$是M上的所有可逆变换的全体。定义

$$\circ : T(M) \times T(M) \to T(M)$$

$$(\phi, \psi) \to \phi \circ \psi$$

为变换的合成(乘法)。则$(T(M), \circ)$是一个群，称为集合M的对称群。
集合M的对称群的子群称为集合M的变换群。

1. 对于任意的$\phi, \psi \in T(M)$，有$\phi \circ \psi \in T(M)$；
2. 对于任意的$\phi, \psi, \theta \in T(M)$，有$(\phi \circ \psi) \circ \theta = \phi \circ (\psi \circ \theta)$；
3. 存在$I \in T(M)$使得任意$\phi \in T(M)$，有$I \circ \phi = \phi \circ I = \phi$；
4. 对于任意$\phi \in T(M)$，存在$\phi^{-1} \in T(M)$，使得$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = I$。

变换群

Definition 11.4 (变换群)

设M是一个非空集合，$T(M)$是M上的所有可逆变换的全体。定义

$$\circ : T(M) \times T(M) \to T(M)$$

$$(\phi, \psi) \to \phi \circ \psi$$

为变换的合成(乘法)。则$(T(M), \circ)$是一个群，称为集合M的对称群。
集合M的对称群的子群称为集合M的变换群。

1. 对于任意的$\phi, \psi \in T(M)$，有$\phi \circ \psi \in T(M)$；
2. 对于任意的$\phi, \psi, \theta \in T(M)$，有$(\phi \circ \psi) \circ \theta = \phi \circ (\psi \circ \theta)$；
3. 存在$I \in T(M)$使得任意$\phi \in T(M)$，有$I \circ \phi = \phi \circ I = \phi$；
4. 对于任意$\phi \in T(M)$，存在$\phi^{-1} \in T(M)$，使得$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = I$。

变换群

Definition 11.4 (变换群)

设M是一个非空集合，$T(M)$是M上的所有可逆变换的全体。定义

$$\circ : T(M) \times T(M) \to T(M)$$

$$(\phi, \psi) \to \phi \circ \psi$$

为变换的合成(乘法)。则$(T(M), \circ)$是一个群，称为集合M的对称群。集合M的对称群的子群称为集合M的变换群。

1. 对于任意的$\phi, \psi \in T(M)$，有$\phi \circ \psi \in T(M)$；
2. 对于任意的$\phi, \psi, \theta \in T(M)$，有$(\phi \circ \psi) \circ \theta = \phi \circ (\psi \circ \theta)$；
3. 存在$I \in T(M)$使得任意$\phi \in T(M)$，有$I \circ \phi = \phi \circ I = \phi$；
4. 对于任意$\phi \in T(M)$，存在$\phi^{-1} \in T(M)$，使得$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = I$。

变换群

Definition 11.4 (变换群)

设M是一个非空集合，$T(M)$是M上的所有可逆变换的全体。定义

$$\circ : T(M) \times T(M) \to T(M)$$

$$(\phi, \psi) \to \phi \circ \psi$$

为变换的合成(乘法)。则$(T(M), \circ)$是一个群，称为集合M的对称群。
集合M的对称群的子群称为集合M的变换群。

1. 对于任意的$\phi, \psi \in T(M)$，有$\phi \circ \psi \in T(M)$；
2. 对于任意的$\phi, \psi, \theta \in T(M)$，有$(\phi \circ \psi) \circ \theta = \phi \circ (\psi \circ \theta)$；
3. 存在$I \in T(M)$使得任意$\phi \in T(M)$，有$I \circ \phi = \phi \circ I = \phi$；
4. 对于任意$\phi \in T(M)$，存在$\phi^{-1} \in T(M)$，使得$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = I$。

变换群

Definition 11.4 (变换群)

设M是一个非空集合，$T(M)$是M上的所有可逆变换的全体。定义

$$\circ : T(M) \times T(M) \to T(M)$$

$$(\phi, \psi) \to \phi \circ \psi$$

为变换的合成(乘法)。则$(T(M), \circ)$是一个群，称为集合M的对称群。集合M的对称群的子群称为集合M的变换群。

1. 对于任意的$\phi, \psi \in T(M)$，有$\phi \circ \psi \in T(M)$；
2. 对于任意的$\phi, \psi, \theta \in T(M)$，有$(\phi \circ \psi) \circ \theta = \phi \circ (\psi \circ \theta)$；
3. 存在$I \in T(M)$使得任意$\phi \in T(M)$，有$I \circ \phi = \phi \circ I = \phi$；
4. 对于任意$\phi \in T(M)$，存在$\phi^{-1} \in T(M)$，使得$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = I$。

平面上的运动群

Example 11.5

用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则有$M(\mathbb{R}) \subseteq T(\mathbb{R})$。令"$\circ$"代表平面$\mathbb{R}^2$上两个运动的合成运算。则$(M(\mathbb{R}), \circ)$是一个群，称为平面$\mathbb{R}^2$上的运动群，是$(T(\mathbb{R}), \circ)$的子群。

Example 11.6

设K是平面$\mathbb{R}^2$上的一个图形。用$S(K)$表示使平面图形K仍回到自身的平面运动的全体。令"$\circ$"代表使平面图形K仍回到自身的平面运动的合成。用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则$(S(K), \circ)$是一个群，称为平面图形K上的对称群。

- 圆形；
- 正方形；
- 正五边形；

平面上的运动群

Example 11.5

用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则有$M(\mathbb{R}) \subseteq T(\mathbb{R})$。令"$\circ$"代表平面$\mathbb{R}^2$上两个运动的合成运算。则$(M(\mathbb{R}), \circ)$是一个群，称为平面$\mathbb{R}^2$上的运动群，是$(T(\mathbb{R}), \circ)$的子群。

Example 11.6

设K是平面$\mathbb{R}^2$上的一个图形。用$S(K)$表示使平面图形K仍回到自身的平面运动的全体。令"$\circ$"代表使平面图形K仍回到自身的平面运动的合成。用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则$(S(K), \circ)$是一个群，称为平面图形K上的对称群。

- 圆形；
- 正方形；
- 正五边形；

平面上的运动群

Example 11.5

用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则有$M(\mathbb{R}) \subseteq T(\mathbb{R})$。令"$\circ$"代表平面$\mathbb{R}^2$上两个运动的合成运算。则$(M(\mathbb{R}), \circ)$是一个群，称为平面$\mathbb{R}^2$上的运动群，是$(T(\mathbb{R}), \circ)$的子群。

Example 11.6

设K是平面$\mathbb{R}^2$上的一个图形。用$S(K)$表示使平面图形K仍回到自身的平面运动的全体。令"$\circ$"代表使平面图形K仍回到自身的平面运动的合成。用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则$(S(K), \circ)$是一个群，称为平面图形K上的对称群。

- 圆形；
- 正方形；
- 正五边形；

平面上的运动群

Example 11.5

用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则有$M(\mathbb{R}) \subseteq T(\mathbb{R})$。令“$\circ$”代表平面$\mathbb{R}^2$上两个运动的合成运算。则$(M(\mathbb{R}), \circ)$是一个群，称为平面$\mathbb{R}^2$上的运动群，是$(T(\mathbb{R}), \circ)$的子群。

Example 11.6

设K是平面$\mathbb{R}^2$上的一个图形。用$S(K)$表示使平面图形K仍回到自身的平面运动的全体。令“$\circ$”代表使平面图形K仍回到自身的平面运动的合成。用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则$(S(K), \circ)$是一个群，称为平面图形K上的对称群。

- 圆形；
- 正方形；
- 正五边形；

平面上的运动群

Example 11.5

用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则有$M(\mathbb{R}) \subseteq T(\mathbb{R})$。令“$\circ$”代表平面$\mathbb{R}^2$上两个运动的合成运算。则$(M(\mathbb{R}), \circ)$是一个群，称为平面$\mathbb{R}^2$上的运动群，是$(T(\mathbb{R}), \circ)$的子群。

Example 11.6

设K是平面$\mathbb{R}^2$上的一个图形。用$S(K)$表示使平面图形K仍回到自身的平面运动的全体。令“$\circ$”代表使平面图形K仍回到自身的平面运动的合成。用$M(\mathbb{R})$代表平面$\mathbb{R}^2$上的所有运动，运动只不过是特殊的保距变换，则$(S(K), \circ)$是一个群，称为平面图形K上的对称群。

