暗号で使う数学2

吉田 努

白勢研ゼミ 2016/05/17

今日の内容

- 群
- ラグランジュの定理
- 環

前回

- 群とはある演算に関する集合の話
- 群が分かれば公開鍵暗号が理解できた気になる

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
  4. 演算が集合に閉じている

群の具体例

- $(\mathbb{Z}, +)$
  $= \{\cdots, -2, -1, 0, 1, 2, \cdots\}$
- 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
- !! 結構重要 !!
  - 詳しくはやらないが興味がある人は是非

剰余群

- 剰余類
  - G: 群
  - H: Gの部分群
  - aH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
  - $G/H = \{a_i H\}$
  - $aH = \{ah | \forall h \in H\}$

結局のところ

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

今回

Quiz

- $(\mathbb{Z}, +)$は群である
  - それでは, $(\mathbb{Z}, \times)$は群かどうか
- 群の条件
  - 演算が閉じている
  - 結合法則
  - 単位元がある
  - 逆元がある

Answer

- $(\mathbb{Z}, \times)$は群ではない
- 反例を探す
- 逆元
  - $3 \times a = a \times 3 = 1$
  - $a = 1/3 \notin \mathbb{Z}$

群の位数

- 群Gの元の個数$\#G$をGの位数という

べき全体のなす集合

- 群Gの元aに対してaのべき全体のなす集合を
$$\langle a \rangle$$
と表す
- $\langle a \rangle$は明らかにGの部分群になる
$$\langle a \rangle = \{a^k | k \in \mathbb{Z}\}$$

群の元の位数

- $a^k = 1$を満たす最小のk

群の位数と群の元の位数

- 位数という言葉は2つ使われる
- 群の位数
  - 群の元の数
- 群の元の位数
  - a^kを満たす最小の$k \in \mathbb{Z}$

同値関係

- ある集合Sにおいて二項関係$\sim$が以下を満たすとき$\sim$はSの同値関係である
  1. 反射律
     - $a \sim a$
  2. 対称律
     - $a \sim b \Rightarrow b \sim a$
  3. 推移律
     - $a \sim b \land b \sim c \Rightarrow a \sim c$

ラグランジュの定理

- 有限群Gの部分群Hにおいて、Hの位数はGの位数を割り切る
- 証明は結構難しい…はず
- 系が便利

ラグランジュの定理の系

- 位数lの有限群Gにおいて、$\forall a \in G$
$$a^l = 1$$
- 1は単位元

具体例

- $(\mathbb{Z}/5\mathbb{Z} - \{0\}, \times)$
  - $(\mathbb{Z}/5\mathbb{Z})^* = \{1, 2, 3, 4\}$
- $3^4 \equiv 81 \equiv 1 \pmod 5$

楕円曲線では

- $\forall P \in E(\mathbb{F}_5)$
- $l = \#E(\mathbb{F}_5)$
- $lP = O$

フェルマの小定理

- ネットワークセキュリティで登場?
- pを素数、rをpと互いに素な整数とするとき
$$r^{p-1} \equiv 1 \pmod{p}$$
が成り立つ

環

集合Rにおいて

1. 加法が可換群
2. $(ab)c = a(bc)$
3. 分配法則
    1. $a(b+c) = ab + ac$
4. 乗法の単位元の存在
5. 乗法の交換法則

参考文献

- 代数学から学ぶ暗号理論