暗号で使う数学

吉田 努

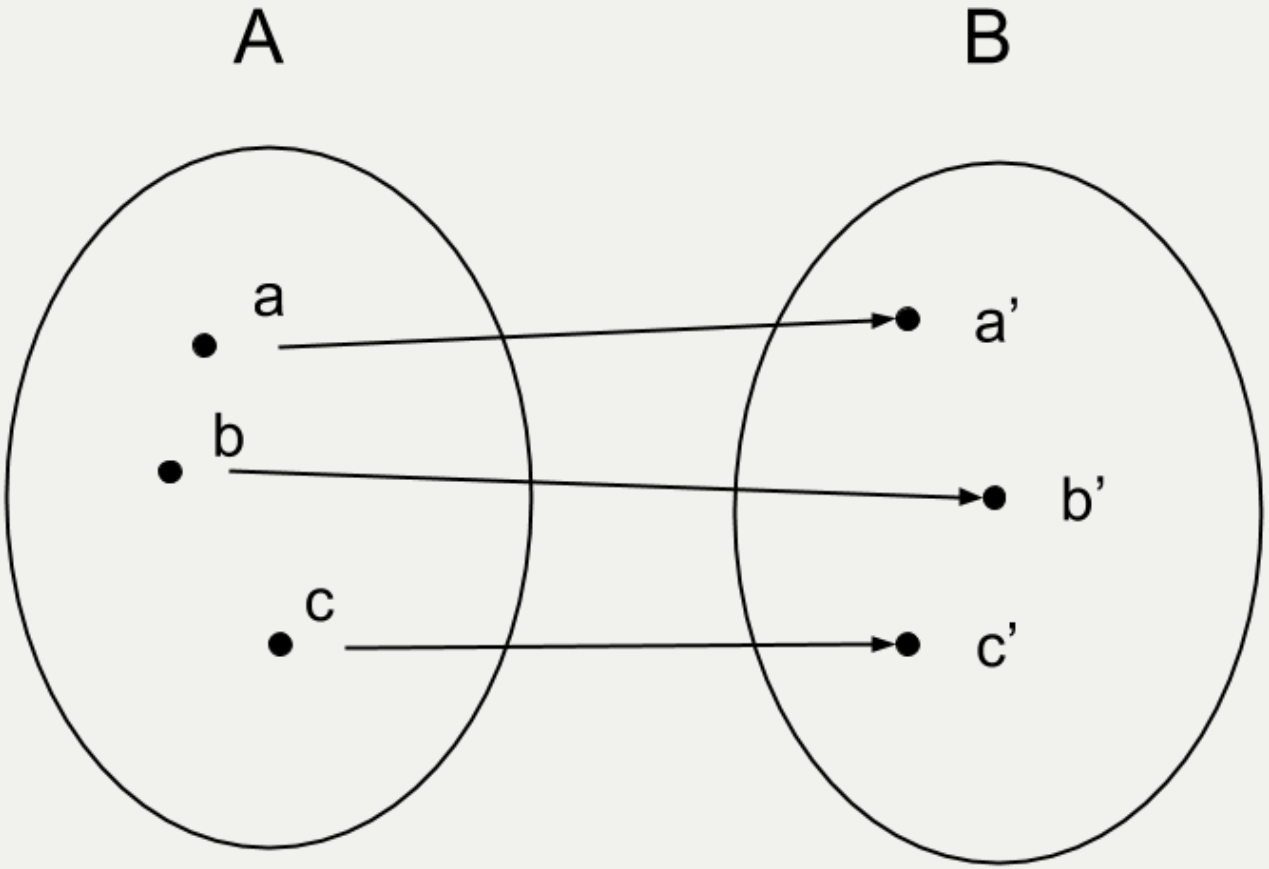
白勢研ゼミ 2016/05/09

今日の内容