- 圆形；
- 正方形；
- 正五边形；

数环和数域

设$\mathbb{C}$是复数集合。

Definition 11.7 (数环)

R的含有0和1的一个子集R，如果对于数的加法、减法和乘法都封闭，则称R是一个数环；如果$0 \neq a \in R$，则a^{-1}也在数环R中，则称R是一个数域。

Example 11.8

数域$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F} = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$都是数域。

Definition 11.9 (数域$\mathbb{F}$的自同构)

1. ϕ是集合$\mathbb{F}$到$\mathbb{F}$的一个一一对应；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(x + y) = \phi(x) + \phi(y)$；$\phi(xy) = \phi(x)\phi(y)$。

数环和数域

设$\mathbb{C}$是复数集合。

Definition 11.7 (数环)

$\mathbb{R}$的含有0和1的一个子集R，如果对于数的加法、减法和乘法都封闭，则称R是一个数环；如果$0 \neq a \in R$，则a^{-1}也在数环R中，则称R是一个数域。

Example 11.8

数域$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F} = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$都是数域。

Definition 11.9 (数域$\mathbb{F}$的自同构)

1. ϕ是集合$\mathbb{F}$到$\mathbb{F}$的一个一一对应；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(x + y) = \phi(x) + \phi(y)$；$\phi(xy) = \phi(x)\phi(y)$。

数环和数域

设$\mathbb{C}$是复数集合。

Definition 11.7 (数环)

R的含有0和1的一个子集R，如果对于数的加法、减法和乘法都封闭，则称R是一个**数环**；如果$0 \neq a \in R$，则a^{-1}也在数环R中，则称R是一个**数域**。

Example 11.8

数域$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F} = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$都是数域。

Definition 11.9 (数域$\mathbb{F}$的自同构)

1. ϕ是集合$\mathbb{F}$到$\mathbb{F}$的一个一一对应；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(x + y) = \phi(x) + \phi(y)$；$\phi(xy) = \phi(x)\phi(y)$。

数环和数域

设$\mathbb{C}$是复数集合。

Definition 11.7 (数环)

R的含有0和1的一个子集R，如果对于数的加法、减法和乘法都封闭，则称R是一个数环；如果$0 \neq a \in R$，则a^{-1}也在数环R中，则称R是一个数域。

Example 11.8

数域$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F} = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$都是数域。

Definition 11.9 (数域$\mathbb{F}$的自同构)

1. ϕ是集合$\mathbb{F}$到$\mathbb{F}$的一个一一对应；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(x + y) = \phi(x) + \phi(y)$；$\phi(xy) = \phi(x)\phi(y)$。

数域自同构的性质

1. $\phi(0) = 0, \phi(1) = 1$；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(-x) = -\phi(x)$；$\phi(x - y) = \phi(x) - \phi(y)$；
3. 对于任意$0 \neq x \in \mathbb{F}$，有$\phi(x^{-1}) = \phi(x)^{-1}$。

Theorem 11.10

令$Aut(\mathbb{F})$表示数域$\mathbb{F}$的所有的自同构的全体。令"$\circ$"代表自同构变换的合成运算，则$(Aut(\mathbb{F}), \circ)$ 是一个群，称为数域$\mathbb{F}$的自同构群。

图形K的对称群$S(K)$刻画了图形的对称；

而数域的自同构群则刻画了数域的对称！

数域自同构的性质

1. $\phi(0) = 0, \phi(1) = 1$；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(-x) = -\phi(x)$； $\phi(x - y) = \phi(x) - \phi(y)$；
3. 对于任意$0 \neq x \in \mathbb{F}$，有$\phi(x^{-1}) = \phi(x)^{-1}$。

Theorem 11.10

令$Aut(\mathbb{F})$表示数域$\mathbb{F}$的所有的自同构的全体。令"$\circ$"代表自同构变换的合成运算，则$(Aut(\mathbb{F}), \circ)$ 是一个群，称为数域$\mathbb{F}$的*自同构群*。

图形K的对称群$S(K)$刻画了图形的对称；

而数域的自同构群则刻画了数域的对称！

数域自同构的性质

1. $\phi(0) = 0, \phi(1) = 1$；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(-x) = -\phi(x)$；$\phi(x - y) = \phi(x) - \phi(y)$；
3. 对于任意$0 \neq x \in \mathbb{F}$，有$\phi(x^{-1}) = \phi(x)^{-1}$。

Theorem 11.10

令$Aut(\mathbb{F})$表示数域$\mathbb{F}$的所有的自同构的全体。令“$\circ$”代表自同构变换的合成运算，则$(Aut(\mathbb{F}), \circ)$ 是一个群，称为数域$\mathbb{F}$的自同构群。

图形K的对称群$S(K)$刻画了图形的对称；

而数域的自同构群则刻画了数域的对称！

数域自同构的性质

1. $\phi(0) = 0, \phi(1) = 1$；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(-x) = -\phi(x)$；$\phi(x - y) = \phi(x) - \phi(y)$；
3. 对于任意$0 \neq x \in \mathbb{F}$，有$\phi(x^{-1}) = \phi(x)^{-1}$。

Theorem 11.10

令$Aut(\mathbb{F})$表示数域$\mathbb{F}$的所有的自同构的全体。令"$\circ$"代表自同构变换的合成运算，则$(Aut(\mathbb{F}), \circ)$ 是一个群，称为数域$\mathbb{F}$的自同构群。

图形K的对称群$S(K)$刻画了图形的对称；

而数域的自同构群则刻画了数域的对称！

数域自同构的性质

1. $\phi(0) = 0, \phi(1) = 1$；
2. 对于所有的$x, y \in \mathbb{F}$有：
   $\phi(-x) = -\phi(x)$；$\phi(x-y) = \phi(x) - \phi(y)$；
3. 对于任意$0 \neq x \in \mathbb{F}$，有$\phi(x^{-1}) = \phi(x)^{-1}$。

Theorem 11.10

令$Aut(\mathbb{F})$表示数域$\mathbb{F}$的所有的自同构的全体。令“$\circ$”代表自同构变换的合成运算，则$(Aut(\mathbb{F}), \circ)$ 是一个群，称为数域$\mathbb{F}$的自同构群。

图形K的对称群$S(K)$刻画了图形的对称；

而数域的自同构群则刻画了数域的对称！

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$;
2. $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2$;
3. $\phi(n) = n$;
4. $\phi(-n) = -n$;
5. $\phi(\frac{1}{n}) = n^{-1}$;
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$;

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$;
2. $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2$;
3. $\phi(n) = n$;
4. $\phi(-n) = -n$;
5. $\phi(\frac{1}{n}) = n^{-1}$;
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$;

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$;
2. $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2$;
3. $\phi(n) = n$;
4. $\phi(-n) = -n$;
5. $\phi(\frac{1}{n}) = n^{-1}$;
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$;

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$；
2. $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2$；
3. $\phi(n) = n$；
4. $\phi(-n) = -n$；
5. $\phi(\frac{1}{n}) = n^{-1}$；
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$；

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$；
2. $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2$；
3. $\phi(n) = n$；
4. $\phi(-n) = -n$；
5. $\phi(\frac{1}{n}) = n^{-1}$；
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$；

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$;
2. $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2$;
3. $\phi(n) = n$;
4. $\phi(-n) = -n$;
5. $\phi(\frac{1}{n}) = n^{-1}$;
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$;

数域自同构的举例

Example 11.11

有理数域$\mathbb{Q}$的自同构群只有一个元素$\{I\}$。

1. $\phi(0) = 0, \phi(1) = 1$;
2. $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2$;
3. $\phi(n) = n$;
4. $\phi(-n) = -n$;
5. $\phi(\frac{1}{n}) = n^{-1}$;
6. $\phi(m/n) = \phi(m)\phi(1/n) = m/n$;

数域自同构的举例

Example 11.12

数域$\mathbb{Q}\left(\sqrt{2}\right) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$的自同构群有两个元素$\{I, \phi\}$。

