SWARTHMORE COLLEGE
Department of Mathematics and Statistics
Honors Examination

Honors Exam
May, 1998

Modern Algebra I and Coding Theory

INSTRUCTIONS: Try to do all six problems on this exam.

Part I

Let C_n denote the cyclic group of order n and let S_n denote the symmetric group on n letters.

1.) (a) Find a non-trivial homomorphism (or prove that there is none) from
(i) C_2 to C_4.
(ii) C_4 to C_2.
(iii) C_2 to C_3.
(iv) C_4 to S_3.
(v) S_3 to C_4.

(b) Show that every element of C_n has order dividing n.

2.) Let $\mathbf{Z}$ denote the integers, let $R = \mathbf{Z}[x]$, and let $S = \mathbf{Z}[x, y]$.
(a) Show that S is not a principal ideal domain.
(b) Find an ideal of S which is prime but not maximal. Explain your answer.
(c) Find an ideal of R which is prime but not maximal. Explain your answer.
(d) Let $(x^2 - 2)$ be the ideal of R generated by $x^2 - 2$. Show that

$$R/(x^2-2) \cong \mathbf{Z}[\sqrt{2}] \stackrel{\text{def}}{=} \{a+b\sqrt{2} : a,b \in \mathbf{Z}\}$$

by explicitly constructing an isomorphism ϕ between these rings. Prove that the ϕ you've constructed is in fact an isomorphism.

3.) (a) Let R be a commutative ring and let $I(a) = \{r \in R : ra = 0\}$.

(i) Prove $I(a)$ is an ideal in R

(ii) Give an example which shows that if R is not commutative, then $I(a)$ may not be an ideal.

(b) An element $r \in R$ is nilpotent if $r^n = 0$ for some integer n.

(i) If $N = \{r \in R : r \text{ is nilpotent }\}$, show that N is an ideal of R.

(ii) Prove that R/N is a ring with no non-zero nilpotent elements.

(iii) Find all nilpotent elements in the ring $\mathbf{Z}/20\mathbf{Z}$.

(c) Let G be a group and let $S = \{aba^{-1}b^{-1} : a,b \in G\}$. If G' is the smallest subgroup of G which contains S, show that the quotient group G/G' is abelian. (You may assume that G' is a normal subgroup of G.)

4.) (a) Let F be a field and let V be an n-dimensional vector space over F. If $S = \{v_1, v_2, \ldots, v_k\}$ is a subset of vectors in V, compare k with n (that is $<, \leq, >, \geq, =$) under the following conditions. Explain your answers.

(i) S is linearly independent.

(ii) S is dependent and generates V.

(iii) S generates V.

(iv) S is linearly independent and generates V.

(v) S is linearly independent and does not generate V.

(b) Let L be a linear transformation on V. Prove that the set of all linear transformations T on V for which $LT = 0$ is a subspace of the space of all transformations on V.

Part II

1.) (a) Let C be the ternary code (i.e. a code over $GF(3)$) with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

(i) List the codewords of C.

(ii) Find the minimum distance of C.

(iii) Is C a perfect code? Explain your answer.

(b) Is each of the following codes cyclic or equivalent to a cyclic code? Explain your answer.

(i) The binary code {0000, 1100, 0110, 0011, 1001}.

(ii) The binary code {00000, 10110, 01101, 11011}.

(iii) The ternary code {0000, 1122, 2211}.

(iv) The q-ary repetition code of length n.

(c) Write out the multiplication table for

$$R = GF(2)[x]/(x^2 + 1)$$

where

$(x^2 + 1)$ is the ideal generated by $x^2 + 1$. Is R a field? Explain. (d) Factor $x^5 - 1$ into irreducible polynomials over $GF(2)$ and use this to determine all

cyclic binary codes of length 5.

2.) (a) Let C be a binary code with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Decode (as best you can) the following received words. Explain your answers.

(i) (1 1 0 1 0 1 1)

(ii) (0 1 1 0 1 1 1)

(iii) (0 1 1 1 0 0 0)

(b) Let $C = (1 + x)$ be the cyclic code in

$$GF(2)[x]/(x^3 - 1).$$

(i) Find the dimension of C.

(ii) Express the codewords of C as a set polynomials and in binary form.

(iii) Find another polynomial which generates C.

(c) Give a simple scheme for error detection with a linear code, making use of the syndrome.