1. Let
\[ A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{bmatrix}. \]

(i) Find the eigenvectors of \( A \).

(ii) Find \( A^{100} \).

Remark: When writing down the entries of \( A^{100} \) use exponential notation, e.g., \( 2^{100} + 3^{100} \), or similar.

2. Let \( A \) be an \( n \times n \)-matrix. Show that
\[ \det(A + I) = \sum_B \det B, \]
where the sum is over all the principal minors of \( A \).

[The principal minors are the matrices \( B \) obtained from \( A \) by removing rows \( 1 \leq i_1 < \ldots < i_r \leq n \) and columns \( i_1 < \ldots < i_r \) indexed by the same numbers, where \( r \) runs through \( \{0, \ldots, n\} \), and the determinant of the "empty matrix" is 1.]

3. Let \( \phi : \mathbb{C}^7 \to \mathbb{C}^7 \) be a be a \( \mathbb{C} \)-linear endomorphism with \( \dim(\ker(\phi^3)) = 5 \) and \( \phi^7 = 0 \). What are the possible Jordan canonical forms of \( \phi \)?

4. Let \( V \) be a finite-dimensional vector space over a field \( k \), and let \( U \subsetneq V \) be a proper subspace. Suppose \( \phi : V \to V \) is an endomorphism of \( V \) which has the following properties:
   - \( \phi|_U = 0 \), i.e., \( U \subset \ker(\phi) \);
   - the induced map \( \overline{\phi} : V/U \to V/U \), defined by \( \overline{\phi}(v + U) := \phi(v) + U \), is the zero map.

(i) Show that \( \phi^2 = \phi \circ \phi \) is the zero map.

(ii) Is \( \phi \) necessarily zero too? If so, give a proof, if not, give a counterexample.
5. Let $G$ be a subgroup of $S_6$, the symmetric group on 6 elements. Suppose $G$ contains a 6-cycle. Prove that $G$ has a normal subgroup $H$ of index 2.

[Hint: You may use the sign homomorphism.]

6. (i) Let $G$ be a finite group. Show that the size (i.e., cardinality) of every conjugacy class in $G$ divides the order of $G$.

(ii) Use (i) to determine all finite groups $G$ such that $G$ has exactly two conjugacy classes.

7. Determine if the following assertions are true or false. Justify why or give a counterexample.

(i) Every subgroup of index 3 in a group is normal.

(ii) Every group is isomorphic to a subgroup of a symmetric group.

(iii) If a homomorphism $\phi : G \rightarrow H$ is onto then there is a subgroup $K$ of $G$ with $H \cong K$.

(iv) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.

8. Show that the group $R^*$ of invertible elements in the ring $R = \mathbb{Z}/105\mathbb{Z}$, is isomorphic to $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

[Recall that an element $x$ of a commutative ring $R$ is called invertible, if there is an element $y$ such that $xy = 1_R$.]

9. Let $\omega = e^{2\pi i/5}$ be a 5th root of unity. The field $L = \mathbb{Q}(\omega)$ contains $K = \mathbb{Q}(\sqrt{5})$ because $\omega + \omega^{-1} = -\frac{1+\sqrt{5}}{2}$.

(i) Find the minimal polynomial for $\omega$ over $\mathbb{Q}$. (Argue from first principles. Do not use "well-known" facts about cyclotomic polynomials.)

(ii) Find the minimal polynomial for $\omega$ over $\mathbb{Q}(\sqrt{5})$.

10. Let $P$ be a prime ideal in a commutative ring $R$ with 1. Let

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in R[x]$$

be a non-constant monic polynomial with coefficients in $R$. Suppose that all coefficients $a_1, \ldots, a_n$ are in $P$, and that $f(x) = g(x)h(x)$, for some non-constant monic polynomials $g(x), h(x) \in R[x]$. Then show that the constant term of $f(x)$ is in $P^2$, the ideal generated by all elements of the form $ab$, where $a, b \in P$. 

2
Solutions

1. (i) The eigenvalues are obviously 1, 2, 3, and corresponding eigenvectors are easily determined to be $(1, 0, 0)^T$, $(1, 1, 0)^T$, $(1, 1, 1)^T$.