- $\phi(a + b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\phi(\sqrt{2})$;
- 做为自同构ϕ应该是保持运算的，故$\sqrt{2}$所满足的有理系数代数关系，$\phi(\sqrt{2})$也应该满足；
- $\sqrt{2}$是$x^2 - 2 = 0$的根，故$\phi(\sqrt{2})$也应该是，所以$\phi(\sqrt{2}) = \sqrt{2}$或者$-\sqrt{2}$;
- 因此有两个自同构：
  $I : a + b\sqrt{2} \to a + b\sqrt{2}$和$\phi : a + b\sqrt{2} \to a - b\sqrt{2}$;

$\circ$	I	ϕ
I	I	ϕ
$\circ$	ϕ	I

数域自同构的举例

Example 11.12

数域$\mathbb{Q}\left(\sqrt{2}\right) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$的自同构群有两个元素$\{I, \phi\}$。

- $\phi(a + b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\phi(\sqrt{2})$;
- 做为自同构ϕ应该是保持运算的，故$\sqrt{2}$所满足的有理系数代数关系，$\phi(\sqrt{2})$也应该满足;
- $\sqrt{2}$是$x^2 - 2 = 0$的根，故$\phi(\sqrt{2})$也应该是，所以$\phi(\sqrt{2}) = \sqrt{2}$或者$-\sqrt{2}$;
- 因此有两个自同构：
  $I : a + b\sqrt{2} \to a + b\sqrt{2}$和$\phi : a + b\sqrt{2} \to a - b\sqrt{2}$;

$\circ$	I	ϕ
I	I	ϕ
ϕ	ϕ	I

数域自同构的举例

Example 11.12

数域$\mathbb{Q}\left(\sqrt{2}\right)=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$的自同构群有两个元素$\{I,\phi\}$。

- $\phi(a+b\sqrt{2})=\phi(a)+\phi(b)\phi(\sqrt{2})=a+b\phi(\sqrt{2})$；
- 做为自同构ϕ应该是保持运算的，故$\sqrt{2}$所满足的有理系数代数关系，$\phi(\sqrt{2})$也应该满足；
- $\sqrt{2}$是$x^2-2=0$的根，故$\phi(\sqrt{2})$也应该是，所以$\phi(\sqrt{2})=\sqrt{2}$或者$-\sqrt{2}$；
- 因此有两个自同构：
  $I:a+b\sqrt{2}\to a+b\sqrt{2}$和$\phi:a+b\sqrt{2}\to a-b\sqrt{2}$；

$\circ$	I	ϕ
I	I	ϕ
ϕ	ϕ	I

数域自同构的举例

Example 11.12

数域$\mathbb{Q}\left(\sqrt{2}\right) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$的自同构群有两个元素$\{I, \phi\}$。

- $\phi(a + b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\phi(\sqrt{2})$;
- 做为自同构ϕ应该是保持运算的，故$\sqrt{2}$所满足的有理系数代数关系，$\phi(\sqrt{2})$也应该满足；
- $\sqrt{2}$是$x^2 - 2 = 0$的根，故$\phi(\sqrt{2})$也应该是，所以$\phi(\sqrt{2}) = \sqrt{2}$或者$-\sqrt{2}$;
- 因此有两个自同构：
  $I : a + b\sqrt{2} \to a + b\sqrt{2}$和$\phi : a + b\sqrt{2} \to a - b\sqrt{2}$;

$\circ$	I	ϕ
I	I	ϕ
$\circ$	ϕ	I

数域自同构的举例

Example 11.12

数域$\mathbb{Q}\left(\sqrt{2}\right) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$的自同构群有两个元素$\{I, \phi\}$。

- $\phi(a + b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\phi(\sqrt{2})$;
- 做为自同构ϕ应该是保持运算的，故$\sqrt{2}$所满足的有理系数代数关系，$\phi(\sqrt{2})$也应该满足;
- $\sqrt{2}$是$x^2 - 2 = 0$的根，故$\phi(\sqrt{2})$也应该是，所以$\phi(\sqrt{2}) = \sqrt{2}$或者$-\sqrt{2}$;
- 因此有两个自同构：
  $I : a + b\sqrt{2} \to a + b\sqrt{2}$和$\phi : a + b\sqrt{2} \to a - b\sqrt{2}$;

$\circ$	I	ϕ
I	I	ϕ
ϕ	ϕ	I

数域自同构的举例

Example 11.12

数域$\mathbb{Q}\left(\sqrt{2}\right)=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$的自同构群有两个元素$\{I,\phi\}$。

- $\phi(a+b\sqrt{2})=\phi(a)+\phi(b)\phi(\sqrt{2})=a+b\phi(\sqrt{2})$;
- 做为自同构ϕ应该是保持运算的，故$\sqrt{2}$所满足的有理系数代数关系，$\phi(\sqrt{2})$也应该满足;
- $\sqrt{2}$是$x^2-2=0$的根，故$\phi(\sqrt{2})$也应该是，所以$\phi(\sqrt{2})=\sqrt{2}$或者$-\sqrt{2}$;
- 因此有两个自同构：
  $I:a+b\sqrt{2}\to a+b\sqrt{2}$和$\phi:a+b\sqrt{2}\to a-b\sqrt{2}$;

$\circ$	I	ϕ
I	I	ϕ
$\circ$	ϕ	I

数域自同构的举例

Example 11.13

数域$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\mid a,b,c,d\in\mathbb{Q}\right\}$的自同构群有两个元素$\{I,\phi_1,\phi_2,\phi_{12}\}$。

- $I: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}$;
- $\phi_1: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a-b\sqrt{2}+c\sqrt{3}-d\sqrt{2}\sqrt{3}$;
- $\phi_2: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a+b\sqrt{2}-c\sqrt{3}-d\sqrt{2}\sqrt{3}$;
- $\phi_{12}: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a-b\sqrt{2}-c\sqrt{3}+d\sqrt{2}\sqrt{3}$;

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

数域自同构的举例

Example 11.13

数域$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\right\}$的自同构群有两个元素$\{I, \phi_1, \phi_2, \phi_{12}\}$。

- $I : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$;
- $\phi_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3}$;
- $\phi_2 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{2}\sqrt{3}$;
- $\phi_{12} : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a - b\sqrt{2} - c\sqrt{3} + d\sqrt{2}\sqrt{3}$;

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

数域自同构的举例

Example 11.13

数域$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\mid a,b,c,d\in\mathbb{Q}\right\}$的自同构群有两个元素$\{I,\phi_1,\phi_2,\phi_{12}\}$。

- $I: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}$;
- $\phi_1: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a-b\sqrt{2}+c\sqrt{3}-d\sqrt{2}\sqrt{3}$;
- $\phi_2: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a+b\sqrt{2}-c\sqrt{3}-d\sqrt{2}\sqrt{3}$;
- $\phi_{12}: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}\rightarrow a-b\sqrt{2}-c\sqrt{3}+d\sqrt{2}\sqrt{3}$;

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

数域自同构的举例

Example 11.13

数域$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\right\}$的自同构群有两个元素$\{I, \phi_1, \phi_2, \phi_{12}\}$。

- $I : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$;
- $\phi_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3}$;
- $\phi_2 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{2}\sqrt{3}$;
- $\phi_{12} : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a - b\sqrt{2} - c\sqrt{3} + d\sqrt{2}\sqrt{3}$;

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

数域自同构的举例

Example 11.13

数域$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\right\}$的自同构群有两个元素$\{I, \phi_1, \phi_2, \phi_{12}\}$。

- $I : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$;
- $\phi_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3}$;
- $\phi_2 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{2}\sqrt{3}$;
- $\phi_{12} : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \rightarrow a - b\sqrt{2} - c\sqrt{3} + d\sqrt{2}\sqrt{3}$;

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

数域的对称群

Definition 11.14

给定两个数域$\mathbb{F},\mathbb{E}$，满足$\mathbb{F}\subseteq\mathbb{E}$。定义

$$Aut(\mathbb{E}:\mathbb{F}) = \{\phi \in Aut(E) \mid \forall x \in \mathbb{F}, \phi(x) = x\}.$$

即使域$\mathbb{F}$中的元素保持不动的$\mathbb{E}$的自同构所构成的群，称之为数域$\mathbb{E}$在数域$\mathbb{F}$上的对称群。