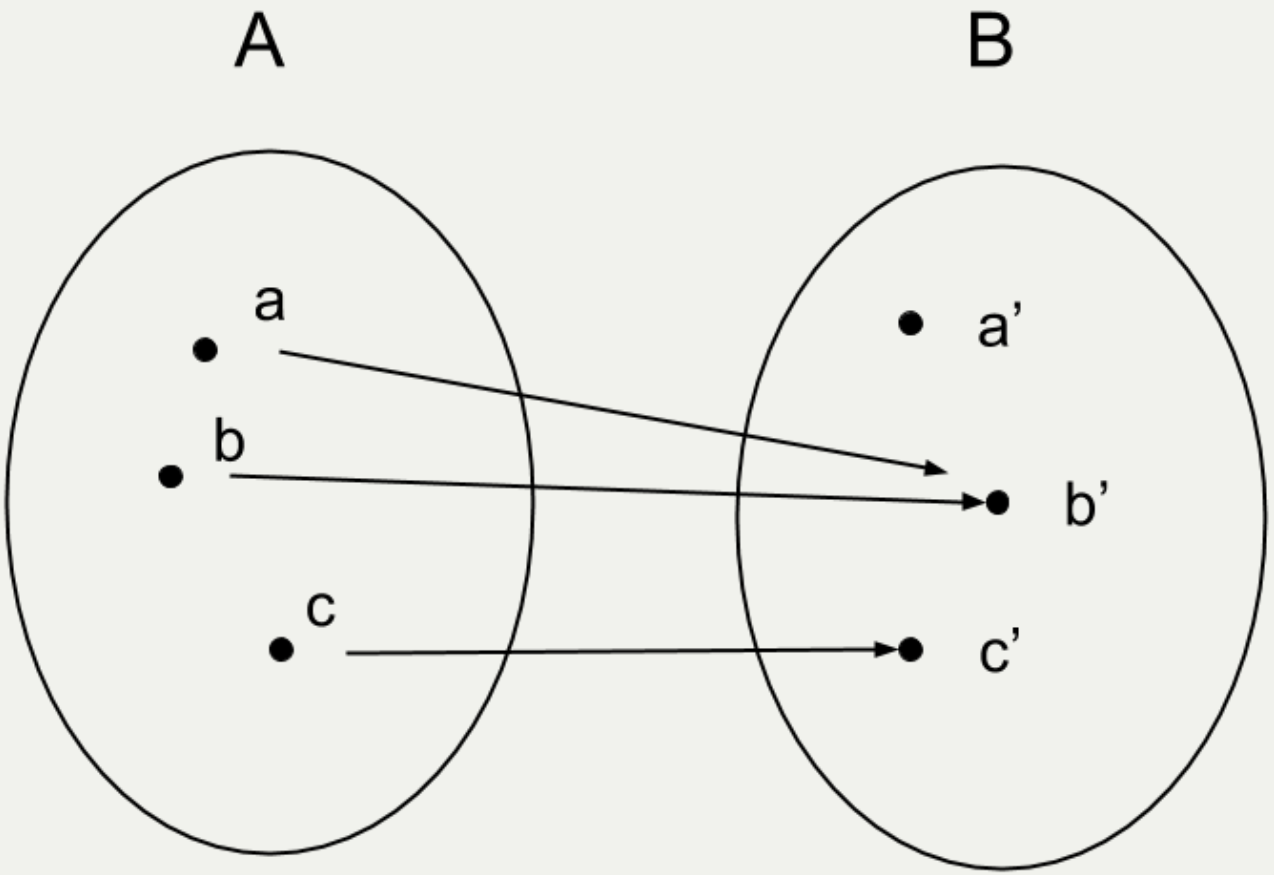
- 写像
- 演算
- 群

写像

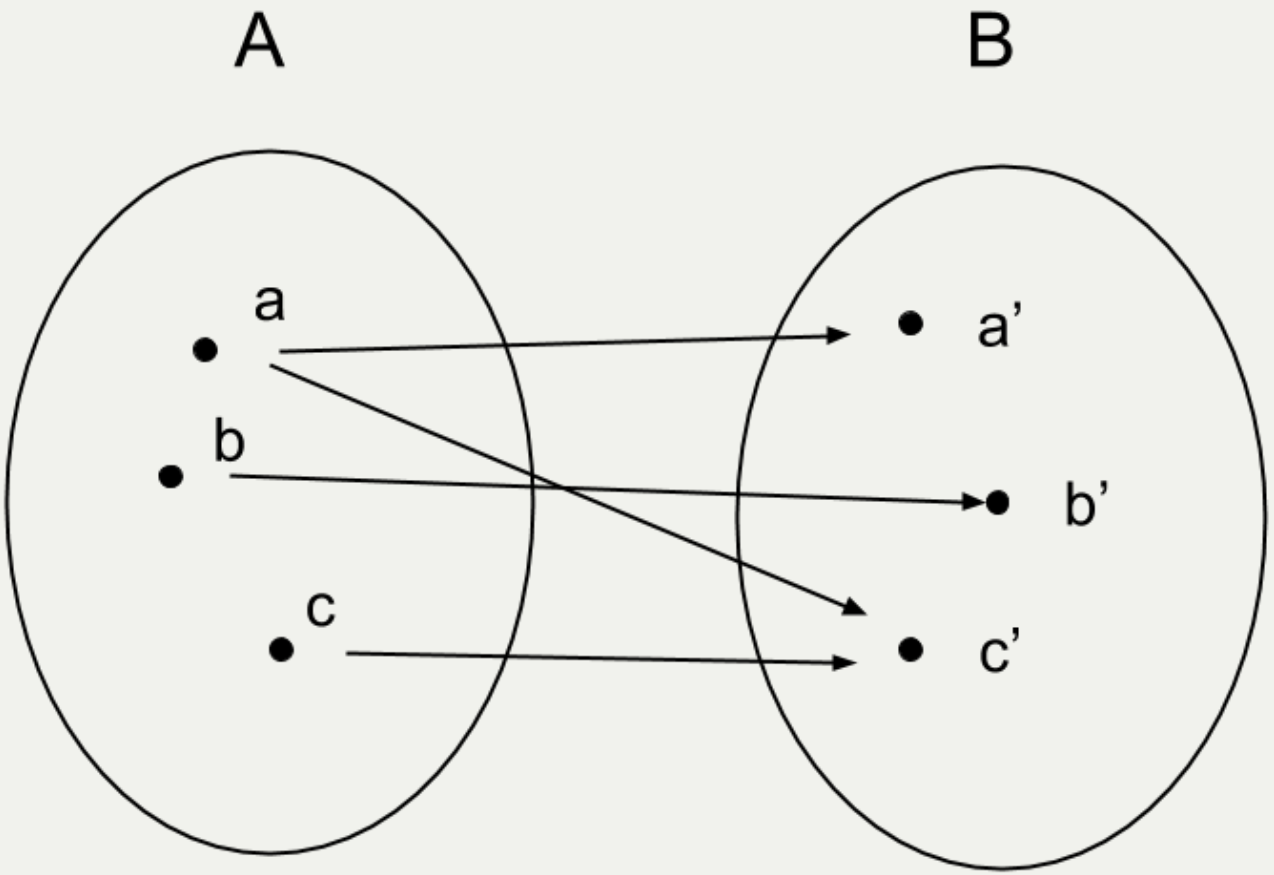
- 集合Aの各元に対して、集合Bの元がただ一つ対応する規則fが定まっているとき、この対応をAからBへの写像という
- $f : A \to B$



