Clemson Algebra Prelim Solutions

The Monster Group

May 26, 2023

Contents

Winter 2019

1. Let V be a finite-dimensional complex inner product space. A set of vectors $\{f_1, ..., f_m\}$ is called a *Parseval frame* for V if for every $v \in V$, $v = \sum_{i=1}^{m} \langle v, f_i \rangle f_i$.

   (a) Prove that every orthonormal basis of V is a Parseval frame.

   Proof. Let $\{e_1, ..., e_n\}$ be an ONB of V. Write v as $\alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_n e_n$ then plug it into the sum. □

   (b) Prove that there exists a Parseval frame which is not an orthonormal basis.

   Proof. Consider the Mercedes–Benz frame:

   $$f_1 = \left(0, \frac{\sqrt{2}}{\sqrt{3}}\right), \quad f_2 = \left(\frac{-\sqrt{2}}{\sqrt{2}}, \frac{-\sqrt{6}}{\sqrt{6}}\right), \quad f_3 = \left(\frac{\sqrt{2}}{\sqrt{2}}, \frac{-\sqrt{6}}{\sqrt{6}}\right).$$

   This is not an ONB, as $f_1 \cdot f_2$ is not $(0, 0)$. I invite you to perform the calculation yourself and verify that $\sum_{i=1}^{3} \langle v, f_i \rangle f_i$ is, in fact, v. □

   (c) Prove that every linearly independent Parseval frame is an orthonormal basis.

   Proof. Basis follows for free. Let $v = f_j$ in the sum to see it must be that $\langle f_j, f_i \rangle = 0$ for all $i \neq j$. □

   (d) Prove that $\{f_1, ..., f_m\}$ is a Parseval frame for V if and only if there is a complex inner product space W such that the following is true:

   (a) V is isometrically embedded in W , i.e., there is a an injective linear map $\phi : V \to W$ such that $\langle v_1, v_1 \rangle_V = \langle \phi(v_1), \phi(v_2) \rangle_W$ for every $v_1, v_2 \in V$.

   (b) $\phi(f_i) = P_{\phi(V)} e_i$ for some orthonormal basis $\{e_1, ..., e_m\}$ of W, where $P_{\phi(V)}$ is the orthogonal projection onto the subspace $\phi(V)$.

   Proof. ($\Leftarrow$)

   ($\Rightarrow$) □

2. Let V be a finite-dimensional vector space over $\mathbb{Q}$. Suppose that $A : V \to V$ is an invertible linear map such that $A^{-1} = \frac{1}{2}A^2 + A$.

   (a) Give all possibilities for the minimal and characteristic polynomials of A.

   Proof. The condition $A^{-1} = \frac{1}{2}A^2 + A$ implies that $A^3 + 2A^2 - 2I = 0$, which by Eisenstein's criterion is irreducible over $\mathbb{Q}$. Thus $\mu_A(x) = x^3 + 2x^2 - 2$ and $\rho_A(x) = (x^3 + 2x^2 - 2)^n$ for $n \in \mathbb{N}$. □

   (b) Prove that dim V is a multiple of 3

   Proof. By part (a) above, since $\dim(V) = \deg(\rho_A)$, we get that $\deg(\rho_A) = 3n$. □

(c) Give an explicit example of how Part (b) can fail if $\mathbb{Q}$ is replaced by $\mathbb{C}$.

Proof. Over $\mathbb{C}$, every polynomial is reducible. If r_1 is a root of $\mu_A(x)$, then the 1×1 matrix $[r_1]$ satisfies $x^3 + 2x^2 - 2 = 0$ yet does not have dimension a multiple of 3. □

(d) Still assuming that V is a $\mathbb{C}$-vector space, prove that if $\dim V = 3$, then all such linear maps are similar.

Proof. Notice that $\rho'_A(x) = x(x + 4/3)$, with roots 0 and $-4/3$. Since neither is a root of $\rho_A(x)$, it has no repeated roots. Thus $\rho_A(x) = \mu_A(x)$, thus all maps are similar. □

(e) Does Part (d) still hold over $\mathbb{Q}$? Fully justify your answer

Proof. It does. Since $\dim V = 3$, $\rho_A(x) = \mu_A(x)$. □

3. A square matrix N is said to be *nilpotent* if there is a positive integer m such that $N^m = 0$. Let A and B be $n \times n$ real matrices.

(a) Prove that the following conditions are equivalent: (i) A is nilpotent, (ii) $A^n = 0$, (iii) the only eigenvalue of A is 0.

Proof. (i) $\Rightarrow$ (ii) Straightforward.

(ii) $\Rightarrow$ (iii) Cayley-Hamilton gives us that $A^n = 0 \;\Rightarrow\; \lambda^n \in \mathrm{Spec}(A)$. So $\lambda = 0$ is the only eigenvalue, with multiplicity n.

(iii) $\Rightarrow$ (i) If $\lambda = 0$ is the only eigenvalue, then the Jordan normal form looks like the 0 matrix, except with maybe some 1's on the superdiagonal. Clearly any such matrix is nilpotent, so $A^n = (P^{-1}JP)^n = P^{-1}J^nP = 0$. □

(b) Prove that A is symmetric and nilpotent if and only if $A = 0$.

Proof. This is a straightforward consequence of the Schur decomposition. Stronger is true: the only *normal* nilpotent matrix is 0. □

(c) Prove that if A and B are both nilpotent and $AB = BA$, then the matrices AB and $rA + sB$ are nilpotent for all $r, s \in \mathbb{R}$.

Proof. Note that $A^n = B^k = 0$ implies $(AB)^{nk} = 0$.

Since they commute, we also have

$$\begin{aligned}(A+B)^{n+k} &= \sum_{i=0}^{n+k} \binom{n+k}{n} A^{(n+k)-i}B^i \\ &= \sum_{i=0}^{k} \binom{n+k}{n} A^{(n+k)-i}B^i + \sum_{i=k}^{n+k} \binom{n+k}{n} A^{(n+k)-i}B^i \\ &= \sum_{i=0}^{k} \binom{n+k}{n} 0B^i + \sum_{i=k}^{n+k} \binom{n+k}{n} A^{(n+k)-i}0 \\ &= 0.\end{aligned}$$

As rA is nilpotent too, we get that $rA + sB$ is nilpotent. □

(d) Prove or disprove: If the matrices AB and $rA + sB$ are nilpotent for all $r, s \in \mathbb{R}$, then $AB = BA$.

Proof. Consider

$$A = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{pmatrix}.$$

These matrices are nilpotent, so any scalar multiple is, and by above so will their sum be nilpotent. Their products are

$$AB = \begin{pmatrix} 0 & 0 & af \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } BA = \begin{pmatrix} 0 & 0 & cd \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Both are nilpotent, but not equal in general. □

4. Let G be an additive abelian group.

For each positive integer n, set $\Gamma_n(G) = \{g \in G \mid n^m g = 0 \text{ for some positive integer } m\}$. Let $\alpha : G \to H$ and $\beta : H \to K$ be homomorphisms of additive abelian groups

(a) Prove that $\Gamma_n(G)$ is a subgroup of G.

Proof. Let $x, y \in \Gamma_n(G)$. Then $n^{m_1}x = 0$ and $n^{m_2}y = 0$. Hence

$$\begin{aligned}n^{m_1+m_2}(x-y) &= n^{m_1+m_2}x - n^{m_1+m_2}y \\ &= n^{m_2}n^{m_1}x - n^{m_1}n^{m_2}y \\ &= n^{m_2}0 - n^{m_1}0 \\ &= 0.\end{aligned}$$

Thus $x - y \in \Gamma_n(G)$ □

(b) Prove that $\alpha(\Gamma_n(G)) \subseteq \Gamma_n(H)$ and that $\Gamma_n(\alpha) : \Gamma_n(G) \to \Gamma_n(H)$ defined by $\Gamma_n(\alpha)(g) = \alpha(g)$ is a well-defined group homomorphism.

Proof. Let $x \in \Gamma_n(G)$, meaning $n^m x = 0$. Now $\alpha(x) = y$ for some $y \in H$. Thus

$$n^m y = n^m \alpha(x) = \alpha(n^m x) = 0.$$

Hence $\alpha(\Gamma_n(G)) \subseteq \Gamma_n(H)$.

Showing well-definedness and homomorphism is just writing it out. □

(c) Prove that if α is injective (i.e., 1-1), then so is $\Gamma_n(\alpha)$.

Proof. Suppose that α is injective. Then $\text{Kern}(\Gamma_n(\alpha)) = \text{Kern}(\alpha(g)) = \{0\}$ implies that $g = 0$. □

(d) Prove or disprove that if α is surjective (i.e., onto), then so is $\Gamma_n(\alpha)$.

Proof. It is not true. Let $G = \mathbb{Z}$ and $H = \mathbb{Z}_2$. Then taking $\alpha : G \to H$ as the reduction modulo 2 is a surjective homomorphism. But $2^1 h = 0$ for all $h \in H$, hence $\Gamma_2(H) = H$. But $\mathbb{Z}$ has no non-zero elements of finite order, so $1 \in H$ has no preimage in $\Gamma_2(G)$. □

(e) Prove that if G is finitely generated, then $\Gamma_n(G)$ is finite.

Proof. Apply the fundamental theorem of finitely generated Abelian groups. □

5. Assume that A is an integral domain with field of fractions K, and let a be a non-zero element of A. Consider A as a subring of the polynomial ring $A[x]$.

(a) Prove that the following set is a subring of K containing A. $A_a = \{r/a^n \in K | r \in A \text{ and } n \in \{0, 1, 2, ...\}\}$.

Proof. This localization obviously contains A when $n = 0$. To show subring, note that

$$\frac{r_1}{a^{n_1}} \cdot \frac{r_2}{a^{n_2}} = \frac{r_1 r_2}{a^{n_1+n_2}}$$

and

$$\frac{r_1}{a^{n_1}} - \frac{r_2}{a^{n_2}} = \frac{r_1 a^{n_2} - r_2 a^{n_1}}{a^{n_1+n_2}}$$

□

(b) Prove that the function $\phi : A \to A[x]/\langle xa - 1\rangle$ given by $\phi(a) = a + \langle xa - 1\rangle$ is a ring homomorphism that is injective (i.e., 1-1).