Example 11.15

- $Aut\left(\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right) = \{I,\phi\}$;
- $Aut\left(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right) = \{I,\phi_1,\phi_2,\phi_{12}\}$;
- $Aut\left(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})\right) = \{I,\phi_2\}$。

数域的对称群

Definition 11.14

给定两个数域$\mathbb{F},\mathbb{E}$，满足$\mathbb{F}\subseteq\mathbb{E}$。定义

$$Aut(\mathbb{E}:\mathbb{F}) = \{\phi \in Aut(E) \mid \forall x \in \mathbb{F}, \phi(x) = x\}.$$

即使域$\mathbb{F}$中的元素保持不动的$\mathbb{E}$的自同构所构成的群，称之为数域$\mathbb{E}$在数域$\mathbb{F}$上的对称群。

Example 11.15

- $Aut\left(\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right) = \{I, \phi\}$;
- $Aut\left(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right) = \{I, \phi_1, \phi_2, \phi_{12}\}$;
- $Aut\left(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})\right) = \{I, \phi_2\}$。

数域的对称群

Definition 11.14

给定两个数域$\mathbb{F}, \mathbb{E}$，满足$\mathbb{F} \subseteq \mathbb{E}$。定义

$$Aut(\mathbb{E} : \mathbb{F}) = \{\phi \in Aut(E) \mid \forall x \in \mathbb{F}, \phi(x) = x\}.$$

即使域$\mathbb{F}$中的元素保持不动的$\mathbb{E}$的自同构所构成的群，称之为数域$\mathbb{E}$在数域$\mathbb{F}$上的对称群。

Example 11.15

- $Aut\left(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right) = \{I, \phi\}$;
- $Aut\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right) = \{I, \phi_1, \phi_2, \phi_{12}\}$;
- $Aut\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\right) = \{I, \phi_2\}$。

数域$\mathbb{F}$上的n元多项式

Definition 11.16

以数域$\mathbb{F}$中的元素为系数的n元多项式的全体记为

$$\mathbb{F}[x_1, x_2, \cdots, x_n] = \left\{ f(x_1, x_2, \cdots, x_n) = \sum_{\alpha} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \right.$$

$$\left. \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n),\ \alpha_i \in \mathbb{Z}^+ \cup \{0\}, a_\alpha \in \mathbb{F} \right\}.$$

Definition 11.17 (n元对称群)

设$M = \{x_1, x_2, \cdots, x_n\}$。用$S_n$表示集合$M$上的变换群，称为$n$元对称群。

数域$\mathbb{F}$上的n元多项式

Definition 11.16

以数域$\mathbb{F}$中的元素为系数的n元多项式的全体记为

$$\mathbb{F}[x_1, x_2, \cdots, x_n] = \left\{ f(x_1, x_2, \cdots, x_n) = \sum_{\alpha} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \right.$$

$$\left. \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n),\ \alpha_i \in \mathbb{Z}^+ \cup \{0\}, a_\alpha \in \mathbb{F} \right\}.$$

Definition 11.17 (n元对称群)

设$M = \{x_1, x_2, \cdots, x_n\}$。用$S_n$表示集合$M$上的变换群，称为$n$元对称群。

数域$\mathbb{F}$上的n元多项式

Definition 11.16

以数域$\mathbb{F}$中的元素为系数的n元多项式的全体记为

$$\mathbb{F}[x_1, x_2, \cdots, x_n] = \left\{ f(x_1, x_2, \cdots, x_n) = \sum_{\alpha} a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \right.$$

$$\left. \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n),\ \alpha_i \in \mathbb{Z}^+ \cup \{0\}, a_\alpha \in \mathbb{F} \right\}.$$

Definition 11.17 (n元对称群)

设$M = \{x_1, x_2, \cdots, x_n\}$。用$S_n$表示集合$M$上的变换群，称为$n$元对称群。

$\mathbb{F}[X]$的置换群

取$\sigma \in S_n$，设$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$。定义

$$\phi_\sigma : \mathbb{F}[X] \to \mathbb{F}[X]$$

$$f(x_1, x_2, \cdots, x_n) \to f(x_{i_1}, x_{i_2}, \cdots, x_{i_n}).$$

则ϕ_σ是集合$\mathbb{F}(X)$上的一个一一变换。

Definition 11.18 ($\mathbb{F}[x]$的n元置换群)

令$T_n = \{\phi_\sigma \mid \sigma \in S_n\}$。则$(T_n, \circ)$是集合$\mathbb{F}[X]$上的变换群，称为$\mathbb{F}[x]$的$n$元置换群。其中

$$\phi_\sigma \circ \phi_\theta = \phi_{\sigma\circ\theta}, \quad (\phi_\sigma)^{-1} = \phi_{\sigma^{-1}}.$$

$\mathbb{F}[X]$的置换群

取$\sigma \in S_n$，设$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$。定义

$$\phi_\sigma : \mathbb{F}[X] \to \mathbb{F}[X]$$

$$f(x_1, x_2, \cdots, x_n) \to f(x_{i_1}, x_{i_2}, \cdots, x_{i_n}).$$

则ϕ_σ是集合$\mathbb{F}(X)$上的一个一一变换。

Definition 11.18 ($\mathbb{F}[x]$的n元置换群)

令$T_n = \{\phi_\sigma \mid \sigma \in S_n\}$。则$(T_n, \circ)$是集合$\mathbb{F}[X]$上的变换群，称为$\mathbb{F}[x]$的$n$元置换群。其中

$$\phi_\sigma \circ \phi_\theta = \phi_{\sigma\circ\theta}, \quad (\phi_\sigma)^{-1} = \phi_{\sigma^{-1}}.$$

多项式$f(x_1, x_2, \cdots, x_n)$的对称群

Definition 11.19 (多项式$f(x_1, x_2, \cdots, x_n)$的对称群)

设$f(x_1, x_2, \cdots, x_n) \in \mathbb{F}[X]$，令

$$S_f = \{\phi_\sigma \in T_n \mid \phi_\sigma(f) = f\}.$$

$(S_f, \circ)$也是群，称为多项式$f(x_1, x_2, \cdots, x_n)$的对称群。

将$\mathbb{F}[X]$与平面类比，将$f(x_1, x_2, \cdots, x_n)$与平面图形K类比，
则$\mathbb{F}[X]$的置换群相当于平面的运动群！
多项式的对称群S_f相当于平面图形的对称群$S(K)$!

多项式$f(x_1, x_2, \cdots, x_n)$的对称群

Definition 11.19 (多项式$f(x_1, x_2, \cdots, x_n)$的对称群)

设$f(x_1, x_2, \cdots, x_n) \in \mathbb{F}[X]$，令

$$S_f = \{\phi_\sigma \in T_n \mid \phi_\sigma(f) = f\}.$$

$(S_f, \circ)$也是群，称为多项式$f(x_1, x_2, \cdots, x_n)$的对称群。

将$\mathbb{F}[X]$与平面类比，将$f(x_1, x_2, \cdots, x_n)$与平面图形K类比，
则$\mathbb{F}[X]$的置换群相当于平面的运动群！
多项式的对称群S_f相当于平面图形的对称群$S(K)$!