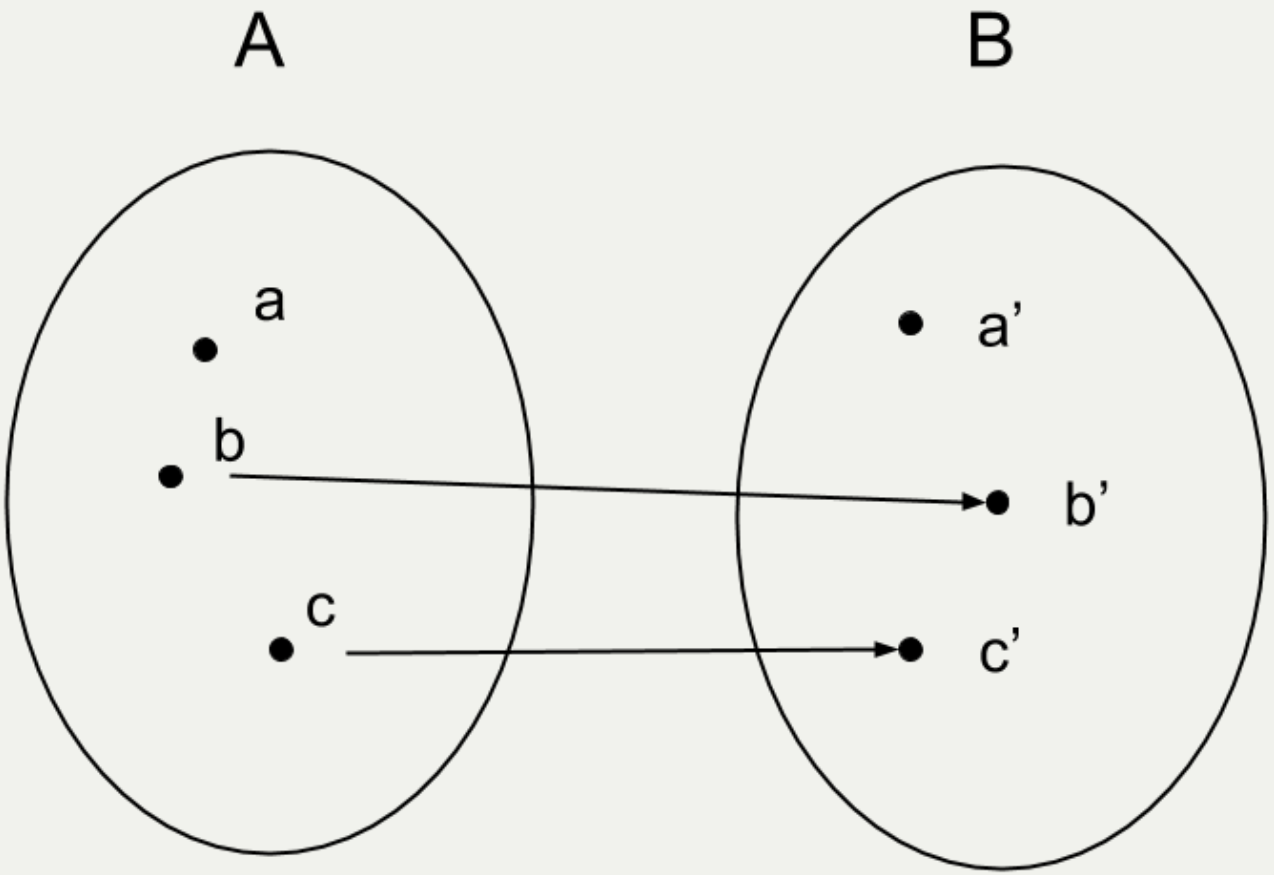
Quiz 1



Quiz 2



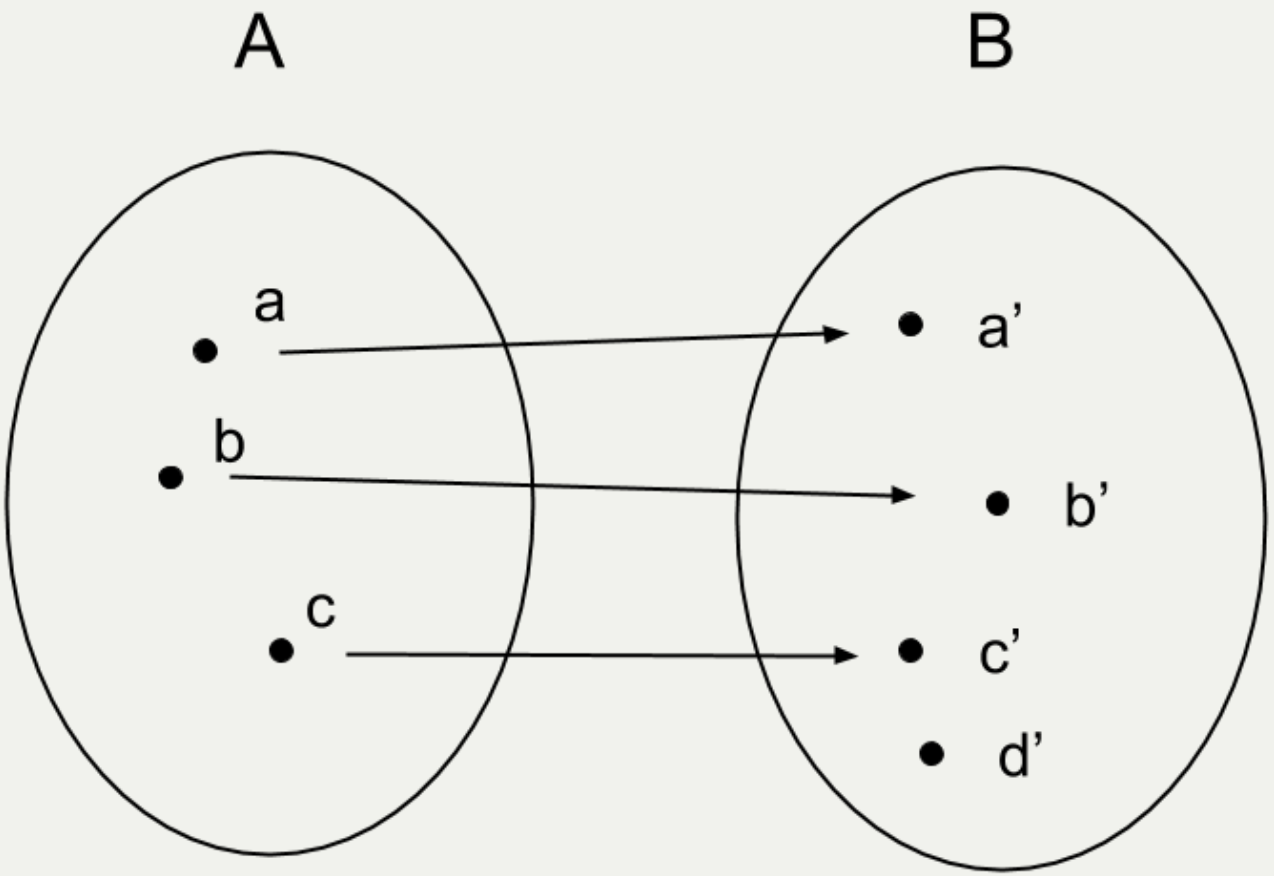
