Assignment on Algebra for Coding Theory

EE512: Error Control Coding

Questions marked (Q) or (F) are questions from previous quizzes or final exams, respectively.

1. (a) Write down the addition and multiplication tables for GF(5) and GF(7).
   (b) Write down the addition and mulitplication tables for GF(4).
2. Construct GF(16) in three different ways by defining operations modulo the irreducible polynomials x^4+x+1, x^4+x^3+1, and $x^4+x^3+x^2+x+1$. Find isomorphisms between the three constructions.
3. (a) Find all polynomials of degree 2 and degree 3 that are irreducible over (a) GF(2) and (b) GF(3). Identify the irreducible polynomials that are primitive.
   (b) Construct GF(9) in two different ways using a primitive and a non-primitive irreducible polynomial. Identify a primitive element in each construction, and find an isomorphism between the two constructions.
4. (a) Find the order of each element of GF(9) and GF(16). Identify all the primitive elements.
   (b) Repeat the same for GF(32). Under what conditions do all non-zero, non-unity elements of GF(p^m) become primitive?
5. (a) Find the order of each element of GF(7) and GF(11). Identify all the primitive elements.
   (b) Can all non-zero, non-unity elements of GF(p) (p: prime) be primitive for $p > 3$? What about $p = 3$?
6. (a) Show that all elements of GF(2^m) have square roots.
   (b) Show that all elements of GF(p^m) have p-th roots.
7. Let x, y be non-zero elements of GF(16) (α is primitive satisfying $\alpha^4+\alpha+1 = 0$). Given $x+y = \alpha^{14}$ and $x^3 + y^3 = \alpha$, find x and y.
8. Consider GF(16) with α primitive satisfying $\alpha^4 + \alpha + 1 = 0$.
   (a) Find all solutions to the simultaneous equations $x + y = \alpha^3$ and $x^2 + y^2 = \alpha^6$.
   (b) Find all solutions to the simultaneous equations $x + y = \alpha^3$ and $x^2 + y^2 = \alpha$.
9. Let x, y, z be distinct, nonzero elements of GF(64). Find some x, y and z such that $x^3+y^3+z^3 = 0$. Given such x, y, z, evaluate $x^{33} + y^{33} + z^{33}$.
10. (a) Factor $x^5 - 1$ over (a) GF(16) and (b) GF(2) and (c) GF(11). In which cases do you get linear factors?
    (b) For what primes p does $x^5 - 1$ factor into linear factors over GF(p)?
11. (a) Find the minimal polynomial of each element of GF(9) and GF(16).
    (b) If the degree of the minimal polynomial of an element of GF(p^m) equals m, is the element primitive?
12. (a) Consider the set $S = \{x + y\sqrt{2} : x, y \in Z\}$, where Z is the set of integers. Show that S with conventional addition and multiplication forms a commutative ring with unity. Is S an integral domain? Is S a field?
    (b) Consider the set $S = \{x + y\sqrt{2} : x, y \in Q\}$, where Q is the set of rational numbers. Show that S with conventional addition and multiplication forms a commutative ring with unity. Is S an integral domain? Is S a field?

13. (a) Consider the ring of integers Z. Describe all elements of $< 4 >$, the ideal generated by 4. Describe all elements of $< 4, 6 >$.

    (b) Consider the ring of polynomials with real coefficients $R[x]$. Describe all elements of the ideals $< x^2 - 1 >$, $< x^2 - 1, x^3 - 1 >$, $< x^2 - 1, x^4 - 1 >$, and $< x^2 - 1, x^3 - 1, x^4 - 1 >$.

14. (a) Consider the ring $Z_{18} = \{0, 1, 2, 3, \cdots, 16, 17\}$ with addition and multiplication performed modulo 18. Show that Z_{18} is not an integral domain by finding zero divisors.

    (b) Find the elements of Z_{18} that have and do not have a multiplicative inverse. Find $< 2 >$ and $< 5 >$ in Z_{18}. For what $a \in Z_{18}$ does $< a >= Z_{18}$?

15. (a) In the ring Z_{18}, find $b \neq 2$ such that $b \times 3 = 2 \times 3$.

    (b) Consider $Z_{18}[x]$, the ring of polynomials with coefficients from Z_{18}. Find $a, b \in Z_{18}$ ($a \neq 1$) such that $2x(x + 1) = 2x(ax + b)$ in $Z_{18}[x]$. Is $Z_{18}[x]$ an integral domain?

16. (a) Consider $R_4 = GF(2)[x]/(x^4 + 1)$, the ring of polynomials with binary coefficients, with operations defined modulo $x^4 + 1$. Show that R_4 is a commutative ring with unity.

    (b) Find all elements of $< x^2 + 1 >$ in R_4. Find a degree-2 polynomial $a(x) \in$GF$(2)[x]$ such that $x(x^2 + 1) = a(x)(x^2 + 1)$ in R_4. Is R_4 an integral domain?

    (c) Find all elements of $I =< x^2 + 1, x^3 + 1 >$ in R_4. Find $g(x) \in I$ such that $I =< g(x) >$.

17. Let $\alpha \in$GF(2^3) be primitive with $\alpha^3 = \alpha + 1$.

    (a) Factor $f(x) = x^3 + \alpha^6 x^2 + \alpha x + \alpha^6$ over GF(2^3).

    (b) Factor $f(x) = x^3 + \alpha^6 x^2 + \alpha^5 x + 1$ over GF(2^3).

18. Perform the following factorizations:

    (a) $x^7 + 1$, $x^9 + 1$, $x^{11} + 1$, $x^{17} + 1$, $x^{21} + 1$, $x^{31} + 1$, $x^{51} + 1$ over GF(2).

    (b) $x^2 + 1$, $x^4 + 1$, $x^8 + 1$, $x^{13} + 1$ over GF(3).

19. Find the splitting field (smallest field in which a polynomial factors into linear factors) for the following polynomials:

    (a) $x^3 + 1$, $x^{13} + 1$, $x^{23} + 1$, $x^{33} + 1$ with coefficients from GF(2).

    (b) $x^2 - 1$, $x^{11} - 1$, $x^{22} - 1$, $x^{31} - 1$ with coefficients from GF(3).

20. Let $\alpha \in$ GF(2^6) be a primitive element. It is easy to see GF$(2) = \{0, 1\} \subseteq$ GF(2^6). Find GF(2^2) and GF(2^3) in terms of α as subsets of GF(2^6). Interpret isomorphism as equality for this question.