多项式$f(x_1, x_2, \cdots, x_n)$的对称群示例

Example 11.20

$\mathbb{F}[x_1, x_2, x_3, x_4]$上的多项式$f = x_1x_2 + x_3x_4$的对称群为

$$S_f = \left\{\phi_\sigma \mid \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \right.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Definition 11.21 (对称多项式)

若$S_f = T_n$，则称该多项式f为对称多项式。

多项式$f(x_1, x_2, \cdots, x_n)$的对称群示例

Example 11.20

$\mathbb{F}[x_1, x_2, x_3, x_4]$上的多项式$f = x_1x_2 + x_3x_4$的对称群为

$$S_f = \left\{\phi_\sigma \mid \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \right.$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

Definition 11.21 (对称多项式)

若$S_f = T_n$，则称该多项式f为对称多项式。

Cayley's Theorem

Theorem 11.22 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. 任何群都同构于一个变换群。

以G为集合，讨论其上的对称群$T(G)$；

- G中的每一个元素g一一对应于集合G上的一个可逆映射$T_g : G \to G$，且$T_g : x \to gx$.
  - T_g是G上的映射：若$gx \neq gx' \Rightarrow x \neq x'$；$T_g$是G上的满射：给定$y \in G$，一定存在$x \in G$，使得$gx = y$。
  - T_g是G上是单射：$gx = gx' \Rightarrow x = x'$。
- $T : G \to T(G)$是一个单射。$T_g = T_h \Rightarrow gx = hx \Rightarrow g = h$。
- $T : G \to \{T_g \mid g \in G\}$是一个双射且保持运算：元素$hg$对应的置换$T_{hg} = T_h \circ T_g$。
- 因此G与G上的对称群的一个变换子群同构。

Cayley's Theorem

Theorem 11.22 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. 任何群都同构于一个变换群。

以G为集合，讨论其上的对称群$T(G)$；

- G中的每一个元素g一一对应于集合G上的一个可逆映射$T_g : G \to G$，且$T_g : x \to gx$.
  - T_g是G上的映射：若$gx \neq gx' \Rightarrow x \neq x'$；
    T_g是G上的满射：给定$y \in G$，一定存在$x \in G$，使得$gx = y$。
  - T_g是G上是单射：$gx = gx' \Rightarrow x = x'$。
- $T : G \to T(G)$是一个单射。$T_g = T_h \Rightarrow gx = hx \Rightarrow g = h$。
- $T : G \to \{T_g \mid g \in G\}$是一个双射且保持运算：元素$hg$对应的置换$T_{hg} = T_h \circ T_g$。
- 因此G与G上的对称群的一个变换子群同构。

Cayley's Theorem

Theorem 11.22 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. 任何群都同构于一个变换群。

以G为集合，讨论其上的对称群$T(G)$：

- G中的每一个元素g一一对应于集合G上的一个可逆映射$T_g : G \to G$，且$T_g : x \to gx$.
  - T_g是G上的映射：若$gx \neq gx' \Rightarrow x \neq x'$；$T_g$是$G$上的满射：给定$y \in G$，一定存在$x \in G$，使得$gx = y$。
  - T_g是G上是单射：$gx = gx' \Rightarrow x = x'$。
- $T : G \to T(G)$是一个单射。$T_g = T_h \Rightarrow gx = hx \Rightarrow g = h$。
- $T : G \to \{T_g \mid g \in G\}$是一个双射且保持运算：元素$hg$对应的置换$T_{hg} = T_h \circ T_g$。
- 因此G与G上的对称群的一个变换子群同构。

Cayley's Theorem

Theorem 11.22 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. 任何群都同构于一个变换群。

以G为集合，讨论其上的对称群$T(G)$；

- G中的每一个元素g一一对应于集合G上的一个可逆映射$T_g : G \to G$，且$T_g : x \to gx$.
  - T_g是G上的映射：若$gx \neq gx' \Rightarrow x \neq x'$；
    T_g是G上的满射：给定$y \in G$，一定存在$x \in G$，使得$gx = y$。
  - T_g是G上是单射：$gx = gx' \Rightarrow x = x'$。
- $T : G \to T(G)$是一个单射。$T_g = T_h \Rightarrow gx = hx \Rightarrow g = h$。
- $T : G \to \{T_g \mid g \in G\}$是一个双射且保持运算：元素$hg$对应的置换$T_{hg} = T_h \circ T_g$。
- 因此G与G上的对称群的一个变换子群同构。

Cayley's Theorem

Theorem 11.22 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. 任何群都同构于一个变换群。

以G为集合，讨论其上的对称群$T(G)$；

- G中的每一个元素g一一对应于集合G上的一个可逆映射$T_g : G \to G$，且$T_g : x \to gx$.
  - T_g是G上的映射：若$gx \neq gx' \Rightarrow x \neq x'$；$T_g$是$G$上的满射：给定$y \in G$，一定存在$x \in G$，使得$gx = y$。
  - T_g是G上是单射：$gx = gx' \Rightarrow x = x'$。
- $T : G \to T(G)$是一个单射。$T_g = T_h \Rightarrow gx = hx \Rightarrow g = h$。
- $T : G \to \{T_g \mid g \in G\}$是一个双射且保持运算：元素$hg$对应的置换$T_{hg} = T_h \circ T_g$。
- 因此G与G上的对称群的一个变换子群同构。

Cayley's Theorem

Theorem 11.22 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. 任何群都同构于一个变换群。

以G为集合，讨论其上的对称群$T(G)$；

- G中的每一个元素g一一对应于集合G上的一个可逆映射$T_g : G \to G$，且$T_g : x \to gx$.
    - T_g是G上的映射：若$gx \neq gx' \Rightarrow x \neq x'$；$T_g$是$G$上的满射：给定$y \in G$，一定存在$x \in G$，使得$gx = y$。
    - T_g是G上是单射：$gx = gx' \Rightarrow x = x'$。
- $T : G \to T(G)$是一个单射。$T_g = T_h \Rightarrow gx = hx \Rightarrow g = h$。
- $T : G \to \{T_g \mid g \in G\}$是一个双射且保持运算：元素$hg$对应的置换$T_{hg} = T_h \circ T_g$。
- 因此G与G上的对称群的一个变换子群同构。

Permutation

Definition 12.1 (permutation)

A permutation of a finite set S is a bijection on S, that is, a function $\pi : S \mapsto S$ that is one-to-one and onto.

Example 12.2

If $S = \{1, 2, 3, 4, 5\}$, then

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{bmatrix}$$

is the permutation such that $\pi(1) = 3, \pi(2) = 5, \pi(3) = 4, \pi(4) = 1, \pi(5) = 2$.

Permutation

Definition 12.1 (permutation)

A permutation of a finite set S is a bijection on S, that is, a function $\pi : S \mapsto S$ that is one-to-one and onto.

Example 12.2

If $S = \{1, 2, 3, 4, 5\}$, then

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{bmatrix}$$

is the permutation such that $\pi(1) = 3, \pi(2) = 5, \pi(3) = 4, \pi(4) = 1, \pi(5) = 2.$

Permutation groups

Definition 12.3 (symmetric group)

- **Symmetric group 对称群:** the set S_n of all permutations of $\{1, 2, \ldots, n\}$.
- The group operation is composition of functions.
- The subgroup of S_n is called a permutation group.

Fact 12.4

- $|S_n| = n!$.

Let $\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, $\sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, then $\sigma_1 \cdot \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$.

Let $\sigma = \begin{bmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{bmatrix}$, then $\sigma^{-1} = \begin{bmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{bmatrix}$

Permutation groups

Definition 12.3 (symmetric group)

- **Symmetric group 对称群:** the set S_n of all permutations of $\{1, 2, \ldots, n\}$.
- The group operation is composition of functions.
- The subgroup of S_n is called a permutation group.

Fact 12.4

- $|S_n| = n!$.

Let $\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, $\sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, then $\sigma_1 \cdot \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$.

Let $\sigma = \begin{bmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{bmatrix}$, then $\sigma^{-1} = \begin{bmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{bmatrix}$

Permutation groups

Definition 12.3 (symmetric group)

- **Symmetric group 对称群:** the set S_n of all permutations of $\{1, 2, \ldots, n\}$.
- The group operation is composition of functions.
- The subgroup of S_n is called a permutation group.

Fact 12.4

- $|S_n| = n!$.

Let $\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$, $\sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, then $\sigma_1 \cdot \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$.

Let $\sigma = \begin{bmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{bmatrix}$, then $\sigma^{-1} = \begin{bmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{bmatrix}$

Fact 12.5 (cycle)

Let S be a finite set. If we start with any element $x \in S$ and apply π repeatedly to obtain $\pi(x), \pi(\pi(x)), \ldots,$ and so on, eventually we must return to x.
We call $(x, \pi(x), \pi(\pi(x)), \ldots)$ a cycle. Cycle of even length is called Even cycle.
Two element cycles are called transpositions.

Example 12.6

For the example

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{bmatrix}$$

we have $1 \to 3 \to 4 \to 1$, $2 \to 5 \to 2$, and $6 \to 6$.
So we express this result by writing $\pi = (1,3,4)(2,5)(6) = (1,3,4)(2,5)$.

