1) Show that if N is a normal subgroup of A_n containing an element x which is a product of disjoint 3-cycles, then N contains a 3-cycle. [You are not allowed to assume the theorem that A_n is simple for n != 5.]

2) Show that there are five ways to inscribe a cube in a regular dodecahedron. Using this, construction a homomorphism from the rotation group of the dodecahedron to S_5. What is the image? What is the kernel? [The first sentence is really a hint for the second one.]

3) Using the generalized Gram-Schmidt algorithm, find a canonical basis for the symmetric bilinear form on \R4 with matrix [[0,1,1,1], [1,0,1,1], [1,1,0,1], [1,1,1,0]], and for the antisymmetric bilinear form with matrix [[0,1,1,1], [-1,0,1,1], [-1,-1,0,1], [-1,-1,-1,0]]. What is the signature of the first form?

4) If A and B are in End(V) for some vector space V over some field F, let kappa(A,B) = Tr(AB) be the trace of the product. (The trace of a linear endomorphism is a basis-independent quantity.) kappa is called the Killing form on End(V).

a) Show that kappa is a symmetric, bilinear form.
b) Is the Killing form on M_2(\R) = End(\R2), the space of two by two real matrices, positive definite? If not, find its signature.
c) Do part (b) for M_n(\R).

5) The purpose of this problem is to exercise the ideas in the classification of Gaussian primes.

a) Recall that the elements of the ring \Z[\omega], where \omega2 + \omega + 1 = 0, are called Eisenstein integers. Show that the Eisenstein integers are a Euclidean domain, and consequently a unique factorization domain.

b) Show that a rational prime p is an Eisenstein prime if and only if it cannot be expressed in the form a2+a b+b2 for rational integers a and b. Here rational means ‘‘pertaining to \Z and \Q’’; a rational integer is an ordinary integer. (For the ‘‘if’’ part, if p had a factor -a+\omega b, what would its norm be?)

c) Show that if a rational prime p = 2 mod 3, then p is also an Eisenstein prime. Is 3 an Eisenstein prime?

d) Show that if a rational prime p = 1 mod 3, then the equation a2 + a + 1 = 0 has a solution in \Z/p. (Hint: First consider the equation a3 - 1 = 0 in \Z/p.)

e) As it happens, a2 + a + 1 = (\omega-a)(\omega2-a). Show that if a rational prime p = 1 mod 3, then it is not an Eisenstein prime.

f) Draw a picture of the Eisenstein integers out to a radius of 4 or 5, and circle the Eisenstein primes.

6) Let phi be a \C-linear endomorphism of a complex vector space V. Show that det_\R phi equals det_\C phi times its complex conjugate.

7) Consider n2 bits arranged in a square grid, and consider the \Z/2-linear code given by the restriction that the sum of each row and column is 0.

a) Find the dimension and distance of this error-correcting code.
b) Give an explicit method to correct one error.
c) Show that the code, considered as a vector space, is equal to P tensor P, where P is the parity code on n bits. (Recall that the parity is code is defined as the subspace where the sum of all bits is 0. Since P is a subspace of X = (\Z/2)^n, P tensor P can be viewed as a subspace of X tensor X.)

8) Find the Smith normal form of the integer matrix [[1,2,3],[1,4,9],[1,8,27]], and the \Q[x] matrix [[x+3,2,1],[-1,x,1],[1,2,x+3]].

9) Show that changing scalars by tensoring does not change the determinant. More precisely, show that if F is a subfield of K and phi_F is an endomorphism of a finite-dimensional F-vector space V, then the induced endormorphism phi_K of K tensor V has the same determinant as phi_F.

10) Let V and W be two complex vector spaces. Show that every \R-linear transformation from V to W is uniquely the sum of a \C-linear transformation and a \C-antilinear transformation. (\C-antilinear means that L(alpha v) = \bar{alpha} L(v).)

11) Let M be the endomorphism of \R4 with matrix [[1,1,0,0],[0,1,0,0],[0,0,1,0],[0,0,1,1]]. Pick a basis for the space V of alternating (scalar-valued) bilinear functions on \R4 and write down a matrix for the induced action of M on V.

12) I said in class that if V and W are infinite-dimensional, then Hom(V,W) is strictly bigger than the tensor product of the duals.

13). Prove that \R (the real numbers) is an infinite-dimensional rational vector space.

14) Let V be the vector subspace of (\Z/2)7 spanned by the seven cyclic permutations of the vector (0,0,1,0,1,1,1). Find a basis for V. Let P be the cyclic permutation endomorphism given by P(a,b,c,d,e,f,g) = (b,c,d,e,f,g,a). Find the matrix for P acting on V in the basis that you chose. (Please try to use forethought to avoid lengthy computations for this problem.)

15) Show that the module \R[x]/(x2+1) + \R[x]/(x2-1) is cyclic and find a generator. (Here the middle ‘‘+’’ means direct sum, and \R is the set of real numbers.)

16) Find all \Z/4-submodules of M = \Z/4 + \Z/4 such

that the quotient module is isomorphic \Z/2. For each submodule, draw a picture of M with the submodule identified.

17) Let A, B, and M be sets, and let Hom(A,B) mean the set of all functions from A to B. Show that the disjoint union of A and B satisfies the universal property of direct sums, while the Cartesian product A x B satisfies the universal property of direct products.

18) The tensor product L = \C tensor_\R \C is a \C-module using the left factor of \C for scalar multiplication. This is in keeping with the S-module structure of S tensor_R M in general. Show that if you instead use the right factor of \C for scalar multiplication, the result is a different (albeit isomorphic) \C-module structure on L.

19) The ring of Eisenstein integers E = \Z[\omega] is a free \Z-module with basis A = {1,\omega}. Another basis is B = {1,\omega2}. Following corollary 10.4.19, A x A and B x B are both bases of E tensor_\Z E. Find a change-of-basis matrix from one to the other. (‘‘Change-of-basis matrix’’ means the same thing here as in linear algebra.)

20) Let I be the set of Hurwitz integers, which are quaternions a+bi+cj+dk, where a,b,c, and d are either all integers or all half integers. (A half-integer here is a number of the form n + 1/2.) Show that I is a ring with 24 units and no zero divisors. Find a subring of I isomorphic to the Gaussian integers \Z[i], and find another subring of I isomorphic to the Eisenstein integers \Z[\omega], where \omega2 + \omega + 1 = 0.

21). Show that if p = 4k+1 is prime, then the abelian group \Z/p has precisely two \Z[i]-module structures. Find the set of module endomorphisms End(\Z/p), interpreting \Z/p as an abelian group, and separately interpreting it as a \Z[i]-module.