Quiz 3



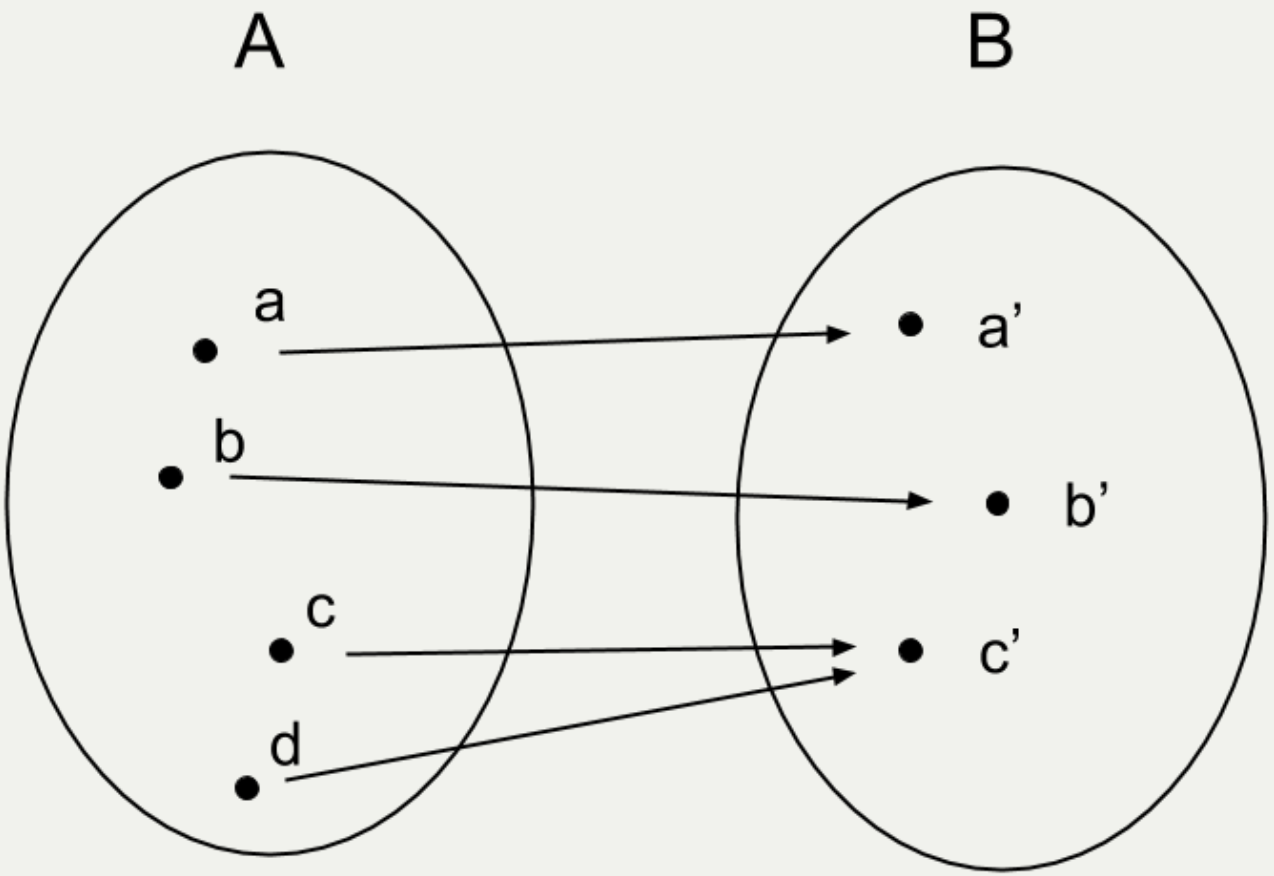
全射・単射

- 写像$f : A \to B$
- 全射
  - $\forall y \in B$に対して
    $f(x) = y$
    を満たす$x \in A$が存在する
- 単射
  - $x_1, x_2 \in A$が
    $f(x_1) = f(x_2)$
    ならば$x_1 = x_2$となる

