

## Error correcting codes: problem set 1

---

1. Finish problem set 0 !
2. Write  $i_m$  for the number of irreducible binary polynomials. Compute  $i_1, i_2, i_3, i_4, i_5, i_6, i_7$  and  $i_8$ . Verify that, for these values of  $m$ , we have

$$2^m = \sum_{d|m} d \cdot i_d.$$

3. Construct fields of order 4, 8 and 32, giving their addition and multiplication tables.
4. Construct a field of order 27.
5. (a) Construct a field  $F$  of order 16 using the polynomial  $X^4 + X^3 + X^2 + X + 1$ .  
 (b) Find a root  $\gamma$  of  $X^4 + X^3 + 1$  in this field.  
 (c) Construct another field  $F'$  of order 16 with the polynomial  $X^4 + X^3 + 1$ .  
 (d) Let  $\delta$  be a root of  $X^4 + X^3 + 1$  in  $F'$ . Show that  $\varphi: F' \rightarrow F'$  with  $\varphi(\delta^k) := \gamma^k$  is a field isomorphism.
6. Find all subfields of the fields you constructed in Ex.3.
7. Look at the field  $F$  of Ex.5.
  - (a) Show that if  $\varphi$  is any automorphism of  $F$  with  $\varphi(\gamma) = \beta$ , then  $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$ .
  - (b) Find all automorphisms of  $F$ .
8. Show that the elements of proper subfields of the field  $F$  of Ex.5 are precisely those  $\beta$  for which  $\beta^k = \beta$  for some  $k = 2^j$ , with  $j \mid 4$ . Show that the last condition is necessary.
9. Show that in a finite field of characteristic  $p$  every element has exactly one  $p$ -th root.
10. What are the primitive elements of the field of order 32 of Ex.3?
11. Show that a field of order 1024 always contains elements  $\beta$  and  $\gamma$  of orders 33 and 93. For such elements we have  $\beta^{11} = \gamma^{31}$  or  $\beta^{11} = \gamma^{-31}$ . We assume that  $\beta^{11} = \gamma^{31}$ . Verify that, in this case,  $(\beta\gamma)^{341} = \beta^{11}\gamma^{-31} = 1$ . But, as  $3 \nmid 341$ , the order of  $\beta\gamma$  is not a multiple of  $\text{ord}(\beta)$  or of  $\text{ord}(\gamma)$ .