Math 230B: Algebra
Final Exam Solutions
Thursday, March 23, 2023.

Problems

1. Let K be a field and let A be an $n \times n$ matrix with entries in K.
   Suppose that $f \in K[x]$ is an irreducible polynomial such that $f(A) = 0$.
   Prove that $\deg(f) \mid n$.

   Solution: Since $f(A) = 0$ the minimal polynomial of $m_A(x)$ divides $f(x)$. Since $f(x)$ is irreducible, $f(x)$ must be the minimal polynomial of A.

   The minimal polynomial of A is the largest invariant factor of A, that is, every other invariant factor divides $m_A(x)$. Since $m_A(x) = f(x)$ is irreducible and each invariant factor has degree at least 1, every invariant factor of A is equal to $f(x)$.

   The characteristic polynomial of A is the product of all of the invariant factors of A, and its degree is n. Since every invariant factor is equal to $f(x)$, taking degrees with see that n equal the degree of f times the number of invariant factors of A. We conclude that $\deg(f) \mid n$.

2. Let A be a finite abelian group of order n. What is the cardinality of $\mathbb{Q} \otimes_{\mathbb{Z}} A$?
   Prove that your answer is correct.

   Solution: Since elementary tensors generate $\mathbb{Q} \otimes_{\mathbb{Z}} A$, if we show that every elementary tensor in $\mathbb{Q} \otimes_{\mathbb{Z}} A$ is trivial, then we can conclude that $\mathbb{Q} \otimes_{\mathbb{Z}} A$ is trivial. (So it has cardinality one.)

   Let $\frac{a}{b} \in \mathbb{Q}$ and $x \in A$. Since A has order n we have $n \cdot x = 0$. By the elementary properties of tensor products we have

$$\frac{a}{b} \otimes x = n \cdot \left(\frac{a}{bn} \otimes x\right) = \frac{a}{bn} \otimes (n \cdot x) = \frac{a}{bn} \otimes 0 = 0.$$

3. Is $\mathbb{Q}$ is a free $\mathbb{Z}$-module? Prove that your answer is correct.

   Solution: A $\mathbb{Z}$-module is free if it contains a spanning set that is linearly independent. We prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

   In any R-module M since $1 \cdot 0 = 0$, $\{0\}$ is an R-linearly dependent set. Also, if $\{m_1, \ldots, m_n\}$ is an R-linearly dependent set and $A \subset M$ contains $\{m_1, \ldots, m_n\}$, then A is R-linearly dependent as well. This is because, the nonzero R-linear combination $r_1 \cdot m_1 + \cdots + r_n \cdot m_n = 0$ gives a nonzero R-linear combination $r_1 \cdot m_1 + \cdots + r_n \cdot m_n + \sum_{a \in A} 0 \cdot a = 0$.

We now show that any two elements of $\mathbb{Q}$ are $\mathbb{Z}$-linearly dependent. By the previous paragraph, we can assume that both elements are nonzero. Suppose $\frac{a}{b}, \frac{c}{d}$ are two nonzero elements of $\mathbb{Q}$. This means $a, b, c, d \neq 0$. Since

$$(bc) \cdot \frac{a}{b} + (-ad) \cdot \frac{c}{d} = 0,$$

and $bc, -ad \neq 0$, we see that these elements are $\mathbb{Z}$-linearly dependent.

Therefore, $\mathbb{Q}$ does not contain any $\mathbb{Z}$-linearly independent set of size at least 2. We show that $\mathbb{Q}$ does not contain a spanning set of size 1. This will complete the proof.

Suppose $\frac{a}{b} \in \mathbb{Q}$. The $\mathbb{Z}$-module spanned by $\frac{a}{b}$ consists of elements of the form $n \cdot \frac{a}{b}$ where $n \in \mathbb{Z}$. It is clear that none of these elements have a denominator larger than b. Since $\mathbb{Q}$ contains elements with arbitrarily large denominators, we see that $\frac{a}{b}$ does not span $\mathbb{Q}$ as a $\mathbb{Z}$-module.