Proof. This might be easier in light of part (c). (Homomorphism)

(Injective) □

(c) Prove that the rings A_a and $A[x]/\langle xa - 1\rangle$ are isomorphic.

Proof. Quotienting a polynomial ring is the same as adjoining roots.

$$A[x]/\langle xa-1\rangle \cong A\left[\frac{1}{a}\right] = A_a.$$

□

(d) Prove that the ring $A[x]/\langle xa-1\rangle$ satisfies the following property: For every commutative ring with identity B, for every ring homomorphism $\psi : A \to B$, if $\psi(a)$ is a unit in B, then there is a unique ring homomorphism $\Phi : A[x]/\langle xa-1\rangle \to B$ such that $\Phi(\psi(c)) = \phi(c)$ for all $c \in A$ and such that $\Psi(x+\langle xa-1\rangle) = \psi(a)-1$.

Proof. □

6. Let A be a non-zero commutative ring with identity, and set

$$\mathrm{Aut}(A) = \{\text{isomorphisms } f : A \xrightarrow{\cong} A\}.$$

Let S be a subset of $\mathrm{Aut}(A)$, and set $A^S = \{a \in A \mid f(a) = a \text{ for all } f \in S\}$.

Let T be a subset of A, and set $\mathrm{Aut}_T(A) = \{f \in \mathrm{Aut}(A) \mid f(t) = t \text{ for all } t \in T\}$.

(a) Prove that $\mathrm{Aut}(A)$ is a group under function composition.

Proof. Standard proof. Composition of bijective is bijective, associativity, identity element, and inverses. If you want to be more clever about it, note that $\mathrm{Aut}(A)$ is a subgroup of $\mathrm{Sym}(A)$, then apply the 2-step subgroup test. □

(b) Prove that A^S is a subring of A.

Proof. Again, standard. Just check the axioms. □

(c) Let G be the subgroup of $\mathrm{Aut}(A)$ generated by S, and prove that $A^S = A^G$.

Proof. Consider the following lemma: if f and g are automorphisms of G that coincide on a set of generators, then $f = g$. □

(d) Prove that $\mathrm{Aut}_T(A)$ is a subgroup of $\mathrm{Aut}(A)$.

Proof. Again, 2-step subgroup test. □

(e) Prove that $G \subseteq \mathrm{Aut}_{A^G}(A) = \mathrm{Aut}_{A^S}(A)$ and $T \subseteq A^{\mathrm{Aut}_T(A)}$. Conclude further that if R is the intersection of all the subrings of A containing T, then $R \subseteq A^{\mathrm{Aut}_T(A)}$.

Proof. Looks annoying : (□

Summer 2019

1. Fix an integer $d \geq 2$, and consider the real vector space

$$V_d = \mathbb{R}[x]_{<d} = \{a_0 + a_1 x + a_2 x^2 + ... + a_{d-1} x^{d-1} | a_0, ..., a_{d-1} \in \mathbb{R}\}.$$

For all $f, g \in V_d$, define

$$\langle f, g \rangle = \int_0^1 fg \, dx$$

where fg is the usual product of f and g from calculus.

(a) Prove that $\langle \cdot, \cdot \rangle$ is an inner product on V_d.

Proof. Linearity follows from properties of integrals. Symmetry is clear, and $\langle f, f \rangle = \int f^2 \, dx \geq 0$. □

(b) In the case $d = 3$, apply the Gram-Schmidt process to the basis 1, x, x^2 to find an orthonormal basis for V_3. Then consider the subspace $W = \text{Span}_{\mathbb{R}}(1 - 2x)$ and find a basis for $W^{\perp}$.

Proof. We should get

$$\left[1, \, 5x - \frac{5}{2}, \, 180x^2 - 180x + 30\right].$$

Note that $W = \text{Span}_{\mathbb{R}}(e_2)$ above, so the basis for $W^{\perp}$ will be everything orthogonal to e_2, which is spanned by e_1 and e_3. □

(c) Let $D : V_d \to V_d$ be the differentiation operator $D(f) = f' = df/dx$, which is a linear transformation. Find the matrix representing D with respect to the basis 1, x, ..., x^{d-1}. Prove or disprove: D is an isomorphism.

Proof.

$$\begin{pmatrix} 0 & 0 & ... & 0 \\ 1 & 0 & ... & 0 \\ 0 & 2 & ... & 0 \\ ... & & & \\ 0 & ... & d-1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ ... \\ x^{d-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2x \\ ... \\ (d-1)x^{d-2} \end{pmatrix}.$$

This is clearly not invertible. Another way to see this is that all constants get sent to 0, so of course it's not an isomorphism. □

(d) Prove or disprove: D is diagonalizable.

Proof. A matrix is diagonalizable if it has n distinct eigenvalues; so if it has n repeated eigenvalues then it is not diagonalizable. The eigenvalues for D will be all 0's, so not diagonalizable. □

(e) Compute $D^*(a_0 + a_1x + a_2x^2 + ... + a_{d-1}x^{d-1})$ where $D^* : V \to V$ is the adjoint of D.

Proof. □

2. Let $A_p = \begin{bmatrix} 4 & 1 & p \\ 0 & 5 & 1 \\ 0 & 1 & 5 \end{bmatrix}$, $p \in \mathbb{R}$.

(a) Find the characteristic and the minimal polynomial of A_p.

Proof. This should be calculated *after* finding the Jordan normal form. Minimal and characteristic coincide here.

$$\chi(x) = x^3 - 14x^2 + 64x - 96 = (x-6)(x-4)^2.$$

□

(b) Find the Jordan normal form J of A_p and a matrix S such that $A = SJS^{-1}$.

Proof. Clearly an eigenvector is $v_1 = (1, 0, 0)$. A less obvious one is $v_2 = (\frac{1+p}{2}, 1, 1)$. An even more less obvious one is $v_3 = (0, \frac{1}{1-p}, \frac{-1}{1-p})$. These show that the eigenvalues are $4, 4, 6$. Thus:

$$J = \begin{bmatrix} 4 & 1 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{bmatrix}$$

and

$$S = \begin{bmatrix} 1 & 0 & \frac{1+p}{2} \\ 0 & \frac{1}{1-p} & 1 \\ 0 & \frac{-1}{1-p} & 1 \end{bmatrix}.$$

□

(c) Prove that $V[A_p] = \{a_0I + a_1A_p + ... + a_nA_p^n | a_i \in \mathbb{R}, n \in \mathbb{N}\}$ with the usual matrix addition and scalar multiplication is a vector space over R.

Proof. Check the axioms. □

(d) Find the dimension and a basis for $V[A_p]$.

Proof. The minimal polynomial being $\chi(x) = x^3 - 14x^2 + 64x - 96$ implies the dimension is 3. A basis is $[I, A, A^2]$, since $A^3 = 14A^2 - 64A + 96I$. □

3. (a) Prove: If W_1 and W_2 are subspaces of V then $W_1 \cup W_2$ is a subspace of V if and only if $W_1 \subset W_2$ or $W_2 \subset W_1$.

Proof. For contradiction, suppose neither is a subset of the other. Then $\exists u \in W_1 \setminus W_2$ and $\exists v \in W_2 \setminus W_1$. Hence both u and v are in $W_1 \cup W_2$. But this union is a subspace, so $u + v \in W_1 \cup W_2$, implying that $u + v \in W_1$ or $u + v \in W_2$. However, this means that either $(u + v) - u \in W_1$ or $(u + v) - v \in W_2$. Either way, we get a contradiction. □

(b) Let x and y be distinct eigenvectors of a matrix A such that $x + y$ is also an eigenvector of A. Prove that x and y correspond to the same eigenvalue.

Proof. Let $Ax = \lambda x$ and $Ay = \mu y$. As $x + y$ is an eigenvector, write $A(x + y) = \nu(x + y)$. Then $\lambda x + \mu y = A(x + y) = \nu x + \nu y$, implying that $\lambda = \nu = \mu$, a contradiction. □

(c) Prove that a self-adjoint linear map $T : V \to V$ on a complex inner product space V has only real eigenvalues and that eigenvectors corresponding to different eigenvalues are orthogonal.

Proof.

$$\lambda \left|\left|x\right|\right|^2 = \lambda\langle x, x\rangle = \langle Tx, x\rangle = \langle x, Tx\rangle = \overline{\lambda}\langle x, x\rangle = \overline{\lambda} \left|\left|x\right|\right|^2.$$

Now, let $Tx = \lambda x$ and $Ty = \mu y$. Then

$$\lambda\langle x, y\rangle = \langle Tx, y\rangle = \langle x, Ty\rangle = \overline{\mu}\langle x, y\rangle = \mu\langle x, y\rangle.$$

Since these correspond to different eigenvalues, it must be that $\langle x, y\rangle = 0$. □

(d) Find all self-adjoint complex $n \times n$ matrices A that satisfy $A^3 = 2A + 4I$.

Proof. This has the trivial solution $x = 2$, and polynomial division gives the other roots as $x = \pm i - 1$. By Cayley-Hamilton, these must be the eigenvalues of A. But a self-adjoint map has only real eigenvalues, hence any such matrix has the eigenvalue 2 repeated with multiplicity n. Thus $A = P\left(\text{diag}\{2\}\right)P^{-1}$ for an invertible P. □

4. Let G be a finite group acting on itself by conjugation. In this problem, you may assume basic results, such as the orbit-stabilizer theorem, or classification of finite abelian groups, provided that you properly state them.

(a) Characterize the orbits, stabilizers, kernel, and fixed points of this action. Your answer should be in terms of familiar group-theoretic objects, not just the definitions of these terms.

Proof. □

(b) Prove that the size of any conjugacy class divides $|G|$.

Proof. □

(c) Show that if G contains an element $x \in G$ that has exactly two conjugates, then G cannot be simple.

Proof. □

(d) Prove that if G is a p-group, then its center is non-trivial.

Proof. □

(e) Classify all simple p-groups, with proof. You may use the results of the previous parts, even if you could not prove them.

Proof. □

5. The *First Isomorphism Theorem* holds for a variety of algebraic structures, and it relates the quotient of the domain of a homomorphism to its kernel and image.

(a) Prove that the kernel of a group homomorphism is a subgroup and that it is normal.