Fact 12.5 (cycle)

Let S be a finite set. If we start with any element $x \in S$ and apply π repeatedly to obtain $\pi(x), \pi(\pi(x)), \ldots,$ and so on, eventually we must return to x.
We call $(x, \pi(x), \pi(\pi(x)), \ldots)$ a cycle. Cycle of even length is called Even cycle.
Two element cycles are called transpositions.

Example 12.6

For the example

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{bmatrix}$$

we have $1 \to 3 \to 4 \to 1$, $2 \to 5 \to 2$, and $6 \to 6$.
So we express this result by writing $\pi = (1, 3, 4)(2, 5)(6) = (1, 3, 4)(2, 5)$.

Fact 12.7

The product $(1,3,4)(2,5)$ is a composition , with the right factor $(2,5)$ applied first, as with composition of functions.

Definition 1

Let $\sigma = (i_1 i_2 \ldots i_r)$ and $\tau = (j_1 j_2 \ldots j_s)$ be two cycles. If

$$i_k \neq j_l, \quad k = 1,2,\ldots,r; \quad l = 1,2,\ldots,s,$$

cycle σ and τ are called disjoint cycles.

Fact 12.8

The product of any two disjoint cycles is commutative. $\sigma \cdot \tau = \tau \cdot \sigma$.

Fact 12.7

The product $(1,3,4)(2,5)$ is a composition , with the right factor $(2,5)$ applied first, as with composition of functions.

Definition 1

Let $\sigma = (i_1 i_2 \ldots i_r)$ and $\tau = (j_1 j_2 \ldots j_s)$ be two cycles. If

$$i_k \neq j_l, \quad k = 1, 2, \ldots, r; \quad l = 1, 2, \ldots, s,$$

cycle σ and τ are called disjoint cycles.

Fact 12.8

The product of any two disjoint cycles is commutative. $\sigma \cdot \tau = \tau \cdot \sigma$.

Fact 12.7

The product $(1,3,4)(2,5)$ is a composition , with the right factor $(2,5)$ applied first, as with composition of functions.

Definition 1

Let $\sigma = (i_1 i_2 \ldots i_r)$ and $\tau = (j_1 j_2 \ldots j_s)$ be two cycles. If

$$i_k \neq j_l, \quad k = 1, 2, \ldots, r; \quad l = 1, 2, \ldots, s,$$

cycle σ and τ are called disjoint cycles.

Fact 12.8

The product of any two disjoint cycles is commutative. $\sigma \cdot \tau = \tau \cdot \sigma$.

Fact 12.7

The product $(1, 3, 4)(2, 5)$ *is a composition , with the right factor* $(2, 5)$ *applied first, as with composition of functions.*

Definition 1

Let $\sigma = (i_1 i_2 \dots i_r)$ *and* $\tau = (j_1 j_2 \dots j_s)$ *be two cycles. If*

$$i_k \neq j_l, \quad k = 1, 2, \dots, r; \quad l = 1, 2, \dots, s,$$

cycle σ *and* τ *are called disjoint cycles.*

Fact 12.8

The product of any two disjoint cycles is commutative. $\sigma \cdot \tau = \tau \cdot \sigma$.

Theorem 12.9

Any permutation can be expressed as a product of disjoint cycles, and the cycle decomposition is unique.

Proof.

对集合S中的元素个数n进行数学归纳：

(1) $n=1$时，$\tau=(1)$显然成立。

(2) 设$n-1$时结论成立。

(3) 设$S=\{1,2,\cdots,n\}$。任取一个置换，

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

- 若$i_n=n$，则

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix}=\alpha'\cdot(n).$$

Theorem 12.9

Any permutation can be expressed as a product of disjoint cycles, and the cycle decomposition is unique.

Proof.

对集合S中的元素个数n进行数学归纳：

(1) $n = 1$时，$\tau = (1)$显然成立。

(2) 设$n - 1$时结论成立。

(3) 设$S = \{1, 2, \cdots, n\}$。任取一个置换，

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

- 若$i_n = n$，则

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix} = \alpha' \cdot (n).$$

Theorem 12.9

Any permutation can be expressed as a product of disjoint cycles, and the cycle decomposition is unique.

Proof.

对集合S中的元素个数n进行数学归纳：

(1) $n = 1$时，$\tau = (1)$显然成立。

(2) 设$n-1$时结论成立。

(3) 设$S = \{1, 2, \cdots, n\}$。任取一个置换，

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

- 若$i_n = n$，则

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix} = \alpha' \cdot (n).$$

Theorem 12.9

Any permutation can be expressed as a product of disjoint cycles, and the cycle decomposition is unique.

Proof.

对集合S中的元素个数n进行数学归纳：

(1) $n=1$时，$\tau=(1)$显然成立。

(2) 设$n-1$时结论成立。

(3) 设$S=\{1,2,\cdots,n\}$。任取一个置换，

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

- 若$i_n=n$，则

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix}=\alpha'\cdot(n).$$

Theorem 12.9

Any permutation can be expressed as a product of disjoint cycles, and the cycle decomposition is unique.

Proof.

对集合S中的元素个数n进行数学归纳：

(1) $n=1$时，$\tau=(1)$显然成立。

(2) 设$n-1$时结论成立。

(3) 设$S=\{1,2,\cdots,n\}$。任取一个置换，

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

- 若$i_n=n$，则

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix}=\alpha'\cdot(n).$$

- 若$i_n \neq n$，则必存在$i_k = n$，则

$$
\begin{aligned}
\beta &:= (i_k\ i_n)\cdot\alpha = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{k-1} & i_n & i_{k+1} & \cdots & i_{n-1} & n \end{pmatrix} \\
\alpha &= (n\ i_n)\alpha'. \qquad (1)
\end{aligned}
$$

而α'是一个$n-1$阶置换，故$\alpha' = \alpha_1\alpha_2\ldots\alpha_r$可分解为一些不相交的轮换的乘积。若存在$\alpha_i$与$(n\ i_n)$相交，则最多有一个这样的$\alpha_i$且相交的元素一定为$i_n$。不失一般性，设$\alpha_1 = (i_n\ a\ \ldots\ b)$。得到$(n\ i_n)\alpha_1 = (n\ i_n\ a\ \ldots\ b)$。故$\alpha = (n\ i_n\ a\ \ldots\ b)\alpha_2\ldots\alpha_r$。

- 若$i_n \neq n$，则必存在$i_k = n$，则

$$
\begin{aligned}
\beta &:= (i_k\ i_n) \cdot \alpha = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{k-1} & i_n & i_{k+1} & \cdots & i_{n-1} & n \end{pmatrix} \\
\alpha &= (n\ i_n)\alpha'. \qquad (1)
\end{aligned}
$$

而α'是一个$n-1$阶置换，故$\alpha' = \alpha_1\alpha_2 \ldots \alpha_r$可分解为一些不相交的轮换的乘积。若存在$\alpha_i$与$(n\ i_n)$相交，则最多有一个这样的$\alpha_i$且相交的元素一定为$i_n$。不失一般性，设$\alpha_1 = (i_n\ a\ \ldots\ b)$。得到$(n\ i_n)\alpha_1 = (n\ i_n\ a\ \ldots\ b)$。故$\alpha = (n\ i_n\ a\ \ldots\ b)\alpha_2 \ldots \alpha_r$。

- 若$i_n \neq n$，则必存在$i_k = n$，则

$$
\begin{aligned}
\beta &:= (i_k\ i_n)\cdot\alpha = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{k-1} & i_n & i_{k+1} & \cdots & i_{n-1} & n \end{pmatrix} \\
\alpha &= (n\ i_n)\alpha'.
\end{aligned} \tag{1}
$$

而α'是一个$n-1$阶置换，故$\alpha' = \alpha_1\alpha_2\ldots\alpha_r$可分解为一些不相交的轮换的乘积。若存在$\alpha_i$与$(n\ i_n)$相交，则最多有一个这样的$\alpha_i$且相交的元素一定为$i_n$。不失一般性，设$\alpha_1 = (i_n\ a\ \ldots\ b)$。得到$(n\ i_n)\alpha_1 = (n\ i_n\ a\ \ldots\ b)$。故$\alpha = (n\ i_n\ a\ \ldots\ b)\alpha_2\ldots\alpha_r$。