4. Let R be a UFD and let α be an irreducible element of R. Prove that α is prime.

   Solution: Consider (α). We want to show that this is prime. Suppose $\beta, \gamma \in R$ such that $\beta\gamma \in (\alpha)$. This is equivalent to $\alpha \mid \beta\gamma$. This implies that there exists $\delta \in R$ such that $\alpha\delta = \beta\gamma$.

   Since R is a UFD we can factor β and γ into finite products of irreducible elements $\beta = p_1 \cdots p_r$ and $\gamma = q_1 \cdots q_s$, where each p_i, q_j is irreducible in R. Since R is a UFD, these factorizations are unique up to reordering and associates.

   Since α is irreducible and divides the left-hand side of the equation $\alpha\delta = \beta\gamma$, it must divide the right-hand side as well. Since $\beta\gamma = p_1 \cdots p_r q_1 \cdots q_s$ there either exists some p_i or some q_j that is associate to α. Without loss of generality, suppose there is some p_i associate to α. This means that $\alpha \mid \beta$.

   We conclude that $\beta\gamma \in (\alpha)$ implies $\beta \in (\alpha)$ or $\gamma \in (\alpha)$, so α is a prime element.

5. Is every Euclidean domain a PID? Either prove that the answer is yes or give an example to show that the answer is no (and explain why your example works).

   Solution: Let I be an ideal of R. We claim that I is the principal ideal generated by any nonzero element of R of minimal norm. Suppose $\alpha \in I$ has minimal norm among all nonzero elements of R. Clearly $(\alpha) \subseteq I$. We show that $I \subseteq R$, completing the proof.

   Let $\beta \in I$. Our goal is to show that $\beta \in (\alpha)$. By the division algorithm in R we have $\beta = q\alpha + r$ for some $q, r \in R$ where either $r = 0$ or $N(r) < N(\alpha)$. Since $\alpha \in I$ we have $q\alpha \in I$. Since $\beta, q\alpha \in I$ we have $\beta - q\alpha = r \in I$.

   If $r \neq 0$, then $N(r) < N(\alpha)$. But this contradicts the assumption that α has minimal norm among all nonzero elements of I. Therefore, $r = 0$. This implies $\beta = q\alpha$, so $\beta \in (\alpha)$.

6. Let V be a vector space of dimension n over a field F. Let W be a subspace of V of dimension m. Let s be the dimension of the vector space V/W. Prove that $m+s=n$.

   Note: Do not use the Rank-Nullity theorem for linear transformations to prove this statement. (We used this statement to prove the Rank-Nullity theorem.)

   Solution: Let $w_1, \ldots, w_m$ be a basis for W. There exists a basis of V of the form $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$.

   Let $\pi \colon V \to V/W$. Since $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$ generate V, we see that the vectors $\pi(w_1), \ldots, \pi(w_m), \pi(v_{m+1}), \ldots, \pi(v_n)$ generate V/W. Since $\pi(w_1), \ldots, \pi(w_m) = 0$ we see that $\pi(v_{m+1}), \ldots, \pi(v_n)$ are a spanning set of V/W of size $n-m$. We need only show that they are linearly independent.

   Suppose that $\alpha_{m+1}, \ldots, \alpha_n \in F$ are such that

$$\alpha_{m+1} \cdot \pi(v_{m+1}) + \cdots + \alpha_n \cdot \pi(v_n) = 0.$$

   This is equivalent to saying that

$$\alpha_{m+1} \cdot v_{m+1} + \cdots + \alpha_n \cdot v_n = w$$

   for some vector $w \in W$. Since $w \in W$, there exist $\alpha_1, \ldots, \alpha_m \in F$ such that

$$w = \alpha_1 \cdot w_1 + \cdots + \alpha_m \cdot w_m.$$

   This implies

$$\alpha_1 \cdot w_1 + \cdots + \alpha_m \cdot w_m - (\alpha_{m+1} \cdot v_{m+1} + \cdots + \alpha_n \cdot v_n) = 0.$$

   Since $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$ are linearly independent, this implies $\alpha_{m+1} = \cdots = \alpha_n = 0$. We conclude that $\pi(v_{m+1}), \ldots, \pi(v_n)$ are linearly independent, completing the proof.