Proof. □

(b) State and prove the First Isomorphism Theorem for groups.

Proof. □

(c) Prove that the kernel of a ring homomorphism is a two-sided ideal.

Proof. □

(d) State and prove the First Isomorphism Theorem for rings

Proof. □

6. Prove or disprove each of the following:

(a) Every Euclidean domain is a principal ideal domain.

Proof. □

(b) Every principal ideal domain is a Euclidean domain.

Proof. □

(c) Every principal ideal domain is a unique factorization domain.

Proof. □

(d) Every unique factorization domain is a principal ideal domain.

Proof. □

(e) Every integral domain is a unique factorization domain.

Proof. □

Winter 2020

1. Let V be an n-dimensional complex vector space and $T : V \to V$ a linear map. We say that $v \in V$ is a cyclic vector for T if $\{v, Tv, ..., T^{n-1}v\}$ is a basis for V . Let $p_T \in \mathbb{C}[x]$ and $m_T \in \mathbb{C}[x]$ be the characteristic polynomial and the minimal polynomial of T, respectively.

   (a) Prove that if $T^{n-1}v \neq 0$ but $T^n v = 0$, then v is a cyclic vector for T.

   Proof. □

   (b) Prove that if V has a cyclic vector for T then $m_T = p_T$.

   Proof. □

   (c) Prove that if T is diagonalizable and $m_T = p_T$, then V has a cyclic vector for T.

   Proof. □

   (d) Prove that if V has a cyclic vector for T and $S : V \to V$ is a linear map which commutes with T, then S is a polynomial in T.

   Proof. □

2. Let V and W be real vector spaces, and let $\mathrm{Hom}_{\mathbb{R}}(W, V)$ denote the set of linear transformations $W \to V$, which is a real vector space.

   (a) Let $z \in \mathbb{C}$ and $\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$. Define $z\phi : \mathbb{C} \to V$ by the formula $(z\phi)(w) = \phi(zw)$. Prove that $z\phi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

   Proof. □

   (b) Prove that $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$ is a complex vector space using part (a) to define scalar multiplication.

   Proof. □

   (c) Prove that if $d = \dim_{\mathbb{R}}(V) < \infty$, then $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)) = d$.

   Proof. □

   (d) Prove that if $f : V \to W$ is a linear transformation over $\mathbb{R}$, then the function $f^* : \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V) \to \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, W)$ defined by $f^*(\phi) = f \circ \phi$ is a linear transformation over $\mathbb{C}$.

   Proof. □

   (e) Prove that if $\lambda \in \mathbb{R}$ is an eigenvalue for a linear transformation $f : V \to V$, then λ is an eigenvalue for $f^* : \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V) \to \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, V)$.

Proof. □

3. Let $\sigma : V \to V$ be any linear map of vector spaces over a field k. Define an action of $k[X]$ on V as follows: for any polynomial $p(X) = \sum i = 0^n c_i X^i \in k[X]$ and any $v \in V$,

$$p(X) \cdot v = p(\sigma)(v) = \sum i = 0^n c_i \sigma^i(v),$$

where σ^0 is the identity map on V . The kernel of $p(X)$ is defined to be

$$\ker(p(X)) = \{v \in V \ : \ p(X) \cdot v = 0\}.$$

(a) Show that, for any two polynomials $a(X), b(X) \in k[X]$ and any $v \in V$,

$$a(X) \cdot (b(X) \cdot v) = (a(X)b(X)) \cdot v$$

Proof. □

(b) Show that $\text{Kern}(p(X))$ is a σ-invariant subspace of V. When $p(X) = X - \lambda$ where $\lambda \in k$, explain why $\text{Kern}(p(X))$ is the eigenspace of σ with respect to λ.

Proof. □

(c) Let $p(X)$ and $q(X)$ be polynomials in $k[X]$ so that $\gcd(p(X), q(X)) = 1$. Show that

$$\text{Kern}(p(X)q(X)) = \text{Kern}(p(X)) + \text{Kern}(q(X))$$

and that this sum is direct. Further show that, if $c(X) \in k[X]$ is factored as

$$c(X) = p_1(X)p_2(X)...p_m(X)$$

where $p_i(X) \in k[X]$ and $\gcd(p_i(X), p_j(X)) = 1$ for all $1 \leq i < j \leq m$, then

$$\text{Kern}(c(X)) = \text{Kern}(p_1(X)) + \text{Kern}(p_2(X)) + ... + \text{Kern}(p_m(X))$$

and that this sum is direct. (**Hint**: Use the fact that if $\gcd(p(X), q(X)) = 1$ then there exist $a(X), b(X) \in k[X]$ so that $a(X)p(X) + b(X)q(X) = 1$.)

Proof. □

(d) Let $\lambda_i \in k$, $1 \leq i \leq t$, be distinct eigenvalues of σ. Let $B_i = \{u_{ij} : 1 \leq j \leq m_i\}$ be a basis for the eigenspace of λ_i for $1 \leq i \leq t$. Use part (c) to show that the union $B_1 \cup B_2 \cup ... \cup B_t$ is a set of independent vectors.

Proof. □

4. For this problem, we let G be a group. If $x, y \in G$, we define the commutator of x and y to be $[x, y] = x^{-1}y^{-1}xy$ and denote the commutator subgroup by $[G, G] = G'$ (recall that the commutator subgroup of G is the subgroup of G that is generated by the commutators of G).

(a) Show that the inverse of a commutator is a commutator and that any conjugate of a commutator is a commutator.

Proof. $[x,y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y,x]$. Similarly, $z^{-1}[x,y]z = (z^{-1}x^{-1}z)(z^{-1}y^{-1}z)(z^{-1}xz)(z^{-1}yz) = [z^{-1}xz, z^{-1}yz]$. □

(b) Show that G' is a normal subgroup of G.

Proof. This was proved above. □

(c) Show that if $\psi \in \mathrm{Aut}(G)$ then $\psi(G')$ is a subgroup of G'.

Proof. $\psi([x,y]) = \psi(x^{-1}y^{-1}xy) = \psi(x)^{-1}\psi(y)^{-1}\psi(x)\psi(y)$. Since $\psi \in \mathrm{Aut}(G)$, this takes the form of $u^{-1}v^{-1}uv = [u,v]$. □

(d) Show that if $\phi : G \to H$ is a homomorphism of groups then $\mathrm{Im}(\phi)$ is abelian if and only if G' is a subgroup of $\mathrm{Kern}(\phi)$.

Proof. ($\Rightarrow$) Suppose $\mathrm{Im}(\phi)$ is Abelian. Then $\phi([x,y]) = e$, so $G' \subseteq \mathrm{Kern}(\phi)$.
($\Leftarrow$) Suppose $G' \subseteq \mathrm{Kern}(\phi)$. Then $\phi([x,y]) = e$ for all $x, y \in G$, i.e.: $\phi(x)\phi(y) = \phi(y)\phi(x)$. □

(e) Show that if N is a subgroup of G which contains G' then N is a normal subgroup of G.

Proof. We know that $G' \lhd G$, and that G/G' is Abelian. Any subgroup of an Abelian group is normal, so H/G' a subgroup of G/G' implies $H/G' \lhd G/G'$. Thus by Third Iso. Thm, $H \lhd G$. □

5. Let R be a commutative ring with identity and $\emptyset \neq S \subseteq R$ be a nonempty subset. We say that S is *multiplicatively closed* if $s, t \in S \;\Rightarrow\; st \in S$. Additionally, we say that the set S is *saturated* if $st \in S \;\Rightarrow\; s, t \in S$.

(a) Let $I \subseteq R$ be an ideal. Show that its complement $S := R \setminus I$ is saturated.

Proof. □

(b) Let $I \subseteq R$ be an ideal. Show that its complement $S := R \setminus I$ is multiplicatively closed if and only if R/I is an integral domain.

Proof. □

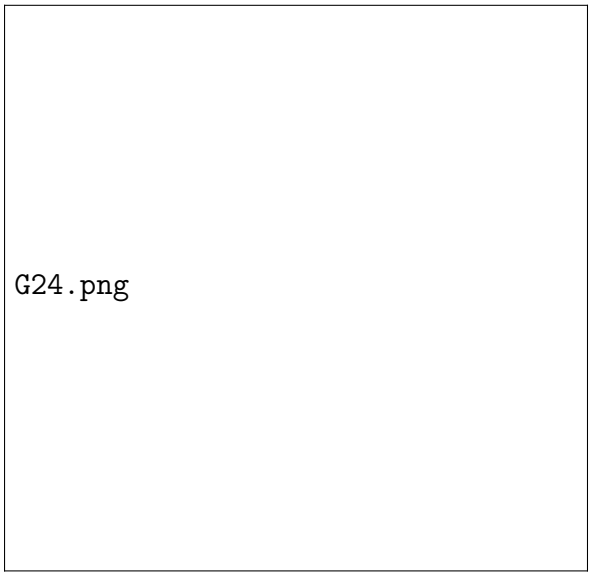
(c) Suppose that S is a multiplicatively closed subset of R that does not contain 0. Show that there is an ideal in $P \subset R$ that is maximal with respect to the property that $P \cap S = \emptyset$.

Proof. □

(d) Let S be as in part (c) and suppose that P is maximal with respect to the property that $P \cap S = \emptyset$. Show that P is necessarily prime.

Proof. □

6. In this problem G refers to the group of order 24 whose subgroup lattice appears below. You must fully justify each answer for full credit.



(a) Show that in any group, a subgroup of order 2 is normal if and only if it is contained in the center.

Proof. □

(b) Partition the fifteen subgroups into equivalence classes by conjugacy.

Proof. □

(c) Is G is solvable? Nilpotent?

Proof. □

(d) What familiar group is the quotient $G/\langle a^3 \rangle$ isomorphic to? Justify your answer by drawing its subgroup lattice.

Proof. □

(e) What familiar group is the subgroup $\langle a^2b, ab^2 \rangle$ isomorphic to? Justify your answer by drawing its subgroup lattice.

Proof. □

(f) What familiar group is the quotient $\langle a^2b, ab^2\rangle/\langle a^3\rangle$ isomorphic to? Use the isomorphism theorems to justify your answer.

