Math 122 Fall 2014 Practice Problems for Final

Practice Problems for matrices and Cayley-Hamilton

1. Basics in characteristic polynomials

(a) Let F be a field, and A a $k \times k$ matrix with entries in F. Show that A is not conjugate to an upper-triangular matrix unless its characteristic polynomial can be factored into (possibly non-distinct) linear polynomials in $F[t]$.
(b) Given an example of a matrix in a field F whose characteristic polynomial cannot be factored into linear polynomials.
(c) Prove that if A is a $k \times k$ matrix with entries in a field F, its characteristic polynomial $\Delta(t)$ is a degree k polynomial in $F[t]$, and that the degree $k-1$ coefficient of $\Delta(t)$ is $-\mathrm{tr}(A)$. (Here, $\mathrm{tr}(A)$ is the trace of A—the sum of its diagonal entries.)
(d) Prove that the constant term of $\Delta(t)$ is $(-1)^k \det A$.

2. Matrices are linear transformations

Let R be a commutative ring and $R^{\oplus k}$ the free module on k generators. Show there is a ring isomorphism

$$T : M_{k\times k}(R) \to \hom_R(R^{\oplus k}, R^{\oplus k})$$

given by sending a matrix A to the homomorphism T_A sending the ith standard basis element of $R^{\oplus k}$ to the element

$$\sum_{j=1}^{k} A_{ji} e_j .$$

If you are lazy and don't want to do every part of the proof, here is the most important part: prove that $T_{AB} = T_A \circ T_B$, so that matrix multiplication is sent to composition of functions.

Remark 2.1. (Recall that a homomorphism from $R^{\oplus k}$ to any module M is determined by the choice of k elements $x_1, \ldots, x_k$ in M, simply be declaring that $e_i \in R^{\oplus k}$ get sent to x_i.)

Remark 2.2. To be clear, the target of T is the set of all left R-module homomorphisms from $R^{\oplus k}$ to itself.

Remark 2.3. By the way, this ring isomorphism is the justification for saying that a linear map from a finite-dimensional vector space over F to itself is the same thing as a matrix—in this case, $R = F$, and every finite-dimensional vector space over F is isomorphic to $F^{\oplus k}$ for some k.

3. Some Cayley-Hamilton applications

Let $\mathbb{F}$ be a field of characteristic p. Let A be an upper-triangular $k \times k$ matrix with entries in $\mathbb{F}$.

(a) Assume A's diagonal entries are equal to 1. Show that for the values $(3,3)$, $(5,5)$, and $(4,2)$ of (k,p), A^k is equal to $(-1)^{k-1}I$.

(b) With the hypothesis as in part (a), prove that A is an element whose order must divide k or $2k$.

4. More Cayley-Hamilton

Let F be a field and A an $k \times k$ matrix with entries in F. When you want to compute $f(A)$ where $f(t)$ is some high-degree polynomial in t, note that by the division algorithm for polynomials, we can write

$$f(t) = q(t)\Delta(t) + r(t)$$

where $\Delta(t)$ is the characteristic polynomial of A. Then we have

$$f(A) = q(A)\Delta(A) + r(A) = r(A)$$

since $\Delta(A) = 0$ by the Cayley-Hamilton theorem. This reduces a potential costly calculation into two steps: A division of polynomials (to find r) and then a degree $k-1$ computation given by evaluating $r(A)$.

(a) If A is a 2×2 matrix which is not invertible in F, prove that A^2 is always a scalar multiple of A. Moreover, prove that A^2 is obtained from A by scaling via the trace of A.

(b) Let A be a 3×3 matrix which is not invertible, and which has trace zero. Compute A^{1000} in terms of A^2 and the degree 1 coefficient of $\Delta(t)$. Derive a general formula for A^N in terms of A^2 and the degree 2 coefficient of $\Delta(t)$.

(c) Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ 5 & 2 & -1 \end{bmatrix}.$$

Compute A^{2014} using the methods above.

(d) What is A^{2014} if you consider A as a matrix with entries in $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$?

Rings and ideals

5. Basics of rings

(a) Give an example of a non-commutative ring with a zero divisor. (Make sure to identify the zero divisor.)

(b) Given an example of a commutative ring with a zero divisor.

6. Prime ideals

Let R be a commutative ring. An ideal I is called *prime* if whenever $xy \in I$, we have that either $x \in I$ or $y \in I$.