7. (a) Let R be a commutative ring with $1 \neq 0$ and let M be an R-module. Define $\mathrm{Ann}(M)$, the annihilator of M.

   (b) Prove that $\mathrm{Ann}(M)$ is an ideal of R.

   (c) Let R be a PID, let B be a torsion R-module and let p be a prime in R. Prove that if $pb = 0$ for some nonzero $b \in B$, then $\mathrm{Ann}(B) \subseteq (p)$.

   Solution: $\mathrm{Ann}(M)$ is the set of all $r \in R$ such that $r \cdot m = 0$ for all $m \in M$.

   It is clear that $0 \in \mathrm{Ann}(M)$. Suppose $x, y \in \mathrm{Ann}(M)$. Since $(x-y) \cdot m = x \cdot m - y \cdot m = 0$, we see that $x - y \in \mathrm{Ann}(M)$. Therefore, $\mathrm{Ann}(M)$ is an additive subgroup of R.

   Since $(rx) \cdot m = r \cdot (x \cdot m) = r \cdot 0 = 0$, we see that $rx \in \mathrm{Ann}(M)$ for any $r \in R$. Therefore, $\mathrm{Ann}(M)$ is an ideal of R.

Since R is a PID and $\mathrm{Ann}(B)$ is an ideal of R, we have $\mathrm{Ann}(B) = (\alpha)$ for some $\alpha \in R$. So $\mathrm{Ann}(B) \subseteq (p)$ is equivalent to $(\alpha) \subseteq (p)$, which is equivalent to $p \mid \alpha$.

We have $\alpha \cdot b = 0$ and so $(r\alpha) \cdot b = r \cdot (\alpha \cdot b) = 0$ for all $r \in R$. Similarly, $(sp) \cdot b = s \cdot (p \cdot b) = 0$ for all $s \in R$. We see that $(r\alpha + sp) \cdot b = (r\alpha) \cdot b + sp \cdot b = 0 + 0 = 0$ for all $r, s \in R$. This means that $x \cdot b = 0$ for all elements in the ideal of R generated by α and p. This is the ideal generated by the greatest common divisor of α and p. Either, this is (p), in which case $p \mid \alpha$ and we are done, or this is $(1) = R$. But since $1 \cdot b \neq 0$, this is not possible.

8. (a) How many similarity classes of 4×4 matrices A with entries in $\mathbb{R}$ satisfy $A^3 = I$? Explain how you know this number is correct.

   (b) Give an example of one matrix in each of these similarity classes.

Solution: Two 4×4 matrices with entries in $\mathbb{R}$ are similar if and only if they have the same set of invariant factors.

If $A^3 = I$ then the minimal polynomial of A divides $x^3 - 1 = (x-1)(x^2+x+1)$. Since $x^2 + x + 1$ has no roots in $\mathbb{R}$ it is irreducible in $\mathbb{R}[x]$. The minimal polynomial of A is its largest invariant factor and the characteristic polynomial of A is the product of all of the invariant factors. The degree of the characteristic polynomial is 4, the size of the matrix.

We divide up the possible sets of invariant factors based on the minimal polynomial.

(a) Suppose that $m_A(x) = x - 1$. Then every invariant factor is $x - 1$, so there must be 4 of them: $(x-1, x-1, x-1, x-1)$.

(b) Suppose that $m_A(x) = x^2 + x + 1$. Since this polynomial is irreducible in $\mathbb{R}[x]$, every other invariant factor must be equal to $m_A(x)$. Therefore, there are two of them: $(x^2 + x + 1, x^2 + x + 1)$

(c) Suppose that $m_A(x) = (x-1)(x^2+x+1)$. The product of the other invariant factors must have degree 1, so there is exactly one more and it must be linear. Since every invariant factor divides $m_A(x)$, it must be $x - 1$. Therefore, the invariant factors are: $(x-1, (x-1)(x^2+x+1))$.

