

2 学期開始時までの課題

1 次にあげる本，または数学に関連していて下記の本と同レベルと考えられる本の中から 1 冊を選び，そこに書かれている内容のうち興味を持った部分について，自分なりに整理し，さらに考えたことを述べよ．字数は 3000 字から 4000 字を基準とする．

- クロード・E. シヤノン，ワレン ウィーバー「通信の数学的理論」(ちくま学芸文庫) ISBN-13: 978-4480092229 (または原書「Mathematical Theory of Communication」ISBN-13: 978-0252725487)
- ジョセフ・メイザー「数学と論理をめぐる不思議な冒険」(日経 BP 社) ISBN: 4822282694
- 市川伸一「考えることの科学」(中公新書) ISBN: 412101345X
- 野矢茂樹「無限論の教室」(講談社現代新書) ISBN: 4061494201
- サイモン・シン「暗号解読 上・下」(新潮文庫) 上: ISBN: 410215972X, 下: ISBN: 4102159738

2 $\mathbf{F}_2 = \{0, 1\}$ を係数とする多項式で，それよりも次数の低い多項式の積に因数分解できない多項式を \mathbf{F}_2 上の既約多項式という． \mathbf{F}_2 の 5 次以下の既約多項式をすべて求めよ．(できれば，6 次の既約多項式も求めよ．)

3 \mathbf{F}_{16} は通常 $\beta^4 + \beta + 1 = 0$ をみたす元 β を用いて， $\mathbf{F}_{16} = \{a\beta^3 + b\beta^2 + c\beta + d \mid a, b, c, d \in \mathbf{F}_2\}$ の形に表される． \mathbf{F}_{16} の 0 以外のすべての元を β^k ($0 \leq k \leq 14$) の形に表せ．[復習]

4 0 以外の元 a に対し， $a^m = 1$ となる最小の正整数 m を a の位数という．

- a) \mathbf{F}_8 の 0 以外の元は $\alpha^3 + \alpha + 1 = 0$ をみたす元 α を用いて， $\{\alpha^k \mid 0 \leq k \leq 6\}$ と表される． \mathbf{F}_8 の 0 と 1 以外の元の位数はすべて 7 であることを示せ．
- b) \mathbf{F}_{16} の 0 以外のすべての元 β^k ($0 \leq k \leq 14$) について，その位数を求めよ．

5 a) $x^{15} - 1$ を \mathbf{F}_2 上で因数分解せよ．

- b) $x^{15} - 1$ は \mathbf{F}_{16} 上では $x^{15} - 1 = (x - 1)(x - \beta)(x - \beta^2) \cdots (x - \beta^{14})$ と因数分解できることを示せ．
[ヒント: 因数定理を用いるとよい]

- c) a) で求めた $x^{15} - 1$ の \mathbf{F}_2 上での各因数を \mathbf{F}_{16} 上で $(x - \beta^k) \cdots (x - \beta^l)$ の形に因数分解せよ．

6 a) $g(x) = (x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ を生成多項式とする長さ 15 の巡回符号の符号語をすべて求めよ．

- b) 上で構成した符号に対し， $(011000011100100) = x + x^2 + x^7 + x^8 + x^9 + x^{12}$ を受信した．これに最も近い符号語を探すことにより，誤りを訂正せよ．

参考文献: 東工大 植松友彦先生の「代数系と符号理論」講義ノート．

<http://www.ocw.titech.ac.jp/index.php?module=General&action=T0300&GakubuCD=101&GakkaCD=53&Kougicd=7222&Nendo=2007&Gakki=1&lang=JA&vid=05>

連絡先: kuwata@tamacc.chuo-u.ac.jp

<http://c-faculty.chuo-u.ac.jp/~kuwata> も随時更新しますので，訪ねてみてください．