Algebra Qualifying Exam, Fall 2000

Instructions: Attempt ALL parts. Throughout, all rings are assumed to have an identity.

Part I. State each of the following theorems, including the definitions of the relevant terminology.

1. Wedderburn's structure theorem for semisimple rings.
2. Jordan-Hölder theorem for groups.
3. The structure theorem for finitely generated modules over a PID.

Part II. Determine whether each statement below is true or false. If true, give a brief explanation. If false, provide a counterexample.

1. An Artinian integral domain is a field.
2. Every algebraic extension of a finite field is finite.
3. Every short exact sequence $0 \to \mathbb{Q} \to A \to B \to 0$ of Abelian groups is split.
4. If R is a PID, its Jacobson radical $J(R)$ is zero.
5. Let $F : \mathfrak{groups} \to \mathfrak{sets}$ be the forgetful functor and $G : \mathfrak{sets} \to \mathfrak{groups}$ be the free group functor, mapping a set X to the free group on X. Then, (F, G) is an adjoint pair of functors, i.e. F is left adjoint to G.
6. If G is a finite nilpotent group and H is a proper subgroup, then $H \neq N_G(H)$.

Part III. Attempt any FOUR of the following.

1. Let p and q be primes with $p > q$ and $q \nmid (p-1)$. Show that all groups of order pq are cyclic.
2. Let V be a finite dimensional vector space over $\mathbb{Q}$, and $f : V \to V$ be a linear transformation with characteristic polynomial $(x-2)^4$.

   (a) Write down all possible Jordan normal forms of f. For each possibility, record *both* the minimal polynomial of f *and* the dimension of its 2-eigenspace.

   (b) Suppose in addition that f leaves invariant only finitely many subspaces of V. What can you say about the Jordan normal form of f now?
3. Let R be a commutative ring and I an ideal. Prove that for any R-module M, $(R/I) \otimes_R M \cong M/IM$. Hence, or otherwise, determine the structure of the Abelian group $\mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n)$.
4. Let $f(X) \in \mathbb{Q}[X]$ be a monic polynomial with distinct roots in $\mathbb{C}$. Prove that $f(X)$ is irreducible over $\mathbb{Q}$ if and only if its Galois group G_f acts transitively on the roots.
5. Let R be a commutative ring and P be a prime ideal. Let R_P denote the localization of R at P and P_P denote the unique maximal ideal of R_P. Prove that the field of fractions of R/P is isomorphic to R_P/P_P.

Solutions

Part I.

1. A left (resp. right) semisimple ring R is a ring such that ${}_RR$ (resp. R_R) is the sum of its simple R-submodules. Then: every left (resp. right) semisimple ring R is isomorphic to a finite product of matrix rings over division rings:

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

for uniquely determined $n_i \geq 1$ and division rings D_i. Conversely, any such ring is both left and right semisimple.

2. A composition series of a group G is a finite chain $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ such that each factor G_i/G_{i-1} is simple. Two composition series $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ and $\{1\} = G'_0 \lhd G'_1 \lhd \cdots \lhd G'_m = G$ are equivalent if $m = n$ and there is a permutation $w \in S_n$ such that $G_i/G_{i-1} \cong G'_{wi}/G'_{wi-1}$ for each $i = 1, \ldots, n$. Then: if G is a group possessing a composition series, then all composition series of G are equivalent.

3. Let R be a PID. A cyclic R module means an R-module C isomorphic to $R/(d)$ for some $d \in R$. The element $d \in R$ here is uniquely determined up to a unit and is called the *order* of C. Then: a finitely generated R-module M can be decomposed as

$$M = M_1 \oplus \cdots \oplus M_s$$

where M_i is a non-zero cyclic submodule of order d_i and $d_1 | \ldots | d_s$ in R. Moreover, s and the orders $d_1, \ldots, d_s$ are uniquely determined up to associates.

Part II.

1. True. Take $x \in R^*$. Then, $(x) \supseteq (x^2) \supseteq \ldots$ stabilizes, so $(x^k) = (x^{k+1})$ for some k. But then $x^k = ax^{k+1}$ for some $a \in R$, whence (as x is non-zero and R is an integral domain) $1 = ax$ and x is a unit.

2. False. For example, the algebraic closure of the finite field $\mathbb{F}_p$ is an algebraic extension, but is infinite since it contains a copy of $\mathbb{F}_{p^n}$ for each $n \geq 1$.

3. True. For, $\mathbb{Q}$ is divisible hence injective.

4. False. Consider $R = \mathbb{Z}_{(p)}$ for p prime. This is a local ring, so has a unique maximal ideal which must be the Jacobson radical. It is not a field, so $J(R) \neq 0$. But R is a PID, because $\mathbb{Z}$ is and every ideal of R is of the form $I_{(p)}$ for I an ideal in $\mathbb{Z}$.