Proof. □

Summer 2020

1. Let V be a vector space over a field k, and consider the following subset of the vector space $V \times V$.

$$\Delta = \{(v, v) \mid v \in V\}.$$

(a) Prove that Δ is a subspace of $V \times V$.

Proof. □

(b) Prove that $\Delta \cong V \cong (V \times V)/\Delta$. Do not assume that V is finite dimensional over k.

Proof. □

(c) Give another proof of part (b) assuming that V is finite dimensional over k.

Proof. □

Assume now that V is a vector space over $\mathbb{R}$ equipped with a Euclidean structure denoted $\langle \cdot, \cdot \rangle$.

(d) Prove that the formula $\langle (v, w), (v', w') \rangle = \langle v, v' \rangle + \langle w, w' \rangle$ describes a Euclidean structure on $V \times V$.

Proof. □

(e) Prove that $(v, v) \perp (-w, w)$ for all $v, w \in V$.

Proof. □

(f) Prove that $\Delta^{\perp} \cong V$ Do not assume that V is finite dimensional over k.

Proof. □

(g) Give another proof of part (f) assuming that V is finite dimensional over k.

Proof. □

2. We consider the inner product space $\mathbb{C}^n$ with its standard inner product$\langle u, v \rangle = u_1 v_1 + ... + u_n v_n$. Let $T : \mathbb{C}^n \to \mathbb{C}^n$ be defined by

$$T(z_1, z_2, ..., z_n) = (z_2 - z_1, z_3 - z_2, ..., z_1 - z_n).$$

(a) Give an explicit expression for the adjoint, T^*. Justify your answer.

Proof. □

(b) Find the characteristic and the minimal polynomials of T. Is T diagonalizable? Explain.

Proof. □

(c) Does $\mathbb{C}^n$ have an orthonormal basis of eigenvectors for T? Justify your answer.

Proof. □

(d) Prove that $\mathbb{C}^n$ is an orthogonal direct sum of the range of T and the kernel of T, i.e., $\mathbb{C}^n = R(T) \dot{\oplus} K(T)$.

Proof. □

(e) Is it true that for every linear map $S : \mathbb{C}^n \to \mathbb{C}^n$, $\mathbb{C}^n = R(T) \dot{\oplus} K(T)$? Prove or disprove.

Proof. □

3. Let $\mathbb{F}$ a field and V a vector space over $\mathbb{F}$ of dimension n. Let $\phi : V \to V$ be an $\mathbb{F}$-linear map. For any polynomial $g(x) \in \mathbb{F}[x]$, define

$$V_g = \{v \in V \ : \ g(\phi)(v) = 0\}$$

(a) Show that V_g is a ϕ-invariant subspace of V. (Need to show that it's a linear subspace and, for each $v \in V_g$, $\phi(v) \in V_g$.)

Proof. □

(b) Suppose $g(x), h(x) \in \mathbb{F}[x]$ are such that $g(\phi)h(\phi) = 0$, the zero map on V, and $\gcd(g(x), h(x)) = 1$. Show that V is the direct sum of V_g and V_h.

Proof. □

(c) Suppose $\mathbb{F} = \mathbb{C}$, and ϕ has characteristic polynomial $f(x) = x^m(x^2+1)^t$ where $m + 2t = n$ and minimal polynomial $m(x) = x(x^2+1)$. Show that ϕ has n independent eigenvectors in V, hence the matrix of ϕ under any basis of V is diagonalizable.

Proof. □

(d) Give an example of V and ϕ so that ϕ has characteristic polynomial $f(x) = x^m(x^2+1)^t$ where $m + 2t = n$ and minimal polynomial $m(x) = x^2(x^2+1)$, and show that the matrix of ϕ under any basis of V is not diagonalizable. (Hint: Fix a basis of V, construct the matrix of ϕ under this basis, using Jordan normal form.)

Proof. □

4. For this problem, let G be a group, $H \leq G$ a subgroup, and $N := \bigcap_{g \in G} gHg^{-1}$.

(a) Show that N is a normal subgroup of G.

Proof. □

(b) Show that if M is any normal subgroup of G contained in H, then M is contained in N.

Proof. □

(c) Show that if $|H| = m$ and H is the only subgroup of G of order m, then H is normal in G.

Proof. □

(d) Is the converse to the previous part true (that is, if H is of order m and normal in G, is it true that H is the only subgroup of G of order m)? Prove this or give a counterexample.

Proof. □

(e) Suppose that H is a subgroup of A_n, $n \geq 5$ with $|H| = m$, and $1 < m < \frac{n!}{2}$. Show that there are at least n subgroups of A_n of order m.

Proof. □

5. Consider a left action of a group G on a set X, both finite.

(a) Fix $x \in X$, and let $H = \mathrm{Stab}(x)$, the stabilizer of x. Show that group elements g_1 and g_2 send x to the same element of X if and only if they are in the same left coset of H.

Proof. □

(b) Recall *Lagrange's theorem*, that $|G| = [G : H]|H|$. Show how this, along with Part (a), implies the *orbit-stabilizer theorem*:

$$|G| = |\operatorname{Orb}(x)||\operatorname{Stab}(x)| \text{ for any } x \in X.$$

Proof. □

(c) Show how the orbit-stabilizer theorem, applied to the appropriate group action, implies Cayley's theorem: If $|G| = n$, then there is an embedding $G \hookrightarrow S_n$.

Proof. □

(d) Show how the orbit-stabilizer theorem, applied to the appropriate group action, implies that the size of any conjugacy class of G divides $|G|$.

Proof. □

(e) Prove that if $|G| = p^n$, then $|Z(G)| > 1$, where $Z(G)$ is the center of G.

Proof. □

2. For this problem, we let p be a positive prime integer, $\mathbb{Z}$ the ring of integers, and $\mathbb{Z}_n$ the ring of integers modulo the natural number n. If R is a ring, then the notation $R[x]$ means the ring of polynomials over R. If $k \in Z$ then we denote its reduction modulo n by $\overline{k}$.

   (a) Show that the ring $\mathbb{Z}_p$ is a field.

   Proof. □

   (b) Show that the ring $\mathbb{Z}_p[x]$ is a PID.

   Proof. □

   (c) Show that if R is a commutative ring with identity, and $M \subseteq N \subsetneq R$ are proper ideals, then N is a maximal ideal of R if and only if N/M is a maximal ideal of R/M.

   Proof. □

   (d) Let $n \in \mathbb{N}$ and $f(x) = x^n + m_{n-1}x^{n-1} + ... + m_1x + m_0 \in \mathbb{Z}[x]$. Show that $(p, f(x))$ is a maximal ideal of $\mathbb{Z}[x]$ if and only if $x^n + \overline{m}_{n-1}x^{n-1} + ... + \overline{m}_1x + \overline{m}_0$ is an irreducible polynomial in $\mathbb{Z}_p[x]$.

   Proof. □

   (e) If $(p, f(x))$ is a maximal ideal of $\mathbb{Z}[x]$, how many elements does $\mathbb{Z}[x]/(p, f(x))$ have? Explain.

   Proof. □

Winter 2021

1. Let X be an n-dimensional vector space over K. We will denote the *dual* of X by the set
$$X' := \{l : X \to K \mid l \text{ is linear}\},$$
and use *scalar product* notation $(l, x) := l(x)$. The transpose of a linear map $A : X \to X$ is a linear map $A' : X' \to X'$ defined by $A' : l \mapsto m$, where $A(l(x)) = m(x)$ for all $x \in X$.

   (a) Write out the definition of the transpose map using scalar product notation, without using "m".

   Proof. □

   (b) Suppose that A has distinct eigenvalues $\lambda_1, ..., \lambda_n$. Prove that the corresponding eigenvectors $v_1, ..., v_n$ are linearly independent.

   Proof. □

   (c) Still using the assumptions of Part (b) let $l_1, ..., l_n \in X'$ be the *dual basis*, which means that
$$(l_i, v_i) = \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$
   Prove that $l_1, ..., l_n$ are eigenvectors of the transpose map $A' : X' \to X'$.

   Proof. □

   (d) Now, suppose that $f_1, ..., f_n$ is any basis of eigenvectors of A' corresponding to $\lambda_1, ..., \lambda_n$. Prove that $(f_i, v_j) = 0$ if $i \neq j$ and $(f_i, v_i) \neq 0$.

   Proof. □

   (e) For any $x = a_1 v_1 + ... + a_n v_n$, derive a formula for a_i in terms of x, v_i, and f_i.

   Proof. □

2. Let R be an arbitrary commutative ring that contains a field $\mathbb{F}$ where the multiplicative identity 1 of $\mathbb{F}$ is also the multiplicative identity of R. For any $a \in R$, define a map $m_a : R \to R$ via multiplication, that is, $m_a(v) = a \cdot v$ for $v \in R$. Note that R is a vector space over $\mathbb{F}$ and m_a is a linear map on R over $\mathbb{F}$. An element $\lambda \in \mathbb{F}$ is called an eigenvalue for a (or m_a) if $av = \lambda v$ for some nonzero $v \in R$, and such a v is called an eigenvector of m_a.

   (a) Show that m_a is injective (one-to-one) if and only if a is a nonzero divisor in R (i.e., $ab \neq 0$ for every nonzero $b \in R$). Give an example of R and $a \in R$ so that m_a is injective but not surjective.

Proof. □

(b) Show that m_a is bijective if and only if a is invertible in R (i.e., there exists $b \in R$ so that $ab = 1$).

Proof. □

(c) Suppose R has dimension n as a vector space over $\mathbb{F}$. Show that, for every $a \in R$, there is a monic polynomial $f(y) \in \mathbb{F}[y]$ of degree $\leq n$ so that $f(a) = 0$. (**Hint**: Fix a basis for R over $\mathbb{F}$ and consider the characteristic polynomial of the linear map m_a.)

Proof. □

(d) Consider the ring $R = \mathbb{Q}[x]/(\phi(x))$ where $\phi(x) = x^3 - x = x(x-1)(x+1)$. Find all eigenvalues and eigenvectors of m_a for $a = 1 + 2x \in R$. Verify that you can pick your eigenvectors $v_1, v_2, v_3 \in R$ so that

$$v_i(p_j) = \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

where $p_1 = -1$, $p_2 = 0$, $p_3 = 1$ (the distinct roots of $\phi(x)$), and $v(p)$ denotes the value of v as a polynomial in $\mathbb{F}[x]$ at a point $p \in \mathbb{F}$.

