Answers to the Algebra Qualifying Exam
January 2004

1. a. If \( H \) and \( K \) are subgroups of \( G \), then it is known that \( |H : H \cap K| \leq |G : K| \). Since we are given that \( |G : H| = n \), we have \( |H : H \cap H^g| \leq |G : H^g| = |G : H| = n \), where the first equality holds because \( |H| = |H^g| \).

b. We are given that \( H \) is abelian. Then \( H^g \) is also abelian, and so both \( H \) and \( H^g \) centralize \( H \cap H^g \). It follows that \( H \subseteq C \) and \( H^g \subseteq C \), where \( C = C_G(H \cap H^g) \) is the centralizer. Since \( H \) is maximal in \( G \), either \( C = G \) or \( C = H \). In the first case, \( H \cap H^g \subseteq Z(G) \), and in particular \( H \cap H^g \triangleleft G \). Otherwise, \( H^g \subseteq C = H \), and thus \( H^g = H \) and \( g \in N_G(H) \). In this case, \( H \cap H^g = H \) and we must show that \( H \triangleleft G \). But \( H < N_G(H) \) since \( g \in N_G(H) \) and we are given that \( g \notin H \). By the maximality of \( H \), therefore, \( N_G(H) = G \) and \( H \triangleleft G \), as wanted.

c. Here \( n \) is prime, and so \( H \) is maximal and we are given that \( H \) is abelian. By (b), we have \( H \cap H^g \triangleleft G \). Since \( G \) is simple and \( H \cap H^g \) is proper, we have \( H \cap H^g = 1 \). By (a), therefore, \( |H| = |H : 1| = |H : H \cap H^g| \leq n \), and so \( |G| = n|H| \leq n^2 \). Since \( G \) is simple and \( n \) is prime, we cannot have equality here and thus \( |G| < n^2 \) and \( |G| = nm \), where \( m < n \). But then a Sylow \( n \)-subgroup of \( G \) has order \( n \) and the number of these divides \( m \). Since \( m < n \), the number of Sylow \( n \)-subgroups must be 1. By simplicity, then, \( |G| = n \) and hence \( |H| = 1 \).

2. a. Since \( X^2, X^3 \in K[X] \) have their coefficient of the indeterminate \( X \) equal to 0, it follows that \( X^2, X^3 \in R \). To show \( X^3 \) is irreducible, observe that it is a nonzero nonunit and suppose \( X^3 = fg \), where \( f, g \in R \). In particular, \( f \) and \( g \) are polynomials and the factorization \( X^3 = f(X)g(X) \) holds in \( K[X] \). But \( K[X] \) is a UFD, and thus if neither \( f \) nor \( g \) is a constant polynomial, the only possibilities are \( f(X) = aX \) and \( g(X) = bX^2 \) or vice versa, where \( a \) and \( b \) are nonzero constants. But this is impossible since the polynomial \( aX \) does not lie in \( R \). Thus one of \( f \) or \( g \) is a constant, hence is a unit in \( R \), and this proves that \( X^3 \) is irreducible. The proof that \( X^2 \) is irreducible is similar.

In the ring \( R \), we see that \( X^3 \) divides \( (X^2)(X^4) \), but it does not divide either \( X^2 \) or \( X^4 \). (That it does not divide \( X^2 \) is clear; it does not divide \( X^4 \) since \( X \notin R \).) Similarly, \( X^2 \) divides \( (X^3)(X^3) \) in \( R \), but it does not divide \( X^3 \). This shows that neither \( X^2 \) nor \( X^3 \) is prime in \( R \).

b. We have \( R = K[X^2, X^3] \), and so \( R \) is a homomorphic image of the polynomial ring \( K[X, Y] \), which is noetherian by the Hilbert Basis theorem. Thus \( R \) is noetherian.

Let \( I \) be the ideal of \( R \) consisting of the polynomials in \( R \) having 0 constant term. Then \( X^2 \) and \( X^3 \) lie in \( I \). If \( I \) is principal, write \( I = (f) \). Note that \( f \) is not a unit in \( R \) since \( I < R \). Then \( f \) divides \( X^2 \) in \( I \) and since \( X^2 \) is irreducible, it follows that \( X^2 \) is a unit multiple of \( f \), and so \( f = aX^2 \) for some nonzero constant \( a \). Similarly, since \( X^3 \) is irreducible, we deduce that \( f = bX^3 \) for some nonzero constant \( b \). This is a contradiction since the polynomials \( aX^2 \) and \( bX^3 \) are different.

