

Some Selected Problems

- 1) Show that if N is a normal subgroup of A_n containing an element x that is a product of disjoint 3-cycles, then N contains a 3-cycle. [You are not allowed to assume the theorem that the group A_n is simple for $n \geq 5$.]
- 2) Show that there are five ways to inscribe a cube in a regular dodecahedron. Using this, construct 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 \mathbb{R}^4 with matrix

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

and for the antisymmetric bilinear form with matrix

$$\begin{bmatrix} 0 & -1 & -1 & -1 \\ 1 & 0 & -1 & -1 \\ 1 & 1 & 0 & -1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

What is the signature of the first form?

- 4) Let A and B be in $\text{End}(V)$ for some vector space V over some field F , and let $\kappa(A, B) = \text{tr}(AB)$ be the trace of the product of A and B . (The trace of a linear endomorphism is a basis-independent quantity.) Note that κ is called the Killing form on $\text{End}(V)$.
 - a) Show that κ is a symmetric bilinear form.
 - b) Is the Killing form on $M_2(\mathbb{R}) = \text{End}(\mathbb{R}^2)$, the space of two by two real matrices, positive definite? If not, find its signature.
 - c) Do part b) for $M_n(\mathbb{R})$.
- 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 $\mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$, 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 $a^2 + ab + b^2$ for rational integers a and b . Here rational means “pertaining to \mathbb{Z} and \mathbb{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 $p = 2 \pmod{3}$, then p is also an Eisenstein prime. Is 3 an Eisenstein prime?
- d) Show that if a rational prime $p = 1 \pmod{3}$, then the equation $a^2 + a + 1 = 0$ has a solution in \mathbb{Z}/p . (Hint: First consider the equation $a^3 - 1 = 0$ in \mathbb{Z}/p .)
- e) As it happens, $a^2 + a + 1 = (\omega - a)(\omega^2 - a)$. Show that if a rational prime $p = 1 \pmod{3}$, 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 ϕ be a \mathbb{C} -linear endomorphism of a complex vector space V . Show that $\det_{\mathbb{R}} \phi$ equals $\det_{\mathbb{C}} \phi$ times its complex conjugate.
- 7) Consider n^2 bits arranged in a square grid, and consider the $\mathbb{Z}/2$ -linear code given by the restriction that the sum of each row and column is 0.
- Find the dimension and distance of this error-correcting code.
 - Give an explicit method to correct one error.
 - Show that the code, considered as a vector space, is equal to $P \otimes P$, where P is the parity code on n bits. (Recall that the parity code is defined as the subspace where the sum of all bits is 0. Since P is a subspace of $X = (\mathbb{Z}/2)^n$, $P \otimes P$ can be viewed as a subspace of $X \otimes X$.)

- 8) Find the Smith normal form of the integer matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \end{bmatrix},$$

and the $\mathbb{Q}[x]$ matrix

$$\begin{bmatrix} x+3 & -1 & 1 \\ 2 & x & 2 \\ 1 & 1 & x+3 \end{bmatrix}.$$

- 9) Show that changing scalars by tensoring does not change the determinant. More precisely, show that if F is a subfield of K and ϕ_F is an endomorphism of a finite-dimensional F -vector space V , then the induced endomorphism ϕ_K of $K \otimes V$ has the same determinant as ϕ_F .
- 10) Let V and W be two complex vector spaces. Show that every \mathbb{R} -linear transformation from V to W is uniquely the sum of a \mathbb{C} -linear transformation and a \mathbb{C} -antilinear transformation. (Note that \mathbb{C} -antilinear means that $L(\alpha v) = \bar{\alpha}L(v)$.)

- 11) Let M be the endomorphism of \mathbb{R}^4 with matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Pick a basis for the space V of alternating (scalar-valued) bilinear functions on \mathbb{R}^4 and write down a matrix for the induced action of M on V .

- 12) Show that if V and W are infinite-dimensional, then $\text{Hom}(V, W)$ is strictly bigger than the tensor product of the duals.
- 13) Prove that \mathbb{R} (the real numbers) is an infinite-dimensional rational vector space.
- 14) Let V be the vector subspace of $(\mathbb{Z}/2)^7$ 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 $\mathbb{R}[x]/(x^2 + 1) + \mathbb{R}[x]/(x^2 - 1)$ is cyclic and find a generator. (Here the middle “+” means direct sum, and \mathbb{R} is the set of real numbers.)
- 16) Find all $\mathbb{Z}/4$ -submodules of $M = \mathbb{Z}/4 + \mathbb{Z}/4$ such that the quotient module is isomorphic to $\mathbb{Z}/2$. For each submodule, draw a picture of M with the submodule identified.
- 17) Let A , B , and M be sets, and let $\text{Hom}(A, B)$ 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 $A \times B$ satisfies the universal property of direct products.
- 18) The tensor product $L = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is a \mathbb{C} -module using the left factor of \mathbb{C} for scalar multiplication. This is in keeping with the S -module structure of $S \otimes_{\mathbb{R}} M$ in general. Show that if you instead use the right factor of \mathbb{C} for scalar multiplication, the result is a different (albeit isomorphic) \mathbb{C} -module structure on L .
- 19) The ring of Eisenstein integers $E = \mathbb{Z}[\omega]$ is a free \mathbb{Z} -module with basis $A = \{1, \omega\}$. Another basis is $B = \{1, \omega^2\}$. Following corollary 10.4.19, $A \times A$ and $B \times B$ are both bases of $E \otimes_{\mathbb{Z}} E$. 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 $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, 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 $\mathbb{Z}[\mathbf{i}]$, and find another subring of I isomorphic to the Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$.

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