Proof. □

3. Let $\mathcal{M}_{n\times n}(\mathbb{R})$ be the space of all real n-by-n matrices with the inner product $\langle A, B\rangle := \operatorname{tr}(A^T B)$. Let $S \in \mathcal{M}_{n\times n}(\mathbb{R})$. Consider the linear map $L_S : \mathcal{M}_{n\times n}(\mathbb{R}) \to \mathcal{M}_{n\times n}(\mathbb{R})$ defined by $L_S : X \to XS + SX$.

(a) Prove that if λ is an eigenvalue of S, v is a corresponding eigenvector, and $v \in \operatorname{null}(L_S(M))$, then Mv is also an eigenvector of S, with a corresponding eigenvalue $-\lambda$.

Proof. □

(b) Prove that if S is symmetric positive definite, then L_S is injective.

Proof. □

(c) Prove that if S is symmetric, then L_S is self-adjoint.

Proof. □

(d) If S is positive definite, is L_S necessarily positive definite? Prove or disprove.

Proof. □

4. For this problem, let R be a commutative ring with identity. We recall that an ideal $I \subsetneq R$ is *radical* if $x^n \in I$ implies that $x \in I$, and that I is primary if $ab \in I$ implies that $a \in I$ or $b^n \in I$ for some $n \in \mathbb{N}$.

   (a) Show that $I \subsetneq R$ is radical if and only if R/I is reduced (that is R/I has no nonzero nilpotent elements).

   Proof. □

   (b) Show that $I \subsetneq R$ is primary if and only if every zero divisor of R/I is nilpotent.

   Proof. □

   (c) Show that an ideal $I \subsetneq R$ is prime if and only if it is both radical and primary.

   Proof. □

   (d) Show that the ideal $I \subsetneq R$ is prime if and only if the ideal $I[x] := \{\sum_{k=0}^{n} \alpha_k x^k | \alpha_k \in I\}$ is a prime ideal of $R[x]$.

   Proof. □

   (e) Now let R be a principal ideal domain (PID). Characterize all nonzero proper ideals of R that are radical, and characterize all nonzero proper ideals of R that are primary.

   Proof. □

5. For this problem, fix p to be a prime number and $G = (\mathbb{Z}/p^3\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})$.

   (a) Prove there is only one subgroup of G of each of the following types:

      (i) Isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ and

      Proof. □

      (ii) Isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})^2$

      Proof. □

   (b) Show that there are

      (i) $p+1$ subgroups of G isomorphic to $\mathbb{Z}/p\mathbb{Z}$,

      Proof. □

      (ii) p^2+p subgroups of G isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$, and

      Proof. □

      (iii) p^2 subgroups of G isomorphic to $\mathbb{Z}/p^3\mathbb{Z}$,

      Proof. □

(c) Show the following:

(i) Suppose that H_1 and H_2 are two subgroups of G isomorphic to $(\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. Prove that $|H_1 \cap H_2| \geq p^2$.

Proof. □

(ii) Using the same notation as Part *i.*, describe the isomorphism class of $H_1 \cap H_2$ as a product of cyclic groups.

Proof. □

(iii) Prove that there are $p+1$ subgroups of G isomorphic to $(\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$,

Proof. □

(iv) By following Parts *i.*, *ii.*, and *iii.*, compute the number of subgroups of G isomorphic to $(\mathbb{Z}/p^3\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

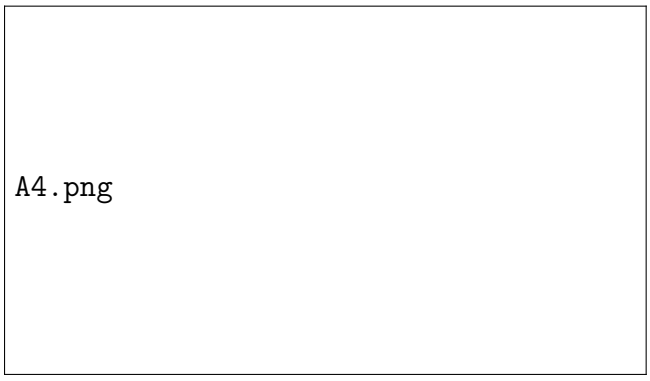
Proof. □

6. Recall that the normalizer of a subgroup $H \leq G$ is the set

$$N_G(H) := \{x \in G | xHx^{-1} = H\},$$

or equivalently, the union of the left cosets that are also right cosets.

(a) Consider the group A_4, whose subgroup lattice is shown below, for convenience.



Partition the ten subgroups of A_4 into equivalent classes by conjugacy. Then, pick one subgroup H from each class, find its normalizer $N_{A_4}(H)$, determine the index $[A_4 : N_{A_4}(H)]$, and decide whether or not H is normal.

Proof. □

(b) The purpose of the previous part was to serve as a gentle "warm-up" for the following. Let H be a subgroup of a finite group G, and consider the following three quantities:

(i) $[G : H]$, the number of cosets of H in G;

(ii) $|\{gHg^{-1} | g \in G\}|$, the number of subgroups conjugate to H;

(iii) $[G : N_G(H)]$, the number of cosets of the normalizer of H in G.

Two of these are always equal to each other, and one can be different. State and prove the correct equality and the inequality.

Proof. □

(c) Consider the action of a p-group G (i.e., $|G| = p^n$) on a finite set X, which is just a homomorphism $\phi : G \to S_X$ to the permutations of X. Prove that

$$|X| \equiv |\mathrm{Fix}(\phi)| \pmod{p},$$

where $\mathrm{Fix}(\phi)$ are the fixed points of the action. You may assume that the size of any orbit divides $|G|$; this is immediate by the orbit-stabilizer theorem.

Proof. □

(d) By considering the action of G on $\{gHg^{-1} | g \in G\}$ by conjugation, and using Part (c), show that the inequality from Part (b) is always strict for proper subgroups of a p-group.

Proof. □

Summer 2021

1. Let V be a finite dimensional complex inner product space. For a linear map T on V, let $K(T)$ be the kernel of T and let $R(T)$ be the range of T.

   (a) Let $A, B : V \to V$ be two self-adjoint maps with orthogonal ranges. Show that $AB = BA = O$, the zero map on V.

   Proof. □

   (b) Let $A, B : V \to V$ be two self-adjoint maps with orthogonal ranges such that $K(A) \cap K(B) = \{0\}$. Prove that $K(A) = R(B)$ and $K(B) = R(A)$.

   Proof. □

   (c) points) Let $A, B : V \to V$ be orthogonal projections with orthogonal ranges such that $K(A) \cap K(B) = \{0\}$. Prove that $A + B = I$, where I is the identity map on V.

   Proof. □

   (d) Let $T = A - B$, where A and B are maps as in (c). Show that T is unitary and self-adjoint.

   Proof. □

   (e) Let $S : V \to V$ be both unitary and self-adjoint. Prove that S is a difference of two orthogonal projections with orthogonal ranges.

   Proof. □

2. Suppose that $A, B \in M_{10}(\mathbb{C})$ are two matrices such that $\text{rank}(A) = 7$, $\text{rank}(A^2) = 4$, $\text{rank}(A^3) = 2$, $A^4 = 0$, B is invertible, and $AB = BA$.

   (a) Find the Jordan normal form of A.

   Proof. □

   (b) Find the minimal and the characteristic polynomials of AB.

   Proof. □

   (c) Prove that $I - A$ is invertible and express it as a polynomial of A.

   Proof. □

3. Let V be a finite dimensional complex vector space. Let $A, B \in \text{Hom}_{\mathbb{C}}(V, V)$ such that $AB = BA$ and let $f_1, f_2 \in V^*$.

(a) Let $g : V \to \mathbb{C}$ be defined by $g(v) = f_1(v)f_2(v)$. Prove that if $g \in V^*$ then at least one of f_1 and f_2 is the zero functional.

Proof. □

(b) Prove that each eigenspace of A is invariant under B.

Proof. □

(c) Prove that A and B have at least one common eigenvector.

Proof. □

(d) Prove that if A^2 has eigenvalue λ^2 then λ or $-\lambda$ is an eigenvalue for A.

Proof. □

4. In this problem, we will let G be a group of order 112.

(a) Find all possibilities for the number of Sylow p-subgroups of G for every relevant prime p.

Proof. Calculate $112 = 2^4 \cdot 7$. By Sylow theorems, $n_2 = 1,\ 7$ and $n_7 = 1,\ 8$. □

(b) If we suppose that G is simple, how many Sylow p-subgroups does G have for each relevant prime p?

Proof. G simple $\Rightarrow n_2 = 7$ and $n_7 = 8$. □

(c) Show that if G is simple, then there is a nontrivial homomorphism $\phi : G \to S_7$ (the symmetric group on 7 letters).

Proof. Cayley's theorem give a hom into S_{112}, but this is too large.
Fix elements of order 2^n for all n, and permute the elements in the 7-subgroup. This will form a non-trivial hom into S_7. □

(d) Show that if G is simple, then G is isomorphic to a subgroup of A_7.

Proof. Assume we have a non-trivial hom into S_7. A non-trivial normal subgroup of S_7 is A_7. Since G is simple, it must actually be isomorphic to some subgroup contained in A_7. □

(e) Conclude there is no simple group of order 112.

Proof. □

5. In this problem, let R be a commutative ring with identity, $\{P_i\}_{i\in\Lambda}$ the set of prime ideals of R, and $\{M_j\}_{j\in\Gamma}$ the set of maximal ideals of R. For this problem you may use the fact that if S is a multiplicatively closed subset of R, and I is an ideal with the property that $I \bigcap S = \emptyset$, then there is a prime ideal P such that $P \bigcap S = \emptyset$.

(a) Show that an arbitrary intersection of prime ideals is a radical ideal.

Proof. Let P and Q be prime ideals, with $K = P \cap Q$. For $r^n \in K$, then $r^n \in P$, thus $r \in P$ or $r^{n-1} \in P$. If it's the first, K is radical. If it's the second, then $r^{n-1} \in K$, so repeat this process until just r is left. □

(b) Show that

$$N = \bigcap_{i \in \Lambda} P_i$$

where N denotes the set of nilpotent elements of R.