(ii) Put

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

so that $P^{-1}AP = D := \text{diag}(1, 2, 3)$, hence $A = PDP^{-1}$. The inverse matrix $P^{-1}$ is

$$P^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

and we compute $A^{100} = PD^{100}P^{-1} =$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^{100} & 0 \\ 0 & 0 & 3^{100} \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2^{100} & 3^{100} \\ 0 & 2^{100} & 3^{100} \\ 0 & 0 & 3^{100} \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2^{100} - 1 & 3^{100} - 2^{100} \\ 0 & 2^{100} & 3^{100} - 2^{100} \\ 0 & 0 & 3^{100} \end{bmatrix}$$

2. Think of the first column as $(1, 0, \ldots, 0)^T + (a_{11}, \ldots, a_{n1})^T$, and apply the linearity of the determinant in the columns. For each of the resulting two determinants, use in the same fashion linearity in their second columns. Continuing this way we end up with a sum of $2^n$ determinants, each with a subset of the columns replaced by columns consisting of a single 1 on the diagonal and zeros elsewhere. Expand along these columns to get principal minors of $A$.

3. As $\phi^\ell = 0$, zero is the only eigenvalue of $\phi$ and the JCF $J$ of $\phi$ is thus a block-diagonal matrix with blocks of type

$$J_m = \begin{bmatrix} 0 & 1 & 0 & \ldots & \ldots & 0 \\ 0 & 0 & 1 & \ldots & \ldots & 0 \\ \vdots & 0 & 0 & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & 0 & 1 \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \end{bmatrix}$$
which has size $m$. The sizes of those blocks must add up to 7. The rank of $J^k_m$ is easily seen to be $\max\{m-k,0\}$. Since $\dim(\ker(\phi^3)) = 5$, we see that $\phi^3$ has rank 2, and there must thus be blocks of size $\geq 4$.

- A block of size 4 contributes a rank of 1 to $\phi^3$. Therefore, an occurrence of block size 4 implies the existence of another block of size $\geq 4$, which is impossible.

- A block of size 5 contributes a rank of 2 to $\phi^3$ — that’s what we want — and we have thus two possibilities for $J$: $J = \text{diag}(J_5, J_2)$ or $J = \text{diag}(J_5, J_1, J_1)$.

- Blocks of size $\geq 6$ cannot occur because they would contribute a rank of $\geq 3$.

4. (i) Because $\overline{\phi}$ is assumed to be the zero homomorphism, we see that $\phi(v) \in U$ for all $v \in V$. But since $U \subset \ker(\phi)$ we find $\phi(\phi(v)) = 0$.

(ii) No, $\phi$ does not need to be zero: take the endomorphism of $k^2$ associated to the Jordan block $J_2$, and let $U = ke_1$.

5. Let $g \in G$ be an element of order 6, e.g. $g = (123456)$. Then $g^3 = (14)(25)(36)$, which is an odd permutation, so $g$ is odd.

This means the homomorphism

$$\sigma: G \to \{1, -1\}$$

given by $\sigma(h) = \text{sign}(h)$ is onto. Let $K \triangleleft G$ be the kernel of $\sigma$. Then $[G : K] = |G/K| = |\{1, -1\}| = 2$. So $N$ has index 2, and is thus normal.

6. (i) If $C_g$ is the conjugacy class of $g$, then the map $G \to C_g$, $x \mapsto xgx^{-1}$, is surjective. We have $xgx^{-1} = yy^{-1} \Leftrightarrow y^{-1}x \in C_G(g)$, where $C_G(g)$ is the centralizer of $g$. The fiber of this map over $xgx^{-1}$ is thus $xC_G(g)$, and hence $|C_g| = [G : C_G(g)]$. In particular, the order of each conjugacy class divides the order of $G$.

(ii) Suppose $n = |G|$. One conjugacy class is the set $\{e\}$, the set containing only the identity element of $G$. Since there are only two conjugacy classes, the second conjugacy class has order $n - 1$, and thus $(n - 1) \mid n$. This implies $n = 2$.

7. (i) Every subgroup of index 3 in a group is normal.
False. The subgroup $N = \{(1,2), e\}$ is an index 3 subgroup of $S_3$, the symmetric group on 3 elements. But $(1,2,3)(1,2)(1,3,2) = (2,3)$ so $N$ is not normal.

(ii) Every group is isomorphic to a subgroup of a symmetric group.
True.