5. False. For example, if (F, G) was an adjoint pair, let A be the trivial group $\{e\}$ and $X = \{x, y\}$ be a set with two elements. Then $\mathrm{Hom}(FA, X)$ is of order 2 and $\mathrm{Hom}(A, GX)$ is trivial as there is only one homomorphism from the trivial group to any group.

6. True. Take $i \geq 0$ such that $G^{i+1} \subseteq H$ but $G^i \not\subseteq H$. Then, $[H, G^i] \subseteq [G, G^i] = G^{i+1} \subseteq H$, so $G^i \subseteq N_G(H)$. Hence $H \neq \mathbb{N}_G(H)$.

Part III.

1. Let n_p and n_q denote the numbers of Sylow p- and q- subgroups, respectively. We have that $n_p \equiv 1(p)$ and $n_p | pq$. Hence, $n_p | q$. Since $p > q$, this implies that $n_p = 1$. Also, $n_q \equiv 1(q)$ and $n_q | p$. Since $q \nmid (p-1)$, this implies $n_q = 1$. Hence there is a unique Sylow p-subgroup P and a unique Sylow q-subgroup Q, necessarily both normal. Then, $[P, Q] \leq P \cap Q = \{1\}$, i.e. elements of P and Q commute. Take $x \in P$ of order p and $y \in Q$ of order q. Then, xy

has order dividing pq. If xy has order 1 or p, then $xy \in P$ whence $y \in P$, a contradiction. Similarly, xy cannot have order q. Hence xy has order pq, so generates all of G. Hence G is cyclic.

2. (a) The matrices are

$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

The minimal polynomials are $(X-2)^4, (X-2)^3, (X-2)^2, (X-2)^2$ and $(X-1)$. The 2-eigenspace dimensions are $1, 2, 2, 3, 4$.

(b) Suppose the 2-eigenspace contains linearly independent vectors v, w. Then the line $\langle v+cw \rangle$ is f-stable for all $c \in F$. Hence the only possibility is for the 2-eigenspace to be 1-dimensional, i.e. the first of the above cases.

3. Define a map $f : R/I \times M \to M/IM$ by $(r+I, m) \mapsto rm + IM$ (check it is well-defined!). It is balanced, so factors to $\bar{f} : R/I \otimes_R M \to M/IM$. Define a map $g : M \to R/I \otimes M$ by $m \mapsto (1+I) \otimes m$. Note every generator im of IM maps to $(1+I) \otimes im = (1+I)i \otimes m = (0+I) \otimes m = 0$, so g factors to $\bar{g} : M/IM \to R/I \otimes M$. Then, $\bar{f}$ and $\bar{g}$ are inverse to one another, so are both isomorphisms.

Hence, $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \mathbb{Z}_m/n\mathbb{Z}_m$. Now define a surjective map $\mathbb{Z} \to \mathbb{Z}_m/n\mathbb{Z}_m$ by $1 \mapsto [1] + n\mathbb{Z}_m$. Let c be a generator of the kernel, i.e. c is the least positive integer such that c is a multiple of n modulo m, i.e. c is the least positive integer that can be written as $an + bm$ for some $a, b \in \mathbb{Z}$, i.e. $c = (m, n)$. Hence, $\mathbb{Z}_m/n\mathbb{Z}_m \cong \mathbb{Z}_{(m,n)}$.

4. If G_f does not act transitively on the roots, we can partition them into two disjoint G_f-stable subsets R and S, and then $f(X) = g(X)h(X)$ where

$$g(X) = \prod_{\alpha \in R} (X - \alpha), \qquad h(X) = \prod_{\beta \in S} (X - \beta).$$

But then G_f leaves $g(X)$ and $h(X)$ invariant, so that their coefficients are in the fixed field of G_f, namely, $\mathbb{Q}$. This contradicts the irreducibilty of $f(X)$ over $\mathbb{Q}$.

Conversely, suppose $f(X)$ is reducible over $\mathbb{Q}$. Write $f(X) = g(X)h(X)$ for f, g not constants, and let R (resp. S) be the roots of g (resp. h) in $\mathbb{C}$ respectively. Then G_f fixes $g(X)$ and $h(X)$, so leaves R and S invariant. Hence it has at least two orbits on the roots of $f(X)$.

5. Define a map $f : R \to R_P/P_P, r \mapsto r/1 + P_P$. We have that $f(r) = 0 \Leftrightarrow r/1 \in P_P \Leftrightarrow r/1 = p/s$ for $p \in P, s \in R - P \Leftrightarrow rst = pt$ for $p \in P, s, t \in R - P \Leftrightarrow ru \in P$ for some $u \in R - P \Leftrightarrow r \in P$ since P is prime. Hence, f factors to give a monomorphism $f' : R/P \to R_P/P_P$. Since P_P is maximal in R_P, R_P/P_P is a field. So by the universal property of fractions, f' induces a unique monomorphism $f'' : Q \to R_P/P_P$ where Q is the field of fractions of the integral domain R/P. Finally, f'' is surjective since (by construction) R_P/P_P is generated as a field by elements of the form $r/1 + P_P$.