Proof. Let $n \in N$. This intersection is radical, so $n^m = 0 \in P_i$, thus $n \in P_i$. Therefore $N \subset \bigcap_{i \in \Lambda} P_i$.

For contrapositive, suppose $n \notin N$. Form the multiplicatively closed subset $S = \{e, n, n^2, ...\}$. If there exists an ideal I (let $I = \{0\}$) such that $I \bigcap S = \emptyset$, then there exists P such that $P \bigcap S = \emptyset$. That is, $n \notin P$, so by contrapositive $P \subseteq N$. □

(c) Use the previous (if you like) to show that if $I \subset R$ is an ideal, then

$$\sqrt{I} = \bigcap_{I \subseteq P} P$$

where the intersection is taken over the set of prime ideals that contain I.

Proof. Let $r \in \sqrt{I}$. Then $r^n \in I$ for some n, so $r^n \in \bigcap P$. Since this intersection is radical, $r \in \bigcap P$.

Like above, suppose for contradiction that $r \notin \sqrt{I}$. Then there exists P such that $P \bigcap S = \emptyset$. That is, $r \notin P$ □

(d) Show that if $J := \bigcap_{j \in \Gamma} M_j$ then $x \in J$ if and only if $1 + rx$ is a unit for all $r \in R$.

Proof. Maximal ⇒ prime, so J is nilpotent. By (e), thus $1 + rx$ is a unit.

From Burr's HW #9, an ideal M is maximal iff for all $r \in R/M$ there exists an x such that $1 + rx \in M$. **INCOMPLETE** □

(e) Show that if x is a nilpotent element of R then $1 + rx$ is a unit for all $r \in R$.

Proof. It is easier to see that $1 - rx$ is nilpotent: suppose that $x^n = 0$ and expand

$$(1 - rx)(1 + rx + (rx)^2 + ... + (rn)^{n-1}).$$

□

6. For this problem, we will let $\mathbb{F}$ be a field, $\mathbb{R}$ and $\mathbb{C}$ the real and complex numbers respectively, and $\mathbb{Z}$ the integers. We will let $f(x)$ be a polynomial in $\mathbb{F}[x]$ such that $\deg(f(x)) \geq 1$.

(a) Find (and prove) necessary and sufficient conditions on the polynomial $f(x)$ for the quotient ring $\mathbb{F}[x]/(f(x))$ to be a field.

Proof. □

(b) Show that $\mathbb{F}[x]/(f(x))$ is a field if and only if $\mathbb{F}[x]/(f(x))$ is an integral domain.

Proof. □

(c) Show that if $f(x)$ is a product of *distinct* irreducible polynomials in $\mathbb{F}[x]$ then $\mathbb{F}[x]/(f(x))$ is a finite direct product of fields.

Proof. □

(d) In the case that $\mathbb{R} = \mathbb{R}$ and $f(x)$ is a product of distinct irreducibles in $\mathbb{R}[x]$, show that $\mathbb{F}[x]/(f(x))$ is isomorphic to a finite direct product of fields each of which is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.

Proof. □

(e) If we now let $f(x) \in \mathbb{Z}[x]$ (still of degree at least 1), show that $\mathbb{Z}[x]/(f(x))$ is *never* a field.

Proof. □

Winter 2022

1. Let $A : X \to X$ be a linear map of an n-dimensional vector space over $\mathbb{C}$.

   (a) Take any $v \neq 0$ in X and consider the set $v, Av, A^2v, ..., A^nv$, which must be linearly dependent. Use this to show that A must have an eigenvector and eigenvalue pair.

   Proof. □

   (b) Let λ be an eigenvalue of A, and for each $j \in \mathbb{N}$, let N_j be the nullspace of $(A - \lambda I)^j$. Show that $A - \lambda I$ extends to a well-defined map $N_{j+1}/N_j \to N_j/N_{j-1}$ that is injective.

   Proof. □

   (c) Give an example of a linear map on a 5-dimensional vector space for which $N_5 \supsetneq N_4$ holds for some eigenvalue λ. Writing your answer in matrix form is sufficient.

   Proof. □

   (d) A linear map is *nilpotent* if $A^k = 0$ for some $k \in \mathbb{N}$. Suppose that A is a nilpotent map on a 4-dimensional vector space. Find all eigenvalues λ, and for each one, list all possible sequences $(d_1, d_2, ...)$, where $d_j = dim(N_j)$.

   Proof. □

   (e) A linear map is *idempotent* if $A^2 = A$. Suppose that A is an idempotent map on a 4-dimensional vector space. Find all possible eigenvalues λ, and for each one, list all possible sequences $(d_1, d_2, ...)$, where $d_j = dim(N_j)$.

   Proof. □

2. Let $\mathbb{F}$ be a field and V a vector space over $\mathbb{F}$ of dimension n. Let $\phi : V \to V$ be an $\mathbb{F}$-linear map. For any polynomial $g(x) \in \mathbb{F}[x]$, define

$$V(g) = \{v \in V : g(\phi)(v) = 0\}.$$

   (a) Show that $V(g)$ is a subspace of V and that it is ϕ-invariant.

   Proof. □

   (b) Suppose $g(x), h(x) \in \mathbb{F}[x]$ satisfy $\gcd(g(x), h(x)) = 1$. Show that $V(gh) = V(g) \oplus V(h)$.

   Proof. □

(c) Suppose $g(x) \in \mathbb{F}[x]$ is a polynomial of degree m and $t \geq 1$ is an integer. Give an example of V with dimension $n = mt$ and a linear map ϕ so that $V(g^2) = V$ but $V(g) \neq V$.

Proof. □

(d) Suppose $g(x) \in \mathbb{F}[x]$ is irreducible of degree m and $t \geq 1$ is an integer. Give an example of V with dimension $n = mt$ and a linear map ϕ so that has characteristic polynomial $g(x)^t$ and minimal polynomial $g(x)$. In your example with $m > 1$, explain why ϕ has no eigenvector in V.

Proof. □

3. Let V be a finite-dimensional inner product space over $\mathbb{C}$.

(a) Prove that for a linear map $T : V \to V$ we have that for all $x, y \in V$

$$\langle Tx, y\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \langle T(x + i^k y), x + i^k y\rangle$$

and use this to show that if $\langle Tv, v\rangle \in \mathbb{R}$ for every $v \in V$, then T is self-adjoint.

Proof. □

(b) A linear map $T : V \to V$ is a contraction if $||Tv|| \leq ||v||$ for every $v \in V$. Prove that T is a contraction if and only if $I - T^*T$ is nonnegative (i.e. positive semidefinite).

Proof. □

(c) Prove that if $T : V \to V$ is a contraction then there exists a positive semidefinite map $S : V \to V$ such that $S^2 = I - T^*T$.

Proof. □

(d) A linear map $U : X \to X$ on a complex inner product space X is unitary if $UU^* = I$ and $U^*U = I$. Let T and S be as in part (c). Prove that if S is the zero map then T is unitary. (This is not true if V is infinite- dimensional, so make sure you emphasize where you have used that V is finite-dimensional.)

Proof. □

(e) Let T and S be as in part (c). Consider the direct product $V \times V = \{(x, y) : x, y \in V\}$ where the addition and multiplication by scalars are defined componentwise, equipped with the inner product

$$\langle (x_1, y_1), (x_2, y_2)\rangle_{V\times V} = \langle x_1, x_2\rangle_V \langle y_1, y_2\rangle_V$$

Prove that $L : V \to V \times V$ defined by $Lv = (Tv, Sv)$ is an isometry.

Proof. □

4. For this problem, R will be a commutative ring with identity, $\mathbb{F}$ will be a field, $\mathbb{Z}$ will be the (ordinary) integers, and $\mathbb{Z}_p$ will denote the integers modulo p. Also recall that a polynomial is said to be *monic* if its leading coefficient is 1.

   (a) Show that if R is a PID (principal ideal domain) then any nonzero prime ideal of R is a maximal ideal of R.

   Proof. □

   (b) Show that there is a one-to-one correspondence between maximal ideals of $\mathbb{F}[x]$ and monic irreducible polynomials in $\mathbb{F}[x]$.

   Proof. □

   (c) Show that if $M \subsetneq \mathbb{Z}[x]$ is a maximal ideal, then $M \bigcap \mathbb{Z} = (p)$ where p is some nonzero prime integer.

   Proof. □

   (d) Now let $0 \neq p \in \mathbb{Z}$ be a fixed prime. Show that there is a one-to- one correspondence between maximal ideals of $\mathbb{Z}[x]$ that contain p and monic irreducible polynomials in $\mathbb{Z}_p[x]$.

   Proof. □

   (e) Characterize all maximal ideals of $\mathbb{Z}[x]$.

   Proof. □

5. Let G be a finite group and H an Abelian subgroup. Recall that the centralizer $C(g)$ of $g \in G$ is the set of all elements of G which commute with g, the center $Z(G)$ is the set of all elements of g that commute with all elements in G, and the conjugacy class $\mathcal{O}(g)$ of an element $g \in G$ is the set of all conjugates of g in G. In the following questions, even if you skip a part, you may use the results of it throughout the remainder of the problem without proof.

   (a) Compute the number of conjugacy classes of G as follows:

      (i) Prove that $|G|/|C(g)|$ is equal to the size of the conjugacy class of g.

      Proof. □

      (ii) Prove that $\frac{1}{|G|}\sum_{g \in G} |C(g)|$ is the number of conjugacy classes of G.

      Proof. □

   (b) Compute a lower bound on the number of conjugacy classes of G as follows:

      (i) Prove that for any $h \in H$, $|C(h)| \geq |H|$.

Proof. □

(ii) Prove that the number of conjugacy classes of G is at least $\frac{|H|^2}{|G|}$.

Proof. □

(c) Suppose that G is not Abelian, then

(i) Prove that $G/Z(G)$ cannot be cyclic.

Proof. □

(ii) Using Part *i.*, prove that $|G| \geq 4|Z(G)|$.

Proof. □

(iii) Prove that for $g \notin Z(G)$, $|\mathcal{O}(g)| \geq 2$.

