

NAME \_\_\_\_\_

Id. No, \_\_\_\_\_

Second Examination, Math 453, Fall 03 8:30MWF Wilkerson Section.

November 20, 2003, 7:30PM-9:00PM, University 317

No notes, books, calculators, tape players, earphones. Show all work. Use back of pages for scratch. Ask if you have questions on how much work needs to be shown, or what can be assumed.

Problem	Score
1.(20)	
2.(20)	
3.(20)	
4.(20)	
5.(20)	
Total(100)	

1. Axioms and definitions. 20 points.

a) State the operations and axioms for a field. Give three examples.

b) State the operations and axioms for a group. Give three examples.

2. Computations in symmetric groups. 20 points. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$$

a) Write  $\sigma$  in disjoint cycle form.

b) Write  $\sigma$  as a composition of transpositions.

c) Compute the parity or sign of  $\sigma$  in two different ways.

d) Compute the inverse  $\sigma^{-1}$  of the above  $\sigma$  and express it in disjoint cycle form.

**3.** Finite Galois fields . 20 points. Let  $P(x) = x^3 + x + 1$  in  $Z/2Z[x]$ .

a) Prove that  $P(x)$  is irreducible.

b) List the non-zero elements of  $GF(2, P(x)) = F$  and write out the multiplication table.

c) List all the primitive elements of  $F$ .

d) How many roots does the polynomial  $Q(x) = x^2 + x + 1$  have in  $GF(2, P(x)) = F$ ?

4. Polynomials . 20 points.

a) Find the GCD of  $P(x) = x^5 + x + 1$  and  $Q(x) = x^6 + x^5 + x^4 + x^3 + 1$  over  $Z/2Z$ .

b) Find polynomials  $A(x)$  and  $B(x)$  such that for the  $P$  and  $Q$  above,

$$A(x)P(x) + B(x)Q(x) = GCD$$

5. Groups, subgroups, and cosets.

Let  $G$  be the symmetric group  $S_4$  on  $\{1, 2, 3, 4\}$ , and  $H$  be the subgroup on  $\{1, 2, 3\}$ .

a) What are the orders of  $G$  and  $H$  and the index of  $H$  in  $G$ .

b) List the cosets of  $H$  in  $G$ . The list should account for all the elements of  $G$ .

c) Find a function  $f(x_1, x_2, x_3, x_4)$  such that  $H = S_{4,f}$ , the subgroup of permutations that fix  $f$ .

d) Find elements  $\sigma$  and  $\tau$  in  $G$  such that  $\sigma\tau \neq \tau\sigma$ .