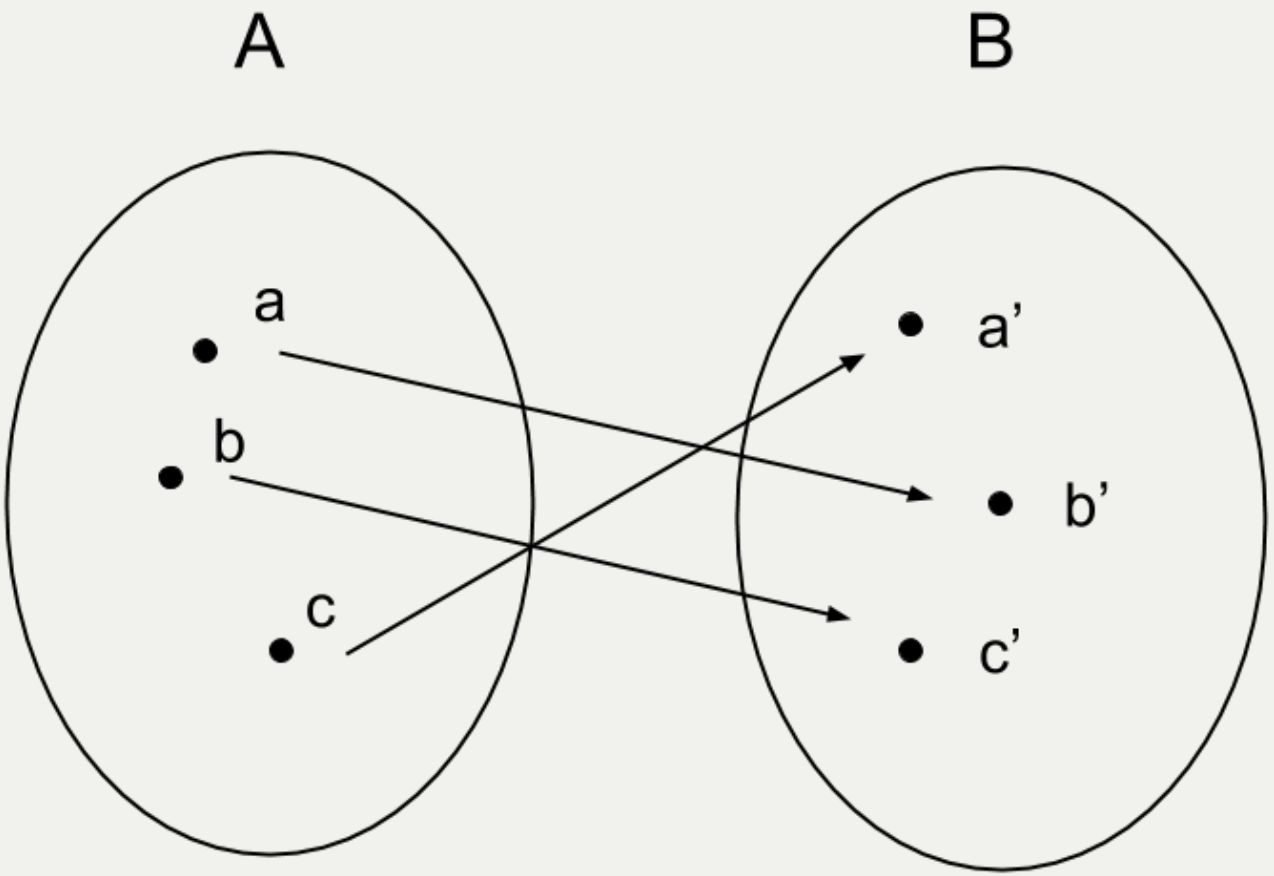
単射



全射



全単射



演算

- 演算は実は写像
- $f : A \times A \to A$ のような写像
- $(x_1, x_2) \mapsto f(x_1, x_2)$
  (ただし$x_1, x_2 \in A$)
- つまり、演算は常に集合Aに閉じている

群って何？

1. 単位元が存在する
2. 結合法則が成り立つ
3. 逆元が存在する

を満たす集合

群

- 集合Gが演算$\cdot$に対して以下を満たすとき群という
  1. (結合律)
     $a, b, c \in G$に対して, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  2. (単位元の存在)
     $\forall a \in G$に対して, $a \cdot e = e \cdot a = a$を満たす$e \in G$が存在する
  3. (逆元の存在)
     $\forall a \in G$に対して, $a \cdot a' = a' \cdot a = e$を満たす$a' \in G$が存在する
- 集合Gが演算$\cdot$に対して群であるとき$(G, \cdot)$と表す

可換群

- 群に加えて
  - (可換律)
    $a, b \in G$に対して, $a \cdot b = b \cdot a$を満たす
- アーベル群とも呼ぶ

群の具体例

- $(Z, +)$
  $= \{\cdots, -2, -1, 0, 1, 2, \cdots\}$
- 結合法則
  - 自明
- 単位元の存在
  - $a + 0 = 0 + a = a$
- 逆元
  - $a + (-a) = (-a) + a = 0$

部分群

- 群Gの部分集合Hが群Gの演算$\cdot$に関して群になる時、Hは群Gの部分群である

例1

- $(Z, +)$の部分集合$\{0\}$はZの部分群である
  - 結合法則
    - 自明
  - 単位元
    - $0 + 0 = 0$
  - 逆元
    - $0 + (-0) = 0$

例2

- $(Z, +)$の部分集合$3Z = \{\cdots, -3, 0, 3, \cdots\}$は$Z$の部分群である
  - 結合法則
    - 自明
  - 単位元
    - $0 + a = a + 0 = a$
  - 逆元
    - $a + (-a) = (-a) + a = 0$

Z/nZの正体

- 今まで何気なく出てきた
- $Z/5Z = \{0, 1, 2, 3, 4\}$?

剰余群

- 剰余類
  - G: 群
  - H: Gの部分群
  - $a \cdot H$の形の部分集合をGにおける剰余類という$(a \in G)$
- 剰余類の全体の集合
  - $G/H = \{a_i \cdot H\}$
  - $a \cdot H = \{a \cdot h | \forall h \in H\}$

結局のところ

- $Z/5Z = \{0 + 5Z, 1 + 5Z, 2 + 5Z, 3 + 5Z, 4 + 5Z\}$

その他

- ラグランジュの定理
- 環
- 体
- 拡大体
- 楕円曲線

何の役に立つの？

- 群の性質
- 公開鍵暗号が理解できた気になれる

群のまとめ

- 群は演算と集合の話
- 演算は何でもよい
- 3つの条件
  - 結合法則
  - 単位元の存在
  - 逆元の存在
- 部分群は意外と重要

参考文献

- 代数学から学ぶ暗号理論