(iii). If a homomorphism $\varphi : G \to H$ is onto then there is a subgroup $K$ of $G$ with $H \cong K$.

This is false. $\mathbb{Z}$ is torsion free but has homomorphic image $C_2$.

(iv). $C_6 \times C_6 \cong C_4 \times C_9$.

False. Every finitely generated abelian group can be uniquely written as a product of cyclic $p$-group factors. Since $C_6 \times C_6 \cong C_2 \times C_2 \times C_3 \times C_3$, it follows that $C_6 \times C_6 \not\cong C_4 \times C_9$.

8. As a ring, $\mathbb{Z}/105$ is $\mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/7$. Each of these three rings is a field, whose group of units is cyclic; thus

$$
(\mathbb{Z}/105)^\ast = (\mathbb{Z}/3)^\ast \times (\mathbb{Z}/5)^\ast \times (\mathbb{Z}/7)^\ast = \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/6,
$$
or, in canonical form, $\mathbb{Z}/12 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

9. (i) We have $1 + \omega + \omega^2 + \omega^3 + \omega^4 = \frac{\omega^5 - 1}{\omega - 1} = 0$, and $f(T) = 1 + T + T^2 + T^3 + T^4$ has $\omega$ as a root. This means that $[L: \mathbb{Q}] \leq 4$. Since $L \subset K$, and $[K: \mathbb{Q}] = 2$, we have $[L: \mathbb{Q}] \in \{2, 4\}$. Now, $[L: \mathbb{Q}] = 2$ would imply that $L = K$, but $K \subset \mathbb{R}$, and $L$ is not contained in $\mathbb{R}$. Hence $L : \mathbb{Q} = 4$ and $f(T)$ must be the minimal polynomial.

**Grading decision to be made:** It's up to you to decide if you want to let the student use that $[K: \mathbb{Q}] = 2$ without comment, or if you want to see an argument like "$\sqrt{5}$ is not in $\mathbb{Q}$ because $T^2 - 5$ is irreducible by Eisenstein". You may want to see such an argument and award 1 point for it.

(ii) This can be done in various ways. I would start by looking at the equation $\omega + \omega^{-1} = \frac{-1 + \sqrt{5}}{4} =: c \in K$ which we gave the student. Then multiply both sides with $\omega$ so as to get $\omega^2 + 1 - c\omega = 0$, then so $g(\omega) = 0$ with $g(T) = T^2 - cT + 1$. Because $[L : K] = 2$, the polynomial $g$ must be the minimal polynomial of $\omega$ over $K$.

10. Let $S = R/P$ be the quotient ring. It is an integral domain. Denote the images in $S[x]$ of the polynomials $f, g, h \in R[x]$ by $\overline{f}, \overline{g}, \overline{h}$. Then $\overline{f} = x^n$, by our assumption on the coefficients of $f$. recall that $g$ and $h$ were assume to be monic: $g(x) = x^m + \text{lower order terms}$ and $h(x) = x^k + \text{lower order terms}$. Hence $m + k = n$. Moreover, $\overline{gh} = x^n$.

**It follows that $\overline{g}$ and $\overline{h}$ must be monomials $\overline{g} = x^m$, $\overline{h} = x^k$.**

To see this, write $\overline{g}(x) = x^m + \ldots + \overline{b_i}x^{m-i}$ and $\overline{h}(x) = x^k + \ldots + \overline{c_j}x^{k-j}$ with non-zero $\overline{b_i}, \overline{c_j} \in S$. Suppose on the contrary that $i > 0$ or $j > 0$ (or both). Then
\[
\overline{g}(x)\overline{h}(x) = x^{m+k} + \ldots + \overline{b_i c_j} x^{m-i+k-j}
\]

Since $S$ is an integral domain, $b_i c_j \neq 0$. But then $\overline{g} \overline{h}$ is not a monomial (since $m + k - i - j < m + k$). This shows that indeed $\overline{g}$ and $\overline{h}$ are both monomials.

**Grading decision to be make:** I leave it up to you if you want to see the argument explained in the previous paragraph with all the details given here.

Hence all but the leading coefficients of $g$ and $h$ are in $P$. In particular, their constant coefficients are in $P$. Thus we have $f(0) = g(0)h(0) \in P^2$. 