Proof. □

(iv) Let $k(G)$ be the number of conjugacy classes in G and observe (you do not need to prove) that $k(G) - |Z(G)|$ is the number of nontrivial conjugacy classes. Use the class equation to prove that

$$|G| \geq |Z(G)| + 2(k(G) - |Z(G)|)$$

Proof. □

(v) Using the previous parts, conclude that $\frac{5}{8}|G| \geq k(G)$.

Proof. □

6. Let G be a group and $H \leq G$. Throughout this problem, you may use the result of a previous part, even if you could not prove it.

(a) Give a direct proof (i.e., w/o appealing to Part (b)), that if $[G : H] = 2$, then $H \trianglelefteq G$.

Proof. □

(b) Show that if $[G : H] = p$, where p is the smallest prime dividing $|G|$, then G cannot be simple.

Proof. □

(c) Show that if G has a nontrivial proper subgroup H of index $[G : H] < 5$, then G cannot be simple.

Proof. □

(d) Now, let G be a group of order 90.

(i) Suppose that G has a nonnormal Sylow 5-subgroup. Show that there is a nontrivial homomorphism $\phi : G \to S_6$.

Proof. □

(ii) If $\phi(G)$ is contained in A_6, show that ϕ is not injective.

Proof. □

(iii) Show that G cannot be simple.

Proof. □

Summer 2022

1. Let X be a finite-dimensional $\mathbb{C}$-vector space. A linear map $P : X \to X$ is a *projection* (not necessarily orthogonal) if $P^2 = P$.

   (a) Show that if P is a projection, then there are complementary subspaces Y and Z such that

   $$X = Y \oplus Z, \quad Py = y, \text{ for all } y \in Y, \quad \text{and} \quad Pz = 0, \text{ for all } z \in Z.$$

   Proof. Write $x = (x - Px) + Px$. It's then apparent that $Y = \text{Kern}(P)$ and $Z = \text{Ran}(P)$ is the correct choice. To show $x - Px \in Y$, note $P(x - Px) = Px - Px = 0$. For $Y \cap Z = \{0\}$, let x be in both. As $x \in Z$, there exists a z such that $x = Pz$. Then
   $$x = Pz = P(Pz)) = Px = 0.$$
   □

   (b) Show that $Q := I - P$ is also a projection. Find its image and nullspace.

   Proof.
   $$Q^2 = (I - P)^2 = I - 2P - P^2 = I - P = Q.$$
   It is straightforward to verify: $\text{Ran}(Q) = \text{Kern}(P)$ and $\text{Kern}(Q) = \text{Ran}(P)$. □

   (c) Show that in matrix form, P is similar to the block matrix $M = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$.

   Proof. Since $P^2 = P$, taking determinants of both sides shows that P has eigenvalues only 0 or 1. The dimension of the range is 1, so there will be no 1's on the superdiagonal of the Jordan block. □

   (d) Show that the dimension of the image of P is equal to its trace.

   Proof. From (c) we know $P = UMU^{-1}$. Using (cyclic) commutativity of trace, $\text{tr}(P)$ is equal to the multiplicity of 1 as an eigenvalue which is equal to $\dim(\text{Im}(P))$.
   □

   (e) If X is an inner product space, show that Y and Z are orthogonal if and only if $P = P^*$, where $P^* : X \to X$ is the *adjoint* of P.

   Proof. ($\Rightarrow$) Suppose that Y and Z are orthogonal. We know that $\langle Px, w\rangle = \langle x, P^*w\rangle$. Let $x = y_1 + z_1$ and $w = y_2 + z_2$.

   $$\langle P(y_1 + z_1), y_2 + z_2\rangle = \langle y_1, y_2 + z_2\rangle = \langle y_1, y_2\rangle + \langle y_1, z_2\rangle = \langle y_1, y_2\rangle.$$

   Similarly, the same computation reveals $\langle y_1 + z_1, P(y_2 + z_2)\rangle = \langle y_1, y_2\rangle$. Thus $\langle x, P^*w\rangle = \langle Px, w\rangle = \langle x, Pw\rangle$, so $P = P^*$.
   ($\Leftarrow$) Suppose $P = P^*$. Then $\langle y, z\rangle = \langle Py, z\rangle = \langle y, Pz\rangle = 0$. □

(f) Show that if $P = P^*$, then $||x||^2 = ||Px||^2 = ||Qx||^2$ for all $x \in X$.

Proof. $||Px||^2 = \langle Px, Px\rangle = \langle x, Px\rangle$, so $||x||^2 - ||Px||^2 = \langle x, x - Px\rangle = 0$. Similarly with $Q = I - P$. □

2. Let $S \in \mathbb{R}^{n\times n}$ and define the linear mapping $T : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ by $T(P) = PS + SP$.

(a) Let λ be an eigenvalue of S and let u be its corresponding eigenvector such that $u \in \text{Null}(T(P))$ and $Pu \neq 0$.

(i) Show that Pu is an eigenvector of S.

Proof. $0 = T(P)(u) = PSu + SPu = \lambda Pu + S(Pu)$. Thus $S(Pu) = -\lambda(Pu)$. □

(ii) What is the corresponding eigenvalue of the eigenvector Pu?

Proof. $-\lambda$ □

(b) Prove that if S is symmetric and positive definite, then T is injective.

Proof. □

(c) Show that if S is symmetric and positive definite, then every $A \in \mathbb{R}^{n\times n}$ can be written as $A = PS + SP$ for some $P \in \mathbb{R}^{n\times n}$.

Proof. As this is a finite-dimensional vector space (see 3a below) T injective implies T surjective. Thus for every A, there exists a P s.t. $A = T(P) = PS + SP$. □

3. Let $\phi : V \to V$ be a linear map on a vector space V over a field $\mathbb{F}$.

(a) Suppose V is finite dimensional. Show that ϕ is surjective (onto) iff it is injective.

Proof. Let $\phi : V \to W$. Recall that ϕ surjective iff $\text{Ran}(\phi) = W$, and ϕ injective iff $\text{Kern}(\phi) = \{0\}$. By the Fundamental Theorem of Linear Algebra, $\dim(V) = \dim \text{Kern}(\phi) + \dim \text{Ran}(\phi)$. Thus if $\dim(V) = \dim(W)$, we have that ϕ is surjective iff ϕ is injective. Since $W = V$ here, the result follows. □

(b) Suppose V is infinite dimensional. Give an example where ϕ is surjective but not injective, and an example where ϕ is injective but not surjective.

Proof. The right-shit operator S s.t. $S(x_1, x_2, x_3, ...) = (0, x_1, x_2, ...)$ is clearly injective, but cannot be surjective. On the other hand, the left-shift operator T s.t. $T(x_1, x_2, x_3, ...) = (x_2, x_3, x_4, ...)$ is clearly surjective, but is not injective. □

(c) A subspace S of V is called ϕ-invariant if $\phi(s) \in S$ for each $s \in S$.

(i) Show that ϕ has an eigenvalue $\lambda \in \mathbb{F}$ iff V has a ϕ-invariant subspace of dimension 1.

Proof. ($\Rightarrow$) Let $\phi(x) = \lambda x$. Then for any $s \in \text{Span}(x)$, we have that $\phi(s)$ is a multiple of s, thus still inside the span.
($\Leftarrow$) □

(ii) Construct an example where ϕ has no eigenvalue in $\mathbb{F}$ and V is the direct sum of two nontrivial ϕ-invariant subspaces.

Proof. □

4. In the following questions, either provide an example or prove the requested statement. Make sure to explain why your example satisfies the given conditions.

(a) In the following questions, suppose that G is a group, H a normal subgroup of G, and K a normal subgroup of H.

(i) Find an example of groups G, H, and K so that K is not normal in G.

Proof. Let $G = D_8 = \langle r, s \,|\, r^4 = s^2 = e, srs = r^3 \rangle$. Take $H = \langle r^2, s \rangle$ and $K = \langle s \rangle$. By looking at the subgroup diagram (Macauley loves these) or computing the order, we see that $K \lhd H$ and $H \lhd G$. However, K is not normal in G, which is easily verified. □

(ii) Prove that if H is cyclic, then K is normal in G.

Proof. Let $H = \langle x \rangle \lhd G$. Then any $K \subseteq H$ is of the form $\langle x^n \rangle$. So for any $g \in G$, since $H \lhd G$, we get that $g^{-1}x^k g$ is still in H, say it equals x^m. Thus

$$g^{-1}(x^n)^k g = (g^{-1}x^k g)^n = (x^m)^n = (x^n)^m \in K.$$

Therefore $K \lhd G$. □

(b) In the following questions, suppose that R and S are rings, I is an ideal of R, and $\varphi : R \to S$ is a ring homomorphism.

(i) Find an example of rings R and S and ideal I where the image $\varphi(I)$ of I is not an ideal of S.

Proof. Consider the inclusion map $\iota : \mathbb{Z} \to \mathbb{Q}$. Of course, $\mathbb{Z}$ is an ideal of itself, but not $\mathbb{Q}$ since $2 \in \mathbb{Z}$ times $\frac{1}{3} \in \mathbb{Q}$ is not in $\mathbb{Z}$.
In fact, many inclusion maps give the same type of counterexample: for $\phi : \mathbb{Z} \to \mathbb{Z}[x]$, the ideal $2\mathbb{Z}$ maps to a non-ideal. □

(ii) Prove that if φ is surjective, then the image $\varphi(I)$ of I is an ideal of S.

Proof. Suppose φ is surjective. Trivially, $\varphi(0) \in \varphi(I)$. Let $x, y \in \varphi(I)$ s.t. $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in I$. Then

$$x - y = \varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(I).$$

By surjectivity, for any $s \in S$ there exists some $r \in R$ s.t. $s = \varphi(r)$. Then

$$sx = \varphi(r)\varphi(a) = \varphi(ar) \in \varphi(I).$$

Likewise, $xs \in \varphi(I)$, hence $\varphi(I)$ is an ideal of S. □

(iii) Suppose that I is a prime ideal and φ is surjective. Prove that if $\text{Kern}(\varphi) \subseteq I$, then the image of I is a prime ideal of S.

Proof. □

5. For this problem, R will be a commutative ring with identity. We say that a (proper) ideal $I \subset R$ is *primary* if whenever $ab \in I$ and $a \notin I$ then $b^n \in I$ for some $n \in \mathbb{N}$. Additionally, if $I \subseteq R$ is an ideal, we recall that the *radical* of I is $\sqrt{I} = \{x \in R | x^n \in I \text{ for some } n \in \mathbb{N}\}$. If $I = \sqrt{I}$, we say that I is a radical ideal.