(a) Let $f \in R$ be an irreducible element and R a PID. Show that the ideal generated by f is prime.

(b) Recall that a commutative ring is called a *domain* if it has no zero divisors. Show that if I is a prime ideal of R, then R/I is a domain.

7. Prime ideals and maximal ideals

Let R be a commutative ring.

(a) Show that every maximal ideal in R is a prime ideal.

(b) Show that if R is a PID, then every non-zero prime ideal is maximal.

8. A ring that is not a PID

(a) Let F be a field, and let $R = F[x_1, x_2]$ be the ring of polynomials with two variables. Exhibit an ideal in R that is not principal.

(b) Show that $\mathbb{Z}[x]$—the ring of polynomials with $\mathbb{Z}$ coefficients—is not a principal ideal domain.

Modules

9. $\mathbb{Z}$-modules

(a) Show that a $\mathbb{Z}$-module is the same thing as an abelian group.

(b) Show that a map of $\mathbb{Z}$-modules (i.e., a $\mathbb{Z}$-linear homomorphism between $\mathbb{Z}$-modules) is the same thing as a homomorphism of abelian groups.

10. $\mathbb{Z}[t]$-modules

Show that a $\mathbb{Z}[t]$-module structure on an abelian group M is the same thing as giving an abelian group homomorphism from M to itself.

11. Submodules

Let M be a left R-module. Recall that an R-*submodule* of M is a subgroup $N \subset M$ such that $rx \in N$ for all $r \in R, x \in N$.

(a) Show that the intersection of two submodules is a submodule.

(b) If R is a commutative ring and $R = M$, show that a submodule of M is the same thing as an ideal of R.

12. Not all modules are free

Give an example of a ring R and a left module M such that M is not isomorphic to a free R-module.

Computations

13. Computations with matrices

Consider the matrices

$$\begin{bmatrix} 1 & 4 \\ 5 & 7 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}.$$

(a) Which of them are invertible as elements of $M_{2\times 2}(\mathbb{Z})$?
(b) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$?
(c) Which are invertible as elements of $M_{2\times 2}(\mathbb{Z}/7\mathbb{Z})$?

14. Polynomial roots

Consider the polynomials

$$t^3 + 2t + 1, \qquad t^4 + 1, \qquad t^2 + 3.$$

(a) Which of these are irreducible elements of $\mathbb{Z}/2\mathbb{Z}[t]$?
(b) Which of these are irreducible elements of $\mathbb{Z}/3\mathbb{Z}[t]$?
(c) Which of these are irreducible elements of $\mathbb{Z}/5\mathbb{Z}[t]$?

Classification of finitely generated PIDs

15. Statement

State the classification of finitely generated modules over a PID.

16. Classifying abelian groups

(a) How does the theorem let us classify finitely generated abelian groups?
(b) Classify all abelian groups of order 12.
(c) Classify all abelian groups of order 16.

17. Another way to phrase classification of abelian groups

(a) Let k, m, n be integers. Prove that $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if and only if $k = mn$ and m, n are relatively prime.
(b) Assume the classification of finitely generated abelian groups stated in class. Prove: If A is a finitely generated abelian group, it is isomorphic to a group of the form

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

where n_i divides n_{i+1} for all $1 \leq i \leq k-1$.

Groups

18. Your common mistakes

(a) Give an example of a group G, and an abelian subgroup $H \subset G$, such that H is not normal in G.

(b) Given an example of a group G, and a sequence of subgroups

$$G_1 \subset G_2 \subset G$$

such that $G_1 \triangleleft G_2$ and $G_2 \triangleleft G$, but G_1 is not normal in G.

19. Sylow's Theorems

Let n_p denote the number of Sylow p-subgroups of G.

(a) * Let $G = S_4$. Compute n_2.

(b) Let $G = S_4$. Compute n_3.

(c) Let $G = D_{2p}$, the dihedral group with $2p$ elements, where $p > 2$ is a prime. Compute n_2 and n_p.

20. Actions and orbit-stabilizer

(a) Show that $H \triangleleft G$ if and only if the normalizer of H is all of G.

(b) Let G be a finite group, and $H \subset G$ a subgroup. Show that the number of subgroups of G conjugate to H is equal to the size of G, divided by the order of the normalizer of H.

(c) Let $x \in G$ be an element, with $|G|$ finite. Show that the number of elements conjugate to x is equal to the size of G, divided by the number of elements that commute with x.