These are the only possible sets of invariant factors of A, so these are all the similarity classes.

The companion matrix of $x - 1$ is (1).

The companion matrix of $x^2 + x + 1$ is $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

The companion matrix of $(x-1)(x^2+x+1) = x^3 - 1$ is $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

We write down a matrix having each of the sets of invariant factors given above that is in rational canonical form. These are

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

9. For each of the following rings, list all of its maximal ideals.
Prove that your list is complete.

   (a) $\mathbb{Q}[x]/(x^2+1)$

   (b) $\mathbb{C}[x]/(x^2+1)$

   (c) $\mathbb{Q}[x]/(x^3+x^2)$.

   Solution: We recall that if F is a field, $F[x]$ is a PID. So every ideal is of the form $(f(x))$, and scaling by a unit if necessary, we see that we can assume that $f(x)$ is monic. Moreover, since we are in a PID, $f(x)$ is irreducible if and only if it is prime, and prime ideas are maximal. Therefore, a major step in this problem is to factor each polynomial into a product of monic irreducible polynomials.

   In $\mathbb{Q}[x]$ we see that x^2+1 is irreducible since it is a quadratic polynomial with no roots in $\mathbb{Q}$. Therefore, $\mathbb{Q}[x]/(x^2+1)$ is a field. The only ideals of a field are the trivial ideal (which is maximal), and the field itself. Therefore, the only maximal ideal is $\{0\}$.

   In $\mathbb{C}[x]$ we see that $x^2+1 = (x-i)(x+i)$. Each of these monic polynomials is irreducible. By the lattice isomorphism theorem for rings, ideals of $\mathbb{C}[x]/((x-i)(x+i))$ correspond to ideals of $\mathbb{C}[x]$ that contain $(x-i)(x+i)$. In $F[x]$ we have $(g(x))$ contains $(f(x))$ if and only if $g(x) \mid f(x)$. Therefore, the only ideals of $\mathbb{C}[x]/((x-i)(x+i))$ are the trivial one, the whole ring, and the two ideals $(x-i)$ and $(x+i)$. We see that these last two ideals are the only maximal ones.

   In $\mathbb{Q}[x]$ we have $x^3+x^2 = x^2(x+1)$. By the same argument as in the previous paragraph, ideals in $\mathbb{Q}[x]/(x^3+x^2)$ correspond to monic factors of $x^2(x+1)$, and the maximal ideals correspond to irreducible monic factors of $x^2(x+1)$. Therefore, the only maximal ideals of $\mathbb{Q}[x]/(x^3+x^2)$ are (x) and $(x+1)$.

10. Let F be a field and let G be a finite subgroup of F^*. Prove that G is cyclic.

    Solution: G is a finite abelian group, so by the classification theorem for finitely generated abelian groups, there exist integers $n_1, \ldots, n_r$ such that

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

where each n_j is at least 2 and that satisfy $n_{i+1} \mid n_i$ for each $i \in 1, \ldots, r-1$. Our goal is to show that $r = 1$, which is equivalent to saying that G is cyclic.

The elements of G of order dividing n_r are all roots of the polynomial $x^{n_r} - 1$ in F. Since this is a polynomial of degree n_r in $F[x]$, it has at most n_r distinct roots in F.

Consider the group $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$. A cyclic group $\mathbb{Z}/m\mathbb{Z}$ where $n_r \mid m$ contains a unique subgroup isomorphic to $\mathbb{Z}/n_r\mathbb{Z}$. This subgroup consists of the n_r elements of $\mathbb{Z}/m\mathbb{Z}$ of order dividing n_r. In this way, we see that $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ contains at least rn_r elements of order dividing n_r. This contradicts the previous paragraph unless $r = 1$.