Answers to the Algebra Qualifying Exam
January 2003

1. a. Let P be a Sylow p-subgroup of G. Then NP/N is a Sylow p-subgroup of G/N, and hence $NP/N = G/N$ since G/N is a p-group. Thus $G = NP$ and $G' = [NP, NP]$. If $a, b \in N$ and $x, y \in P$, then the commutator $[ax, by]$ satisfies $[ax, by] = (ax)^{-1}(by)^{-1}(ax)(by) = x^{-1}y^{-1}xy = [x, y]$ since a and b are central. It follows that $G' = [NP, NP] = [P, P] = P' \subseteq P$ is a p-group.

b. Now G acts on N by conjugation and, in this way, $G/\mathbf{C}_G(N)$ embeds in $\mathrm{Aut}(N)$. Since N is cyclic, $\mathrm{Aut}(N)$ is abelian, and consequently $G/\mathbf{C}_G(N)$ is abelian. Thus $G' \subseteq \mathbf{C}_G(N)$, so G' centralizes N and $N \cap G' \subseteq \mathbf{Z}(G')$. Furthermore, since $G'/(N \cap G')$ embeds in the p-group G/N, it follows that $G'/(N \cap G')$ is also a p-group. We can now conclude from part (a), applied to $G' \cap N \triangleleft G'$, that the commutator subgroup G'' of G' is a p-group.

2. a. Since s is not a unit, the principal ideal (s) is not equal to R. Now let A be an ideal of R properly larger than (s) and choose $a \in A \setminus (s)$. Since s is special, there exist $q, r \in R$ with $a = qs + r$ and with $r = 0$ or a unit of R. But $r = 0$ implies that $a = qs \in (s)$ which is not the case. Thus r is a unit and, since $r = a - qs \in A$, it follows that $A = R$. We conclude that (s) is maximal.

b. Let s be a polynomial of degree 1 in $\mathbb{Q}[X]$. If $a \in \mathbb{Q}[X]$ then, since $\mathbb{Q}$ is a field, the division algorithm implies that $a = qs + r$ where either $r = 0$ or $\deg r < \deg s = 1$. In particular, if $r \neq 0$, then r is a nonzero constant polynomial and hence a unit in $\mathbb{Q}[X]$.

c. The units of $\mathbb{Z}[X]$ are the units of $\mathbb{Z}$, and hence they are ± 1. Suppose by way of contradiction that s is a special element of $\mathbb{Z}[X]$. If $a \in \mathbb{Z}[X]$ then, by definition, there exists $q \in \mathbb{Z}[X]$ with $a = qs + r$, where $r = 0$, -1 or 1. In particular, s divides a, $a + 1$ or $a - 1$. If we take $a = 2$, then s divides 2, 3 or 1 and, at the very least, we see that s is a constant polynomial. (Note that ± 2 and ± 3 are special elements of $\mathbb{Z}$.) Furthermore, if we take $a = X$, then s divides X, $X + 1$ or $X - 1$. Since $s \in \mathbb{Z}$ must divide the coefficient of X in X, $X + 1$ or $X - 1$, we see that s divides 1, so $s = \pm 1$, a contradiction.

3. a. Since $F/\mathbb{Q}$ is a finite Galois extension, F is the splitting field in $\mathbb{C}$ of some polynomial $g(X) \in \mathbb{Q}[X]$. If τ is any automorphism of $\mathbb{C}$, for example τ could be complex conjugation $\overline{\ }$, then F^τ is the splitting field in $\mathbb{C}$ of $g(X)^\tau = g(X)$, and hence $F^\tau = F$.

b. If β is a complex root of the irreducible polynomial $f(X)$, then $\beta = \alpha^\sigma$ for some $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. By part (a), complex conjugation restricts to an automorphism of F and hence becomes a member of $\mathrm{Gal}(F/\mathbb{Q})$. In particular, since the latter group is abelian, we have $\overline{\beta} = \overline{\alpha^\sigma} = (\overline{\alpha})^\sigma$ and consequently $|\beta|^2 = \beta\overline{\beta} = \alpha^\sigma(\overline{\alpha})^\sigma = (\alpha\overline{\alpha})^\sigma = (|\alpha|^2)^\sigma = 1^\sigma = 1$. Since $|\beta| \geq 0$, we conclude that $|\beta| = 1$.

c. We know that a_i is $\pm$ the sum all products of the roots of $f(X)$ taken $n - i$ at a time. By part (b), each of these products has absolute values 1, and the number of such summands is clearly $\binom{n}{n-i} \leq 2^n$. Thus $|a_i| \leq 2^n$ for all i.

