

## Math 558 Spring 2009

### Review for second exam

#### I. Calculations

1. Find the remainder in  $\mathbb{Z}_7[x]$  when you divide  $x^{143} + 3x$  by  $x + 6$ . [Hint: don't even think of dividing.]

2. Factor  $x^4 + 1$  completely in  $\mathbb{Z}_2$ .

3. Using the Euclidean algorithm, find a gcd of  $x^4 + x^2 + 3$  and  $x^6 + 4x^4 + x^2 + 4$  in (a)  $\mathbb{R}$ ; (b)  $\mathbb{Z}_5[x]$ .

4. If  $x^3 + ax^2 + bx + c$  has roots  $r, -r, r^2$ , what are  $a, b, c$ ?

5. If  $\deg P = 8$  and  $P$  has roots (counting multiplicities)  $r, r, s, s, -r, -r, -s, -s$ , what is the coefficient of  $x^7$ ? Of  $x^6$ ? What is the constant term?

6. (a) Show that  $x^3 + x + 4$  is irreducible in  $\mathbb{Z}_{11}$ .

(b) If  $\gamma$  is a Galois imaginary for  $x^3 + x + 4$  over  $\mathbb{Z}_{11}$ , what's  $\gamma^5$ ?

7. For each of the following functions, say whether it is invariant. If it is not invariant, say how many variants it has:

(a)  $rst + stu$

(b)  $\frac{rst}{r+s+t+u}$

(c)  $rs + rst + rstu$

8. Let  $f = x_1x_2 + x_3x_4 + x_5x_6$ .

(a) if  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 1 & 2 \end{pmatrix}$ , what's  $\sigma f$ ?

(b) If  $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 1 & 2 & 4 \end{pmatrix}$ , what's  $\tau f$ ?

(c) Are any of  $f, \sigma f, \tau f$  equal?

9. Which permutations leave  $x_1x_2 + x_1x_3 + x_1x_4$  invariant?

10. Write a function of three variables that has exactly two variants.

11. Let  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 10 & 6 & 7 & 4 & 8 \end{pmatrix}$

(a) Decompose  $\sigma$  into disjoint cycles.

(b) What's  $\sigma^{-1}$ ?

12. Let  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 9 & 1 & 2 & 3 & 10 & 6 & 7 & 4 & 8 \end{pmatrix}$ ,  $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 8 & 2 & 9 & 7 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$ .

What's  $\sigma\tau$ ?

13. Decompose (13542) as a composition of transpositions in two distinct ways.

#### II. Short Answer

1. Yes or no:

(a) In  $R[x]$  are there polynomials  $A, B$  so  $(x^2 - 1)A + (x^4 - 1)B = 5x - 5$ ?

(b) In  $R[x]$  are there polynomials  $A, B$  so  $(x^2 - 1)A + (x^4 - 1)B = 5x^2 - 5$ ?

2. Look at problem I.6. Why would it be really mean for me to ask you the order of  $\gamma$ ?

3. Suppose  $\deg P = 5$  and  $P$  is irreducible over  $\mathbb{Z}_7$ .
  - (a) Is there an element  $\alpha$  in  $GF(7, P)$  with  $o(\alpha) = 10$ ? Briefly explain.
  - (b) Is there an element  $\beta$  in  $GF(7, P)$  with  $o(\beta) = 2801$ ? Briefly explain.
4. Suppose for every  $\alpha \in GF = GF(p, P)$  with  $\alpha \neq 0, 1$ ,  $o(\alpha) = 7$ . What can you say about  $\#GF^+$ ? About  $p$ ? About  $P$ ?
6. Can a function of 20 variables have exactly 18 variants? Briefly explain.
- \* 7. Which of the following is a group? Briefly explain.
  - (a) The set of even permutations in some  $S!$
  - (b) The set of odd permutations in some  $S!$
  - (c) The set of permutations in  $S_7$  that leave 3 fixed.
  - (d) The set of permutations  $\sigma$  in  $S_7$  for which  $\sigma(2) = 5$ .
  - (e)  $\{1, 3, 5\}$  in  $(\mathbb{Z}_7, \cdot)$ .
  - (f)  $\{1, 3, 5\}$  in  $(\mathbb{Z}_7, +)$ .
8. For which elements  $\alpha$  of  $GF(3, P)$  does  $\alpha = -\alpha$ ?

### III. Proofs and explanations

1.  $x^4 + 1$  is irreducible in  $\mathbb{Z}_3$ . Why?
  2. Let  $P$  be a linear polynomial which is not constant, and let  $Q$  be any polynomial. Prove there there are polynomials  $A, B$  so  $AP + BQ = 1$  iff  $P, Q$  have no zeroes in common.
  3. (a) Prove that if  $p$  is a prime,  $p > 2$ , and  $P$  is irreducible over  $p$ , then the sum of the elements of  $GF(p, P)$  equals 0.
    - (b) Prove that if  $p$  is a prime,  $p > 2$ , and  $P$  is irreducible over  $p$ , then the product of the elements of  $GF(p, P)^+$  equals -1.
    - (c) Does (a) hold for  $\mathbb{Z}_2$ ?
    - (d) Prove that (b) holds if  $p = 2$ .
- [Remark: Yes, (a) and (b) were homework problems. But this time I want a short and elegant proof.]
4. Show that if  $\tau f = f$  for all transpositions  $\tau$  then  $f$  is invariant.
  5. Show by induction that if  $\sigma f = f$  then  $\forall k \in \mathbb{N} \sigma^k f = f$ .
  - \*6. Show that if  $(G, \circ)$  is a group then  $g \circ h = g \circ h'$  iff  $h = h'$ .<sup>1</sup>

### IV. To memorize

1. Definition of primitive element of a Galois field.
2. Definition of permutation.
3. Definition of Galois polynomial.
3. Outline of proof that every Galois field has a primitive element. I.e., state the technical lemma needed, and then give the proof that the theorem follows from the technical lemma.
4. Proof that if a Galois field has a primitive element, then every element is a zero of the Galois polynomial. [This proof is not in the book, but we did it in class and it is very simple.]

---

<sup>1</sup> $\circ$  is just a group operation, it need not be composition.

5. Statement of Cauchy's theorem about variants of a function.
6. The proof that if  $f$  is a function of several variables, and  $\sigma$  is a permutation of these variables, then there is  $k$  so  $\sigma^k f = f$
7. The proof that if  $\sigma$  is a permutation and  $o(\sigma) = m$  then  $\{Id, \sigma, \sigma^2, \dots, \sigma^{k-1}\}$  is a group.
8. Definition of a group.