21. Prove Lagrange's Theorem

Prove Lagrange's Theorem.

22. Cayley's Theorem

(a) Show that every group acts on itself.

(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem.

23. Groups of order 8

Recall the quaternion ring, otherwise called the Hamiltonians. Consider the set

$$Q = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{R}^4$$

where

$$1 = (1,0,0,0) \qquad i = (0,1,0,0) \qquad j = (0,0,1,0) \qquad k = (0,0,0,1).$$

(a) Show that Q is a group of order 8.
(b) Show that Q is non-abelian.
(c) Write down all subgroups of Q.
(d) * Show that Q is not isomorphic to $D_{2\cdot 4} = D_8$, the dihedral group with 8 elements.

24. Some big theorems

(a) Let p be a prime number. If $n \in \mathbb{Z}$ is not divisible by p, prove that
$$n^{p-1} - 1$$
is divisible by p. This is called Fermat's Little Theorem. (Hint: If $\mathbb{Z}/p\mathbb{Z}$ is a field, what can you say about $\mathbb{Z}/p\mathbb{Z} - \{0\}$?)
(b) Show that every finite group is isomorphic to a subgroup of S_n for some n. This is called Cayley's Theorem. (Hint: Every group acts on itself by left multiplication.)

Terms you'll need to know

(1) Group
(2) Finite group
(3) Isomorphism
(4) Subgroup
(5) Homomorphism
(6) Trivial homomorphism (i.e., one whose image is $\{1\}$)
(7) Order of an element g (size of $\langle g \rangle$—equivalently, smallest $n \geq 1$ for which $g^n = 1$. Orders can be infinite.)
(8) Order of a group (number of elements in the group—possibly infinite.)
(9) Abelian group
(10) p-Sylow subgroup
(11) Normal subgroup
(12) Quotient group
(13) Simple group
(14) Automorphisms of a set (i.e., a bijection from a set to itself)
(15) Automorphisms of a group (i.e., a group isomorphism from a group to itself)
(16) Group action
(17) Orbits
(18) Disjoint union
(19) Center of a group (the set of all x such that $gx = xg$ for all $g \in G$.)
(20) Direct product of groups
(21) Semidirect product
(22) Characteristic polynomial of a matrix with entries in a field F
(23) Ring
(24) Multiplicative identity of a ring
(25) Additive identity of a ring
(26) Ring homomorphism (remember that 1 must be sent to 1!)
(27) Left R-module (sometimes, simply called an R-module; especially if R is commutative)
(28) A homomorphism of left R-modules (a.k.a. R-linear map)
(29) Direct sum $M \oplus N$ of R-modules
(30) Ideals
(31) Ideal generated by a single element
(32) Quotient rings
(33) Field
(34) Vector space (i.e., a module over a field)
(35) Algebraically closed field
(36) Polynomial ring $F[t]$

(37) Irreducible polynomial
(38) Upper triangular matrix
(39) Cayley-Hamilton Theorem
(40) Relatively prime numbers (i.e., those such that $gcd = 1$.)

Some of the ideas you'll want to know (emphasis on "some")

(1) How to pass from semidirect products to split short exact sequences (Given $L \rtimes_\phi R$, there is the inclusion $L \to L \rtimes_\phi R$ given by $l \mapsto (l, 1_R)$ and $j : R \to L \rtimes_\phi R$ given by $j(r) = (1_L, r)$. Then the short exact sequence $L \to L \rtimes_\phi R \to R$ is split by j.)

(2) How to pass from split short exact sequences to semidirect products ($L \to H \to R, j : R \to H$ means $j(R)$ acts on L by conjugation, meaning one has a homomorphsim $\phi : R \cong j(R) \to \mathrm{Aut}(L)$, so a semidirect product $L \rtimes_\phi R$. You haven't lost information because the map $L \rtimes_\phi R \to H$ given by $(l, r) \mapsto l \cdot j(r)$ is an isomorphism, and $L \rtimes_\phi R$ has the obvious split short exact sequences $L \to L \rtimes_\phi R \to R, R \to L \rtimes_\phi R$. We are identifying L with its image in H.)

(3) Classify all abelian groups of finite order

(4) Classification theorem of finitely generated modules over a PID

(5) Using Sylow's Theorems to count Sylow subgroups

(6) Characteristic polynomials don't change under conjugation—so $\det(tI - A) = \det tI - BAB^{-1})$, regardless of the field in which the A takes entries.