類別とTepla

吉田 努

白勢研ゼミ 2016/05/30

前回

- 群
- ラグランジュの定理
- 環

今回

- 類別
- Tepla

類別がものすごく重要らしい

- 「類別」という概念は人間の精神およびその歴史の中でもっとも原初的・根源的な位置を占めていることが理解される
- 基本的な概念にもかかわらず, 類別という概念が明確に定式化されたのはごく最近のことのようである
- 数字自身が類別という手段によって抽象化された存在である
- 抽象代数 -> 商群 -> 同値律 なのでは？

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
     - $a \sim b \land b \sim c \Rightarrow a \sim c$

等号

- 基本的にどんな集合でもよい？
  1. 反射律
     - $a = a$
  2. 対称律
     - $a = b \Rightarrow b = a$
  3. 推移律
     - $a = b \land b = c \Rightarrow a = c$

合同

- 整数mを法とする合同(≡)

1. 反射律
   - $a \equiv a \pmod{m}$
2. 対称律
   - $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. 推移律
   - $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

剰余群

- Gを群, Hをその部分群とする
- aH(a $\in$ G)の形の部分集合をHの剰余類という
- $aH = bH \Leftrightarrow ab^{-1} \in H$
  - aとbはHを法として合同
- Hを法として合同という関係は同値関係である

具体例 $\mathbb{Z}/7\mathbb{Z}^*$

- $G = Z/7Z^* = \{1, 2, 3, 4, 5, 6\}$
- $H = \langle 2 \rangle = \{2^0, 2^1, 2^2\} = \{1, 2, 4\}$
  - $1H = \{1, 2, 4\}$
  - $2H = \{2, 4, 1\}$
  - $3H = \{3, 6, 5\}$
  - $4H = \{4, 1, 2\}$
  - $5H = \{5, 3, 6\}$
  - $6H = \{6, 5, 3\}$

具体例: $\mathbb{Z} / 7\mathbb{Z}^*$

- $G = 1H \cup 3H$
  と表すことができる
  - $1H = \{1, 2, 4\}$
  - $3H = \{3, 6, 5\}$

つまり

- $G = 1H \cup 3H$
- $|G| = 2 \times |H|$
  - $6 = 2 \times 3$
- $|G:H|$をHのGにおける指数という

ラグランジュの定理

- Gを有限群, その部分群をHとする Hの位数はGの位数を割り切る

Tepla

- 筑波大学が作成したペアリング演算ライブラリ
- C言語
- GMPとOpenSSLを必要とする
- 提供する機能
  - 有限体上の演算
  - 楕円曲線の演算
  - ペアリング演算
- 最近version 2がリリースされた

GMP

- 任意精度演算
  - 要するに巨大な桁数が簡単に計算できる
- 自分で作るのは難しい

なにができそうか

- ペアリングを使った暗号の構築
  - IDベース暗号
  - タイムリリース暗号
  - プロキシ暗号
- 楕円曲線暗号系の実装
  - 使える楕円曲線が決まっている
  - 余り面白くないかもしれない
  - GMPを使って実装するよりは楽？

Documentを見る

sampleを見る

参考文献

- 代数学から学ぶ暗号理論