Proposed algebra questions

1. Let G be a group, and let H be a subgroup of G. If every prime p dividing $|H|$ is at least $[G : H]$, prove that H is a normal subgroup of G.

   Solution: It is a general fact that the action of H by left-multiplication on the set G/H of left cosets is trivial iff H is normal. The orbit of the identity coset is itself. The orbit of any non-trivial left coset does not contain the trivial coset, and therefore the size of the orbit is $m < [G : H]$. The orbit-stabilizer formula implies that m divides the order of H, so every prime p dividing m is at least $[G : H]$ by assumption. Therefore $m = 1$, so every orbit is trivial, which means that the action itself is trivial. Therefore H is normal in G.

2. Let $\{e_1, e_2, e_3, e_4\}$ be the standard basis of $\mathbf{R}^4$. Let G be the additive subgroup of $\mathbf{R}^4$ generated by the four elements

   $$e_1, e_1 + e_2, \frac{1}{2}(e_1 + e_2 + e_3 + e_4), \frac{1}{2}(e_1 + e_2 + e_3 - e_4)$$

   and let H be the subgroup of G generated by the four elements

   $$e_1 - e_2, e_2 - e_3, e_3 - e_4, e_3 + e_4.$$

   Identify the abelian group G/H as a direct sum of cyclic groups.

   Solution: Let the four generators for G be $x_1, \ldots, x_4$ and let the four generators for H be $y_1, \ldots, y_4$. The matrix of the y_i's in terms of the x_j's is

   $$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & -1 \\ 0 & -1 & 0 & 2 \\ 0 & -1 & 2 & 0 \end{pmatrix}$$

   Performing elementary row and column operations leads to the Smith Normal Form

   $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

   Therefore $G/H \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

3. Let I be the ideal $(n, x^3 + 2x + 2)$ in $\mathbf{Z}[x]$. For which n with $1 \leq n \leq 7$ is I a maximal ideal?

Solution: I is maximal if and only if the quotient ring $R = \mathbf{Z}[x]/I$, which is isomorphic to $(\mathbf{Z}/n\mathbf{Z})[x]/(x^3 + 2x + 2)$, is a field. This happens if and only if $n = p$ is prime and $x^3 + 2x + 2$ is irreducible over $\mathbf{F}_p$. So we just need to test whether $x^3 + 2x + 2$ is irreducible over $\mathbf{F}_p$ for $p = 2, 3, 5, 7$, which happens iff the cubic does not have a root in $\mathbf{F}_p$. By inspection, the polynomial has a root for $p = 2, 5, 7$ but not for $p = 3$ so the only value of n for which I is maximal is $n = 3$.

4. Let R be a commutative ring with identity.

   a. Let I, J be ideals of R, and let P be a prime ideal of R. If $IJ \subset P$, prove that either $I \subset P$ or $J \subset P$.

   b. Let A, B, I be ideals of R. If $I \subset A \cup B$, prove that either $I \subset A$ or $I \subset B$.

Solution: (a) Suppose $I \not\subset P$ and $J \not\subset P$. Then there exist $x \in I$ and $y \in J$ with $x, y \notin P$. Therefore $xy \notin P$, by the definition of a prime ideal. But $xy \in IJ$ by definition and $IJ \subset P$ by assumption, so $xy \in P$, a contradiction.

(b) Suppose $I \not\subset A$ and $I \not\subset B$. Then there exist $x, y \in I$ with $x \notin A$ and $y \notin B$. Thus $x \in B$ and $y \in A$. But also $x + y \in I$ so $x + y \in A$ or $x + y \in B$. Without loss of generality we may assume that $x + y \in A$. Then $x = (x + y) - y \in A$, a contradiction.

5. Let L/K be a field extension of degree n. Prove that L is isomorphic to a subring of the ring of $n \times n$ matrices over K.

Solution: Choose a basis $\alpha_1, \ldots, \alpha_n$ for L as a vector space over K, and define $\varphi : L \to M_n(K)$ by letting $\varphi(\alpha)$ be the matrix of multiplication by α with respect to the chosen basis. By linear algebra, φ is a homomorphism, and if $\varphi(\alpha) = \varphi(\beta)$ then $\alpha\alpha_i = \beta\alpha_i$ for all i and thus $\alpha = \beta$ (by writing 1 as a linear combination of the α_i). It follows that φ is injective. By the first isomorphism theorem, L is isomorphic to the subring $\varphi(L)$ of $M_n(K)$.

6. Let α, β be complex numbers with $\beta \in \mathbf{Q}(\alpha)$ and $\beta \notin \mathbf{Q}$. Prove that $\mathbf{Q}(\alpha)$ is an algebraic extension of $\mathbf{Q}(\beta)$.

Solution: Write $\beta = F(\alpha)/G(\alpha) \in \mathbf{Q}(\alpha)$, where F, G are polynomials in one variable over $\mathbf{Q}$ with G nonzero. Then $G(\alpha)\beta - F(\alpha) = 0$. This equation can be viewed as a non-constant polynomial in α with coefficients in $\mathbf{Q}(\beta)$. (Since $\beta \notin \mathbf{Q}$, at least one of F and G is non-constant, and therefore α actually appears in the equation.) Thus α is algebraic over $\mathbf{Q}(\beta)$, and $\mathbf{Q}(\alpha)$ is an algebraic extension of $\mathbf{Q}(\beta)$.

7. Let A be a complex $n \times n$ matrix such that the sequence $(A^n)_{n=1}^{\infty}$ converges to a matrix B. Prove that B is similar to a diagonal matrix with 0's and 1's along the main diagonal.

   Solution: Since the squaring map on $M_n(\mathbf{C})$ is continuous, we have

   $$B^2 = (\lim_{n\to\infty} A^n)^2 = \lim_{n\to\infty} A^{2n} = B.$$

   Therefore the minimal polynomial $m_B(x)$ of B divides $x^2 - x$. In particular, all eigenvalues of B are either 0 or 1 and (since $m_B(x)$ is square-free) B is diagonalizable.

   Alternate solution: Let S be an invertible matrix so that $A' = SAS^{-1}$ is in Jordan canonical form. If A^n converges to B as $n \to \infty$, then A'^n converges to $B' = SBS^{-1}$. Now note that the powers of a Jordan block with eigenvalue λ converge if and only if the block is 1×1 with $\lambda = 1$, or if $|\lambda| < 1$. (Write $J = \lambda I + N$ with N nilpotent, say $N^k = 0$, and use the fact that I and N commute to show that $J^n = \lambda^n I + \binom{n}{1}\lambda^{n-1}N + \cdots + \binom{n}{k-1}\lambda^{n-k+1}N^{k-1}$.) The corresponding limits are the 1×1 matrix (1) or a 0 block. Thus B is conjugate to B' in the desired form.