d. Write $m = (F : \mathbb{Q})$. Now suppose that $\alpha \in F$ is any algebraic integer of absolute value 1 and let $f(X) \in \mathbb{Q}[X]$ be its minimal monic polynomial. Since $\mathbb{Q}[\alpha] \subseteq F$, it follows that $n = \deg f(X) = (\mathbb{Q}[\alpha] : \mathbb{Q}) \leq (F : \mathbb{Q}) = m$. Furthermore, since all roots of $f(X)$ are Galois conjugate to α, they are all algebraic integers. In particular, each $a_i \in \mathbb{Q}$ is integral over $\mathbb{Z}$, and hence each a_i is contained in $\mathbb{Z}$. (Any unique factorization domain is integrally

closed in its field of fractions.) By part (c), a_i is an ordinary integer with $|a_i| \leq 2^n \leq 2^m$. Thus there are only finitely many possibilities for each a_i and hence only finitely many possibilities for $f(X)$. Since each such $f(X)$ has only finitely many roots in $\mathbb{C}$, there are only finitely many choices for α, with this number actually bounded by a function of m. Finally, if α is given, then $\alpha, \alpha^2, \alpha^3, \ldots$ are integral elements in F of absolute value 1, and hence they cannot all be distinct. Thus $\alpha^j = \alpha^k$ for some $k > j$ and, since $\alpha \neq 0$, we conclude that $\alpha^{k-j} = 1$.

4. a. Let $m = \dim W < \dim V = n$ and let $\{w_1, w_2, \ldots, w_m\}$ be a basis for W. For each i, the map $\lambda_i \colon V \to K$ given by $v \mapsto (w_i, v)$ is a linear functional with $\ker \lambda_i$ being a subspace of V of codimension ≤ 1. Since $m < n = \dim V$, it follows that $U = \bigcap_{i=1}^{m} \ker \lambda_i \neq 0$. Finally, let $0 \neq u \in U$. Then $(w_i, u) = \lambda_i(u) = 0$ for all i, and hence each w_i is contained in the kernel of the linear functional given by $v \mapsto (v, u)$. Since $\{w_1, w_2, \ldots, w_m\}$ spans W, it follows that W is contained in this kernel and hence $(W, u) = 0$, as required.

b. Since $\mathcal{B}$ is a basis for V, there exists a linear functional $\mu \colon V \to K$ such that $\mu(b) = 1$ for all $b \in \mathcal{B}$. Note that $\mu(V) = K \neq 0$, so $\ker \mu$ is a proper subspace of V. But each $a - b$, with $a, b \in \mathcal{B}$, is contained in $\ker \mu$, and hence $W \subseteq \ker \mu < V$. Now suppose that $(W, v) = 0$ and write $v = \sum_{c \in \mathcal{B}} k_c c$ with $k_c \in K$. Since this sum is finite and $\mathcal{B}$ is infinite, there exists a basis element b with $k_b = 0$. Now, for all $a \in \mathcal{B}$, we have $a - b \in W$, so $0 = (a - b, v) = k_a - k_b$, by definition of the bilinear form. In particular, $k_a = k_b = 0$ for all $a \in \mathcal{B}$ and hence $v = 0$.

5. a. Let $\mathcal{X}$ be the set of all infinitely generated submodules X of V with $X \supseteq W$, and partially order $\mathcal{X}$ by inclusion. Note that $W \in \mathcal{X}$ and hence $\mathcal{X} \neq \emptyset$. Now let $\mathcal{C}$ be a nonempty chain (linearly ordered subset) of $\mathcal{X}$ and let $C = \bigcup_{X \in \mathcal{C}} X$ be the union of all members of $\mathcal{C}$. We claim that $C \in \mathcal{X}$ is an upper bound for all $X \in \mathcal{C}$. To start with, C is clearly closed under multiplication by R. Furthermore, if $x, y \in C$, then say $x \in X$ and $y \in Y$ with $X, Y \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, we have $X \subseteq Y$ or $Y \subseteq X$. If, for example, $X \subseteq Y$, then $x, y \in Y$, so $x + y \in Y \subseteq C$. It follows that C is a submodule of V containing all members of $\mathcal{C}$. If $C \notin \mathcal{X}$, then C is finitely generated, say with generators $x_1, x_2, \ldots, x_n$. Then $x_i \in X_i \in \mathcal{C}$ and, since $\mathcal{C}$ is a chain, there exists a subscript k with $X_i \subseteq X_k$ for all i. Hence $x_1, x_2, \ldots, x_n \in X_k$, so $C = \sum_i x_i R \subseteq X_k \subseteq C$ and $X_k = \sum_i x_i R$ is finitely generated, a contradiction. We have therefore shown that each nonempty chain in $\mathcal{X}$ has an upper bound in $\mathcal{X}$, so Zorn's Lemma implies that $\mathcal{X}$ has a maximal member M. By definition, $M \supseteq W$, M is infinitely generated, and all submodules of V properly larger than M are finitely generated.

b. Assume that R is right Noetherian. If V is finitely generated, then V is a Noetherian R-module and hence all its submodules are also be finitely generated, a contradiction since $W \subseteq V$ is infinitely generated. Thus V is infinitely generated and hence, if M has the given property of part (a), then V cannot be properly larger than M. In other words, we must have $M = V$.

c. If R is not right Noetherian, let W be an infinitely generated right ideal of R. Set $V = R_R$ and note that $V \supseteq W$ and that V is generated by the single element 1. In particular, $M \neq V$ since M is infinitely generated.