SWARTHMORE COLLEGE
Department of Mathematics and Statistics
Honors Examination

Honors Exam
May, 1997

Modern Algebra I and Coding Theory

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

Part I

1.) 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,

a) show that G' is a normal subgroup of G.

b) show that G/G' is abelian.

c) show that if H is a normal subgroup of G and G/H is abelian, then H contains G'.

2.) Let $\mathbf{Z}$ denote the integers, and let $R = \mathbf{Z}[x]$.

(a) Find a prime ideal of R which is not maximal. Explain your answer.

(b) Give an example of an ideal of R which is not principal. Prove that your example is in fact non-principal.

(c) Let (x^2+1) be the ideal in R generated by x^2+1 and let $i = \sqrt{-1}$. Show that

$$R/(x^2+1) \simeq \mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$$

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

3.) (a) Let $\mathbf{C}$ denote the complex numbers, and let $V = \mathbf{C}^3$. Determine if the following two statements are true or false. Justify your answer - a true statement requires a proof and a false statement requires a counterexample.

(i) $\{(\alpha, \beta, \gamma) \in V : \alpha \text{ is real }\}$ is a vector subspace of V.

(ii) $\{(\alpha, \beta, \gamma) \in V : \alpha + \beta = 0\}$ is a vector subspace of V.

(b) Prove that the vectors $(\alpha_1, \alpha_2), (\beta_1, \beta_2)$ in $\mathbf{C}^2$ are linearly dependent iff $\alpha_1\beta_2 = \alpha_2\beta_1$.

(c) Let T be a linear transformation on an n dimensional vector space V.

(i) Prove that the set of all linear transformations S on V for which $TS = 0$ is a subspace of the space of all linear transformations on V.

(ii) Show that for a suitable choice for T, the dimension of the subspace described in (i) can be equal to 0, n, or n^2.

4.) (a) Let G be a group and let $Aut(G)$ be the set of all automorphisms of G. (Recall that an automorphism of G is a homomorphism from G to G that is one-to-one and onto.)

(i) Show that under the binary operation of composition of functions, $Aut(G)$ is a group.

(ii) Let $\mathbf{Z}_2$ be the finite group of order 2. If $G = \mathbf{Z}_2 \oplus \mathbf{Z}_2$, compute $Aut(G)$.

(b) Give an example of

(i) a non-abelian group G which has an abelian normal subgroup N for which G/N is abelian.

(ii) a non-abelian group G with normal subgroup N such that G/N is *not* isomorphic to a proper subgroup of G. (You may not choose N to be either the identity or G.)

Part II

1.) (a) List the irreducible polynomials over $GF(2)$ of degree 3 and of degree 4. Then, explain how to construct a field of order 8.

(b) Given that the factorization of $x^7 - 1$ into irreducible polynomials over $GF(2)$ is $(x-1)(x^3+x^2+1)(x^3+x+1)$, determine all the cyclic binary codes of length 7. Give a name or a description of each of these codes.

(c) Let $g(x)$ be the generator polynomial of a binary cyclic code which contains some codewords of odd weight, and let $< g(x) >$ be the code generated by $g(x)$. Is the set of codewords in $< g(x) >$ of even weight a cyclic code? If so, what is the generator polynomial of this subcode?

2.) (a) For a binary linear code with parity-check matrix H, show that the transpose of the syndrome of a received vector is equal to the sum of those columns of H corresponding to where the errors occured.

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

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

(i) Find a generator matrix for C in standard form.

(ii) Find a parity check matrix for C in standard form.

(iii) Use syndrome decoding to decode the received vectors 2121, 1201, and 2222.

(c) Write down a parity check matrix for the Hamming [15, 11, 3] code $\mathcal{H}_4$. Explain how the code can can be used to correct any single error in a codeword. What happens if two or more errors occur in any codeword?

(d) Suppose a certain binary channel accepts words of length 7 and that the only kind of error vector ever observed is one of the eight vectors 0000000, 0000001, 0000011, 0000111, 0001111, 0011111, 0111111, 1111111. Design a binary linear [7, k]-code which will correct all such errors with as large a rate as possible. Can you design a similar code of maximum possible rate for *any* given length?