Answers to the Algebra Qualifying Exam
August 1993

1. (i) Let $C = \langle x \rangle$ be the given cyclic group of order 21. If $P = \langle x^3 \rangle$ is the subgroup of C of order 7, then P is a Sylow 7-subgroup of G and $C \subseteq \mathbb{N}_G(P)$. Thus $n_7 = |G : \mathbb{N}_G(P)|$ divides $|G : C| = 8 \cdot 3 = 24$. On the other hand, $n_7 \equiv 1 \bmod 7$ by Sylow's theorem and therefore $n_7 = 1$ or 8. If $n_7 = 8$, then $\mathbb{N}_G(P)$ is a subgroup of G of index 8. If $n_7 = 1$, then $P \triangleleft G$. In this case, if Q is a Sylow 3-subgroup of G, then $H = PQ$ is a subgroup of G of order $7 \cdot 9$ and hence of index 8.

(ii) Suppose G is simple. If G has an element x of order 21, then G has a subgroup of index 8 by (i) above, and G embeds in the symmetric group Sym_8. But Sym_8 has no elements of order 21, since any subgroup of order 7, being generated by a 7-cycle, is clearly self-centralizing. Thus x cannot exist.

2. Let $\theta \colon M \to M$ be a nonzero R-endomorphism of M with kernel K. Since $\theta \neq 0$, it follows that $M/K \cong \theta(M) \neq 0$. Now M has a composition series, so any nonzero submodule contains the unique minimal submodule N. In particular, $\theta(M) \supseteq N$, and if L is the complete inverse image of N under θ, then $M \supseteq L \supset K \supseteq 0$ and $L/K \cong N$.

If $K \neq 0$, then K also contains N, and by refining $M \supseteq L \supset K \supseteq N \supset 0$ to a composition series, we see that $N \cong L/K$ is a composition factor of M/N, contradiction. Thus $K = 0$ and θ is one-to-one. Furthermore, this implies that $\theta(M) \cong M$, so both modules have the same composition length. But $M \supseteq \theta(M)$ and therefore, by the latter equality of length, $M = \theta(M)$ and θ is onto.

3. (i) Write $f(x) = (x - a_1)h(x)$ in $K[a_1][x]$. Then $|K[a_1] : K| \leq n$ with equality precisely when $f(x)$ is irreducible. Similarly we have $|K[a_1, a_2] : K[a_1]| \leq n - 1$ with equality precisely when $g(x)$ is irreducible in $K[a_1][x]$. But

$$n(n-1) = |K[a_1, a_2] : K| = |K[a_1, a_2] : K[a_1]|\,|K[a_1] : K|$$

so it follows that f and g are both irreducible. Thus there is just one irreducible factor of f over K and it has degree n. There are two irreducible factors of f over $K[a_1]$, one is linear and one has degree $n - 1$.

(ii) We continue with the above notation. We are given $g(x) \in K[x]$ having $a_1 + a_2$ as a root. Hence $g(x + a_1)$ is a polynomial in $K[a_1][x]$ having a_2 as a root, and therefore $g(x + a_1)$ is divisible by $h(x)$, the minimal polynomial of a_2 over $K[a_1]$. It follows that $g(x + a_1)$ has a_k as a root for all $k \geq 2$, and therefore $a_1 + a_k$ is a root of $g(x)$ for all such k. Finally, let $i \neq j$ be subscripts. Since $f(x)$ is irreducible, there exists a field automorphism $\sigma \in \mathrm{Gal}(K[a_1, \ldots, a_n]/K)$ with $\sigma^{-1}(a_i) = a_1$. Of course, $\sigma^{-1}(a_j) = a_k$ for some $k \neq 1$. Thus $\sigma(a_1 + a_k) = a_i + a_j$. But $g(x) \in K[x]$ and $a_1 + a_k$ is a root of $g(x)$, so it follows that $\theta(a_1 + a_k) = a_i + a_j$ is also a root of $g(x)$.

4. Suppose first that $Y = (\, y_1 \quad y_2 \quad \cdots \quad y_n \,)^{\mathrm{T}}$ is a solution to the given system of equations over the rationals $\mathbb{Q}$. Choose an integer $m \neq 0$ so that $my_i \in \mathbb{Z}$ for all subscripts i. Then $X = mY$ is an integer solution so, by assumption, $my_i = my_j$ for all $i \neq j$. Thus $y_i = y_j$ since $m \neq 0$.

Next we use a result from linear algebra. Specifically, if $F \subseteq K$ are two fields and if $AX = 0$ is a homogeneous system of linear equations with A a matrix over F, then the solution space over K is spanned by the solution space over F. This is a trivial consequence of solving the system by elementary row operations. Returning to the problem at hand, this theorem tells us what the solutions look like over $\mathbb{R}$. If the solution space over $\mathbb{Q}$ is 0-dimensional, then the same is true for $\mathbb{R}$ and hence $(\, 0 \quad 0 \quad \cdots \quad 0 \,)^{\mathrm{T}}$ is the unique solution. On the other hand, if the solution space over $\mathbb{Q}$ has dimension ≥ 1, then by the above it is 1-dimensional with basis vector $(\, 1 \quad 1 \quad \cdots \quad 1 \,)^{\mathrm{T}}$. Thus any solution over $\mathbb{R}$ is just a scalar multiple of this vector and therefore all its entries are equal.

5. $R = \mathbb{Z}[i]$ is the ring of Gaussian integers and, for a number of reasons, it is integrally closed in its field of quotients $K = \mathbb{Q}[i]$. First, we could quote the fact that R is known to be a Euclidean domain. Thus it is a PID and a UFD, and any UFD is integrally closed in its field of fractions. Alternately, R is known to be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[i]$ and hence R is again integrally closed in K. In any case, we can now assume this fact.

Suppose α is a root of the monic polynomial $f(x) \in R[x]$. Since $f(x)$ is monic, all its roots are integral over R. If $g(x)$ is the minimal monic polynomial satisfied by α over K, then $g(x)$ divides $f(x)$ and therefore all roots of $g(x)$ are roots of $f(x)$ and hence are integral over R. Now the coefficients of $g(x)$ are $\pm$ the elementary symmetric functions in the roots of $g(x)$, so each such coefficient is integral over R. On the other hand, each coefficient is in K. Thus, by the remarks of the preceding paragraph, all coefficients of $g(x)$ are in R and $g(x) \in R[x]$.