例：3次对称群S_3中的6个置换可以用轮换进行表示：

$$\sigma_1 = I,\ \sigma_2 = (1\ 2),\ \sigma_3 = (1\ 3),$$

$$\sigma_4 = (2\ 3),\ \sigma_5 = (1\ 2\ 3),\ \sigma_6 = (1\ 3\ 2).$$

Fact 12.10

- *置换σ的级：若σ是一个r长轮换，则$ord(\sigma) = r$；*
- *置换$\sigma = \sigma_1\sigma_2\cdots\sigma_t$的轮换分解。则$ord(\sigma) = l.c.m(ord(\sigma_1)\cdots ord(\sigma_t))$.*

Fact 12.11

设$a,\ldots,b,c,\ldots,d,k,l$为互不相同的正整数，则

- $(k\ l)(k\ a\ \cdots\ b)(l\ c\ \cdots\ d) = (k\ a\ \cdots\ b\ l\ c\cdots\ d)$;
- $(k\ l)(k\ a\ \cdots\ b\ l\ c\ \cdots\ d) = (k\ a\ \cdots\ b)(l\ c\cdots\ d)$;

例：3次对称群S_3中的6个置换可以用轮换进行表示：

$$\sigma_1 = I,\ \sigma_2 = (1\ 2),\ \sigma_3 = (1\ 3),$$

$$\sigma_4 = (2\ 3),\ \sigma_5 = (1\ 2\ 3),\ \sigma_6 = (1\ 3\ 2).$$

Fact 12.10

- 置换σ的级：若σ是一个r长轮换，则$ord(\sigma) = r$；
- 置换$\sigma = \sigma_1\sigma_2\cdots\sigma_t$的轮换分解。则$ord(\sigma) = l.c.m(ord(\sigma_1)\cdots ord(\sigma_t))$.

Fact 12.11

设$a,\ldots,b,c,\ldots,d,k,l$为互不相同的正整数，则

- $(k\ l)(k\ a\ \cdots\ b)(l\ c\ \cdots\ d) = (k\ a\ \cdots\ b\ l\ c\cdots\ d)$;
- $(k\ l)(k\ a\ \cdots\ b\ l\ c\ \cdots\ d) = (k\ a\ \cdots\ b)(l\ c\cdots\ d)$;

例：3次对称群S_3中的6个置换可以用轮换进行表示：

$$\sigma_1 = I,\ \sigma_2 = (1\ 2),\ \sigma_3 = (1\ 3),$$

$$\sigma_4 = (2\ 3),\ \sigma_5 = (1\ 2\ 3),\ \sigma_6 = (1\ 3\ 2).$$

Fact 12.10

- 置换σ的级：若σ是一个r长轮换，则$ord(\sigma) = r$；
- 置换$\sigma = \sigma_1\sigma_2\cdots\sigma_t$的轮换分解。则$ord(\sigma) = l.c.m(ord(\sigma_1)\cdots ord(\sigma_t))$.

Fact 12.11

设$a,\ldots,b,c,\ldots,d,k,l$为互不相同的正整数，则

- $(k\ l)(k\ a\ \cdots\ b)(l\ c\ \cdots\ d) = (k\ a\ \cdots\ b\ l\ c\cdots\ d)$;
- $(k\ l)(k\ a\ \cdots\ b\ l\ c\ \cdots\ d) = (k\ a\ \cdots\ b)(l\ c\cdots\ d)$;

Definition 12.12 (even and odd permutation)

- A permutation π is said to be even if its cycle decomposition contains an even number of even cycles; otherwise π is odd.

Theorem 12.13

A cycle can be decomposed further into a product of two element cycles, called transpositions.

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3)\cdots(i_{r-2} i_{r-1})(i_{r-1} i_r)$$

例：$(1,2,3,4,5) = (1,2)(2,3)(3,4)(4,5) = (1,5)(1,4)(1,3)(1,2).$

Fact 12.14

- *Any even permutation can be decomposed into even number of transpositions.*
- *Any odd permutation can be decomposed into odd number of transpositions.*

Definition 12.12 (even and odd permutation)

- A permutation π is said to be even if its cycle decomposition contains an even number of even cycles; otherwise π is odd.

Theorem 12.13

A cycle can be decomposed further into a product of two element cycles, called transpositions.

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3) \cdots (i_{r-2} i_{r-1})(i_{r-1} i_r)$$

例：$(1,2,3,4,5) = (1,2)(2,3)(3,4)(4,5) = (1,5)(1,4)(1,3)(1,2)$.

Fact 12.14

- *Any even permutation can be decomposed into even number of transpositions.*
- *Any odd permutation can be decomposed into odd number of transpositions.*

Definition 12.12 (even and odd permutation)

- A permutation π is said to be even if its cycle decomposition contains an even number of even cycles; otherwise π is odd.

Theorem 12.13

A cycle can be decomposed further into a product of two element cycles, called transpositions.

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3) \cdots (i_{r-2} i_{r-1})(i_{r-1} i_r)$$

例：$(1,2,3,4,5) = (1,2)(2,3)(3,4)(4,5) = (1,5)(1,4)(1,3)(1,2)$.

Fact 12.14

- *Any even permutation can be decomposed into even number of transpositions.*
- *Any odd permutation can be decomposed into odd number of transpositions.*

Definition 12.12 (even and odd permutation)

- A permutation π is said to be even if its cycle decomposition contains an even number of even cycles; otherwise π is odd.

Theorem 12.13

A cycle can be decomposed further into a product of two element cycles, called transpositions.

$$(i_1 i_2 \cdots i_r) = (i_1 i_2)(i_2 i_3)\cdots(i_{r-2} i_{r-1})(i_{r-1} i_r)$$

例：$(1,2,3,4,5) = (1,2)(2,3)(3,4)(4,5) = (1,5)(1,4)(1,3)(1,2).$

Fact 12.14

- *Any even permutation can be decomposed into even number of transpositions.*
- *Any odd permutation can be decomposed into odd number of transpositions.*

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a,b)为任意对换，则$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若$a, b \in \tau_1 = (ac_1c_2\ldots, c_kbd_1d_2\ldots d_h)$，则

    $$(a,b)\cdot\sigma = (ac_1c_2\ldots, c_k)(bd_1d_2\ldots d_h)\cdot\tau_2\cdot\tau_3\cdot\ldots\cdot\tau_s$$

    故$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若a, b分别处于σ的两个不同的轮换中，设$\tau_1 = (ac_1\ldots c_k)$，$\tau_2 = (bd_1\ldots d_h)$，则

    $$(a,b)\cdot\sigma = (ac_1c_2\ldots, c_kbd_1d_2\ldots d_h)\cdot\tau_3\cdot\tau_4\cdot\ldots\cdot\tau_s$$

    ，故$f((a,b)\sigma) = (-1)f(\sigma)$；故$f((a,b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h)\ldots(a_2b_2)(a_1b_1) = (c_kd_k)\ldots(c_2d_2)(c_1d_1)$则

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a, b)为任意对换，则$f((a, b)\sigma) = (-1)f(\sigma)$；
  - 若$a, b \in \tau_1 = (ac_1c_2\ldots, c_kbd_1d_2\ldots d_h)$，则
    $$(a, b)\cdot\sigma = (ac_1c_2\ldots, c_k)(bd_1d_2\ldots d_h)\cdot\tau_2\cdot\tau_3\cdot\ldots\cdot\tau_s$$
    故$f((a, b)\sigma) = (-1)f(\sigma)$；
  - 若a, b分别处于σ的两个不同的轮换中，设$\tau_1 = (ac_1\ldots c_k)$，$\tau_2 = (bd_1\ldots d_h)$，则
    $$(a, b)\cdot\sigma = (ac_1c_2\ldots, c_kbd_1d_2\ldots d_h)\cdot\tau_3\cdot\tau_4\cdot\ldots\cdot\tau_s$$
    ，故$f((a, b)\sigma) = (-1)f(\sigma)$；故$f((a, b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h)\ldots(a_2b_2)(a_1b_1) = (c_kd_k)\ldots(c_2d_2)(c_1d_1)$则

