

研究テーマ：素体について

名列番号 080 氏名 野崎 将人

1. まえがき

数は現実には無限に存在し、加減乗除などの演算はその上で成り立っている。しかし、コンピュータ上で数をあつかう際はメモリが有限であるため、数も有限のものしか扱うことが出来ない。そのため、有限体という考え方が有効である。また有限体は符号理論においても数学的基礎をなしており、暗号を作成する際などにも頻繁に用いられる。本研究では有限体についての理解を深めることを目的とする。

2. 研究内容

有限体は、元の個数が素数のものしか構成できない事が知られている。そこで実際にある程度の有限体を構成しそれを確かめると同時に、なぜ元の個数が素数のときしか有限体が構成できないのかを考察する。また、構成可能な有限体の数を増やすための概念である拡大体についても調査する。

3. 研究結果

表 1 に元の個数を変化させたときの有限体が構成できたかどうかを示す。結果の欄の○は構成できた、×は構成できなかったことを表す。やはり元の個数が素数の時しか有限体が構成できなかったことが確かめられた。構成できなかったときの理由としては、ある元に対する乗法逆元が存在しないことが主な理由である。これについての証明は長くなるためここでは省略し、最終レポートに記す。

元の個数 N	結果
2	○
3	○
4	×
5	○
6	×
7	○
8	×
9	×
10	×
11	○
12	×
13	○
14	×
15	×
16	×
17	○
18	×
19	○
20	×

表 1 有限体の構成結果

4. 感想

今回の研究を通して、体について理解を深めることができた。今後は拡大体についてさらに理解を深めていけるよう学んでいきたいらいいと思う。

参考文献

今井秀樹著「符号理論」
社団法人電子情報通信学会出版