(a) Show that the ideal I is prime if and only if it is both primary and radical.

Proof. ($\Rightarrow$) Clearly, a prime ideal is primary. Also, it's easy to see that for a prime idea I, we have $I \subseteq \sqrt{I}$. To see the opposite inclusion, let $a \in \sqrt{I}$ implying that $a^k \in I$ for some k. Then either $a \in I$ or $a^{k-1} \in I$. If $a \in I$, we're done. If $a^{k-1} \in I$, the either $a \in I$ or $a^{k-2} \in I$...
Continuing this, we get that $a \in I$, hence $I = \sqrt{I}$.
($\Leftarrow$)

□

(b) Characterize the radical of a primary ideal.

Proof. Let P be a primary ideal. Suppose $ab \in \sqrt{P}$, implying there exists an k s.t. $a^k \cdot b^k = (ab)^k \in P$. As P is primary, thus either $a^k \in P$ or $(b^k)^n \in P$ for some n. By definition of a radical ideal, thus either a or b is in $\sqrt{P}$, thus $\sqrt{P}$ is a prime ideal. □

(c) Suppose that R is a PID. Characterize the nonzero primary ideals.

Proof. □

(d) Show that I is primary if and only if all zero-divisors in R/I are nilpotent.

Proof. □

(e) Give an example to show that, in general, there are primary ideals which are not prime powers.

Proof. A classic example is $\mathbb{F}[x, y]$, with the ideal $I = (x, y^2)$. Then I is a primary ideal, but not a power of (x, y) - thus is not a power of a prime ideal (even in a Noetherian ring).

Remark: A classic converse is $\mathbb{Z}[x]$ s.t. the coefficient on x is divisible by 3. Then $J = (3x, x^2, x^3)$ is a prime ideal, but J^2 is not primary. So this shows powers of a prime ideal may not be primary.

□

6. For this problem, let G be a finite group of order $132 = 2^2 \cdot 3 \cdot 11$.

(a) For each prime, p, dividing the order of G, enumerate the possibilities for the number of Sylow p-subgroups of G.

Proof. □

(b) Show that G cannot be simple.

Proof. □

(c) Let P be a Sylow 11-subgroup of G. show that if P is not normal in G, then $N_G(P) = P$.

Proof. □

(d) Use the previous part to show that if P is not normal in G then all elements of G that are not contained in some Sylow 11-subgroup of G must be conjugate.

Proof. □

(e) Show that G has a unique (normal) Sylow 11-subgroup.

Proof. □

Winter 2023

1. (a) Let $A, B \in \mathbb{C}^{n\times n}$ be Hermitian matrices. Prove that the eigenvalues of $(A + B)$ are real.

   Proof. □

   (b) Let $A, B \in \mathbb{R}^{n\times n}$ be symmetric matrices. State and prove a sufficient condition about the matrices A, B in order to conclude that AB has only real eigenvalues

   Proof. □

   (c) Let $A \in \mathbb{C}^{n\times n}$ be an arbitrary matrix. Prove that if $\langle Ax, x\rangle = 0$ for all $x \in \mathbb{C}^n$, then $A = 0$.

   Proof. □

   (d) Let $A \in \mathbb{R}^{n\times n}$ be an arbitrary matrix. Prove or disprove: if $\langle Ax, x\rangle = 0$ for all $x \in \mathbb{R}^n$, then $A = 0$.

   Proof. □

2. (a) Let $T : V \to V$ be a linear operator. Suppose $v_1, ..., v_n$ are non-zero vectors in V such that $T(v_1) = 0$ and $T(v_i) = v_{i-1}$ for $2 \leq i \leq n$. Prove that $\{v_1, ..., v_n\}$ is a linearly independent set.

   Proof. □

   (b) Let $B = \{u_1, ..., u_n\}$ be a basis of a vector space V. Let $C = \{v_1, ..., v_m\}$ be a linearly independent set in V. Prove that there is an integer k, $1 \leq k \leq n$, such that vectors $u_k, v_2, ..., v_m$ are linearly independent.

   Proof. □

   (c) Let V be the vector space of all polynomial functions from $\mathbb{R}$ to $\mathbb{R}$ which have degree less than or equal to $n - 1$. Let $t_1, ..., t_n$ be any n distinct real numbers, and define linear functionals $L_i(p) = p(t_i)$ on V. Show that $L_1, ..., L_n$ are linearly independent.

   Proof. □

3. Let $\mathbb{F}$ be a field and V a vector space over $\mathbb{F}$ of dimension n. Let $\phi : V \to V$ be an $\mathbb{F}$-linear map. For any polynomial $g(x) \in \mathbb{F}[x]$, define

$$B(g) = \{v \in V : g(\phi)(v) = 0\}.$$

   Note that $B(g)$ is a subspace of V.

   (a) For any $g(x) \in \mathbb{F}[x]$, prove that $B(g)$ is ϕ-invariant.

Proof. □

(b) Let $g(x) \in \mathbb{F}[x]$ be the minimal polynomial of ϕ. Suppose $g = g_1(x)g_2(x)...g_t(x)$ where $g_1(x), ..., g_t(x) \in \mathbb{F}[x]$ are pairwise relatively prime. Prove that

$$V = B(g_1) \oplus ... \oplus B(g_t),$$

that is, for every $v \in V$, there exist unique $v_1 \in B(g_1), ..., v_t \in B(g_t)$ so that $v = v_1 + ... + v_t$.

Proof. □

(c) Suppose $g(x) \in \mathbb{F}[x]$ is irreducible of degree m and $t \geq 1$ is an integer. Give an example of V with dimension $n = mt$ and a linear map ϕ so that ϕ has characteristic polynomial $g(x)^t$ and minimal polynomial $g(x)$. In your example with $m > 1$, explain why ϕ has no eigenvector in V.

Proof. □

4. Let G be a group of order $n = 2km$ where m is odd and $k \geq 1$. Suppose that $G = g_1, ..., g_n$. If you do not know how to do one part, you may earn points on subsequent parts by assuming the previous results.

(a) Define a map $\phi : G \to S_n$ where $h \mapsto \pi_h$ with the property that $g_{\pi_h(i)} = hg_i$. Prove that ϕ is an injective homomorphism.

Proof. □

(b) Prove that $\pi_h^t(i) = i$ for some i if and only if $|h|$ divides t. Here, π_h^t denotes applying π_h t-many times. From this, conclude that π_h is a product of cycles of length $|h|$.

Proof. □

(c) Prove that the sign of the permutation π_h is $(-1)^{\frac{|G|}{|h|}}$.

Proof. □

(d) Prove that π_h is an odd permutation if and only if 2^k divides $|h|$. Conclude that $\phi(G)$ has an odd permutation if and only if G has an element whose order is divisible by 2^k.

Proof. □

(e) Suppose that G has an element whose order is divisible by 2^k. Prove that $\phi(G)A_n = S_n$. Conclude that $\phi(G) \cap A_n$ has index 2 in $\phi(G)$, and, hence, that G is not simple.

Proof. □

5. Given a group G, let $\mathrm{Aut}(G)$ be its automorphism group

   (a) For some fixed $g \in G$, define the function

   $$\varphi_g : G \to G, \quad \varphi_g : x \mapsto g^{-1}xg.$$

   Show that φ_g is an automorphism.

   Proof. □

   (b) Automorphisms of the form φ_g, as defined in Part (a), are called inner automorphisms. Let

   $$\mathrm{Inn}(G) = \{\varphi_g | g \in G\}$$

   be the set of inner automorphisms. Show that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ and that it is normal.

   Proof. □

   (c) Show that the map $G \to \mathrm{Inn}(G)$ defined by $g \mapsto \varphi_g$ is a homomorphism.

   Proof. □

   (d) Show that $\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$, where $\mathrm{Z}(G)$ is the center of G.

   Proof. □

   (e) Prove that if $G/\mathrm{Z}(G)$ is cyclic, then G is abelian.

   Proof. □

   (f) Show that $\mathrm{Inn}(G)$ cannot be a nontrivial cyclic group.

   Proof. □

6. In this problem, you will prove the four isomorphism theorems for rings. Rings are additive abelian groups, and you can and should assume all results from group theory, such as the group isomorphism theorems, and the specific homomorphism(s) used to prove them, which will be described below. A key aspect of this problem is recognizing and understanding what you have to prove; none of the individual parts should be long.

   (a) Show that the kernel of a ring homomorphism is a 2-sided ideal.

   Proof. □

(b) The *fundamental homomorphism theorem* (FHT) says that if $\phi : R \to S$ is a ring homomorphism, then $R/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$. The proof of this for groups involves constructing a map

$$\iota : R/I \to \mathrm{Im}(\phi), \quad \iota(r + I) = \phi(r),$$

where $I = \mathrm{Ker}(\phi)$, and showing that it is a well-defined group isomorphism. Carry out the remaining details to prove the ring-theoretic version of the FHT.

Proof. □

(c) By the *correspondence theorem*, every subgroup of R/I has the form S/I for some subgroup S satisfying $I \leq S \leq R$.

i Show that S/I is a subring of R/I if and only if S is an subring of R.

Proof. □

ii Show that $J/I$is an ideal of R/I if and only if J is an ideal of R.

Proof. □

(d) The *fraction theorem* says that $(R/I)/(J/I) \cong R/J$. The proof of this theorem for groups involves showing that the following map

$$\phi : R/I \to R/J, \quad \phi(r + I) = r + J$$

is a group homomorphism with $\mathrm{Ker}(\phi) = J/I$. Carry out the remaining details to establish the ring-theoretic version of this theorem.

Proof. □

(e) The *diamond theorem* says that $(S + I)/I \cong S/(S \cap I)$ for a subring S and ideal I.

i Show that the subgroup $S \cap I$ of S is also an ideal.

Proof. □

ii In proving the diamond theorem for groups, the map

$$\phi : S \to (S + I)/I, \quad \phi(s) = s + I$$

is shown to be a group homomorphism with $\mathrm{Ker}(\phi) = S \cap I$. Carry out the remaining details to prove the ring-theoretic version.

Proof. □