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a,b)为任意对换，则$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若$a, b \in \tau_1 = (ac_1c_2\ldots,c_kbd_1d_2\ldots d_h)$，则
    $$(a,b)\cdot\sigma = (ac_1c_2\ldots,c_k)(bd_1d_2\ldots d_h)\cdot\tau_2\cdot\tau_3\cdot\ldots\cdot\tau_s$$
    故$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若a, b分别处于σ的两个不同的轮换中，设$\tau_1 = (ac_1\ldots c_k)$，$\tau_2 = (bd_1\ldots d_h)$，则
    $$(a,b)\cdot\sigma = (ac_1c_2\ldots,c_kbd_1d_2\ldots d_h)\cdot\tau_3\cdot\tau_4\cdot\ldots\cdot\tau_s$$
    ，故$f((a,b)\sigma) = (-1)f(\sigma)$；故$f((a,b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h)\ldots(a_2b_2)(a_1b_1) = (c_kd_k)\ldots(c_2d_2)(c_1d_1)$则

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a,b)为任意对换，则$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若$a,b \in \tau_1 = (ac_1c_2\ldots,c_kbd_1d_2\ldots d_h)$，则

$$(a,b)\cdot\sigma = (ac_1c_2\ldots,c_k)(bd_1d_2\ldots d_h)\cdot\tau_2\cdot\tau_3\cdot\ldots\cdot\tau_s$$

    故$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若a,b分别处于σ的两个不同的轮换中，设$\tau_1 = (ac_1\ldots c_k)$，$\tau_2 = (bd_1\ldots d_h)$，则

$$(a,b)\cdot\sigma = (ac_1c_2\ldots,c_kbd_1d_2\ldots d_h)\cdot\tau_3\cdot\tau_4\cdot\ldots\cdot\tau_s$$

    ，故$f((a,b)\sigma) = (-1)f(\sigma)$；故$f((a,b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h)\ldots(a_2b_2)(a_1b_1) = (c_kd_k)\ldots(c_2d_2)(c_1d_1)$则

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a,b)为任意对换，则$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若$a, b \in \tau_1 = (ac_1c_2\ldots, c_kbd_1d_2\ldots d_h)$，则
    $$(a,b)\cdot\sigma = (ac_1c_2\ldots, c_k)(bd_1d_2\ldots d_h)\cdot\tau_2\cdot\tau_3\cdot\ldots\cdot\tau_s$$
    故$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若a, b分别处于σ的两个不同的轮换中，设$\tau_1 = (ac_1\ldots c_k)$，$\tau_2 = (bd_1\ldots d_h)$，则
    $$(a,b)\cdot\sigma = (ac_1c_2\ldots, c_kbd_1d_2\ldots d_h)\cdot\tau_3\cdot\tau_4\cdot\ldots\cdot\tau_s$$
    ，故$f((a,b)\sigma) = (-1)f(\sigma)$；故$f((a,b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h)\ldots(a_2b_2)(a_1b_1) = (c_kd_k)\ldots(c_2d_2)(c_1d_1)$则

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a,b)为任意对换，则$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若$a,b \in \tau_1 = (ac_1c_2\ldots,c_kbd_1d_2\ldots d_h)$，则
    $$(a,b)\cdot\sigma = (ac_1c_2\ldots,c_k)(bd_1d_2\ldots d_h)\cdot\tau_2\cdot\tau_3\cdot\ldots\cdot\tau_s$$
    故$f((a,b)\sigma) = (-1)f(\sigma)$；
  - 若a,b分别处于σ的两个不同的轮换中，设$\tau_1 = (ac_1\ldots c_k)$，$\tau_2 = (bd_1\ldots d_h)$，则
    $$(a,b)\cdot\sigma = (ac_1c_2\ldots,c_kbd_1d_2\ldots d_h)\cdot\tau_3\cdot\tau_4\cdot\ldots\cdot\tau_s$$
    ，故$f((a,b)\sigma) = (-1)f(\sigma)$；故$f((a,b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h)\ldots(a_2b_2)(a_1b_1) = (c_kd_k)\ldots(c_2d_2)(c_1d_1)$则

Theorem 12.15

将一个置换表示为对换的乘积，表示方法可能不唯一，但对换个数的奇偶性是唯一的。奇置换的对换个数必为奇，偶置换的对换个数必为偶。

给定一个n阶置换σ，设其分解为s个不相交的轮换$\sigma = \tau_1\tau_2\cdots\tau_s$(包括1-轮换)。定义函数$f(\sigma) = (-1)^{n-s}$。

- 对n阶恒等置换I，可得$f(I) = (-1)^{n-n} = 1$；
- 设(a, b)为任意对换，则$f((a, b)\sigma) = (-1)f(\sigma)$；
  - 若$a, b \in \tau_1 = (ac_1c_2 \ldots, c_kbd_1d_2 \ldots d_h)$，则
    $$(a, b) \cdot \sigma = (ac_1c_2 \ldots, c_k)(bd_1d_2 \ldots d_h) \cdot \tau_2 \cdot \tau_3 \cdot \ldots \cdot \tau_s$$
    故$f((a, b)\sigma) = (-1)f(\sigma)$；
  - 若a, b分别处于σ的两个不同的轮换中，
    设$\tau_1 = (ac_1 \ldots c_k)$，$\tau_2 = (bd_1 \ldots d_h)$，则
    $$(a, b) \cdot \sigma = (ac_1c_2 \ldots, c_kbd_1d_2 \ldots d_h) \cdot \tau_3 \cdot \tau_4 \cdot \ldots \cdot \tau_s$$
    ，故$f((a, b)\sigma) = (-1)f(\sigma)$；故$f((a, b)\sigma) = (-1)f(\sigma)$。
- 设$\sigma = (a_hb_h) \ldots (a_2b_2)(a_1b_1) = (c_kd_k) \ldots (c_2d_2)(c_1d_1)$则

- 设$\sigma = (a_h b_h)\ldots(a_2 b_2)(a_1 b_1) = (c_k d_k)\ldots(c_2 d_2)(c_1 d_1)$则

$$f(\sigma) = f(\sigma \cdot I) = (-1)^h = (-1)^k.$$

Fact 12.16

- *The product of two even permutations is even.*
- *The product of two odd permutations is even.*
- *The product of an even and an odd permutation is odd.*

- 设$\sigma = (a_h b_h)\ldots(a_2 b_2)(a_1 b_1) = (c_k d_k)\ldots(c_2 d_2)(c_1 d_1)$则

$$f(\sigma) = f(\sigma \cdot I) = (-1)^h = (-1)^k.$$

Fact 12.16

- *The product of two even permutations is even.*
- *The product of two odd permutations is even.*
- *The product of an even and an odd permutation is odd.*

Permutation groups

Definition 12.17 (symmetric group and alternating group)

- **Symmetric group 对称群:** the set S_n of all permutations of $\{1, 2, \ldots, n\}$.
- **Alternating group 交错群:** the subgroup A_n of all even permutations of $\{1, 2, \ldots, n\}$
- The group operation is composition of functions.

Fact 12.18

- $|S_n| = n!$.
- $n > 1$时， $|A_n| = \frac{1}{2}n!$

Permutation groups

Definition 12.17 (symmetric group and alternating group)

- **Symmetric group 对称群：** the set S_n of all permutations of $\{1, 2, \ldots, n\}$.
- **Alternating group 交错群：** the subgroup A_n of all even permutations of $\{1, 2, \ldots, n\}$
- The group operation is composition of functions.

Fact 12.18

- $|S_n| = n!$.
- $n > 1$时，$|A_n| = \frac{1}{2}n!$

Example 12.19

- S_3: $\{\sigma_1, \sigma_2, \ldots, \sigma_6\}$ with

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- A_3: $\{\sigma_1, \sigma_5, \sigma_6\}$ with

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Example 12.19

- S_3: $\{\sigma_1, \sigma_2, \ldots, \sigma_6\}$ with

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- A_3: $\{\sigma_1, \sigma_5, \sigma_6\}$ with

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

作业

P5， 习题1-1题目：4, 8

P16， 习题1-2题目：5, 12， 13， 16

P25， 习题1-3题目：5, 6, 7, 8, 18, 19

证明：如果$N = n_1 \cdot n_2$，且$\gcd(n_1, n_2) = 1$，那么$\mathbb{Z}_N^* \cong \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$。

P32， 习题1-4题目：3, 4,6

P40， 习题1-5题目： 1, 5, 12

P54. 习题1-6题目：5.(1)(4), 12, 24, 25