3. a. Let \( g(X) \in E[X] \). We want to show that \( g \) splits, and so it suffices to assume that \( g \) is irreducible over \( E \) and to show that \( g \) is linear. Adjoin a root \( \alpha \) of \( g \) to \( E \) to get a field \( K = E[\alpha] \). Now \( K \) is algebraic over \( E \), which is algebraic over \( F \), and so \( \alpha \) is algebraic over \( F \). Let \( f(X) \in F[X] \) be the minimal polynomial of \( \alpha \) over \( F \). By hypothesis, \( f \) splits over \( E \), and so all roots of \( f \) in any extension field of \( E \) actually lie in \( E \). In particular,
\( \alpha \in E \) and thus the irreducible polynomial \( g(X) \in E[X] \) has a root in \( E \). It follows that \( g \) is linear, as wanted.

b. By (a), it suffices to show that every polynomial \( f(X) \in F[X] \) splits over \( E \). Given \( f \), let \( L \) be a splitting field for \( f \) over \( F \). Then \( L \) has finite degree over \( F \), and since \( F \) has characteristic 0, the primitive element theorem tells us that there exists \( \beta \in L \) such that \( L = F[\beta] \). Now by hypothesis, the minimal polynomial of \( \beta \) over \( F \) has a root \( \gamma \in E \). Since \( \beta \) and \( \gamma \) have the same minimal polynomial over \( F \), we see that \( F[\beta] \) and \( F[\gamma] \) are \( F \)-isomorphic fields. But \( f \in F[X] \) splits over \( F[\beta] \), and thus \( f \) also splits over \( F[\gamma] \). But \( F[\gamma] \subseteq E \), and so \( f \) splits over \( E \), as wanted.

4. a. We can factor \( f(X) = g(X)h(X) \), where \( \deg(g) = m > 0 \). Since \( f \) is the minimal polynomial of \( T \) and \( h \) has smaller degree, we know that \( h(T) \) is not the 0 operator and we can choose \( v \in V \) such that \( h(T)(v) \neq 0 \), and we write \( w = h(T)(v) \). Now let \( W \) be the span of \( \{w, T(w), T^2(w), \ldots, T^{m-1}(w)\} \) and note that \( W \) is nonzero and \( \dim(W) \leq m \).

To prove that \( T(W) \subseteq W \), it suffices to show that \( T^m(w) \in W \). By the division algorithm for polynomials, we can write \( X^m = g(X)g(X) + r(X) \), where \( \deg(r) < \deg(g) = m \). Then \( T^m(w) = g(T)g(T)(w) + r(T)(w) \). But \( q(T)g(T)(w) = g(T)g(T)h(T)(v) = 0 \), where the second equality follows since \( g(T)h(T) = f(T) = 0 \). It follows that \( T^m(w) = r(T)(w) \). This vector lies in \( W \), however, since either \( r = 0 \) or \( \deg(r) < m \), and this completes the proof.

b. Now assume \( W \subseteq V \) is a nonzero subspace such that \( T(W) \subseteq W \) and \( \dim(W) = n \). Let \( g(X) \in F[X] \) be the minimal polynomial of the restriction of \( T \) to \( W \), so that \( 0 < \deg(g) \leq n \), where the first inequality holds since \( W \) is nonzero. To show that \( g \) divides \( f \), write \( f(X) = q(X)g(X) + r(X) \), where \( \deg(r) < \deg(g) \). Since \( f(T) = 0 \) annihilates \( W \) and \( g(T) \) also annihilates \( W \), it follows that \( r(T) - f(T) - q(T)g(T) \) also annihilates \( W \). But \( r \) cannot be nonzero since otherwise its degree would be smaller than the degree of the minimal polynomial \( g \) of the restriction of \( T \) to \( W \). It follows that \( r = 0 \) and \( g \) divides \( f \), as wanted.

5. a. We have \( V = X \oplus Y \), where \( X \) and \( Y \) are nonzero modules. Suppose \( X \) and \( Y \) are simple and not isomorphic and let \( U \subseteq V \) be a submodule different from 0 and \( V \). We want to show that \( U \) must be \( X \) or \( Y \), so we suppose not. Then \( U \cap X = 0 \) since \( X \) is simple. Also \( U + X > X \). But \( V/X \cong Y \) is simple, and this shows that \( U + X = V \). Then \( V = X \oplus U \) and \( U \cong V/X \cong Y \). Similarly, \( U \cong X \), so \( X \cong Y \), a contradiction.

Conversely, now assume that there are no submodules other than the obvious four. Then \( X \) must be simple since if it had a nonzero proper submodule, that would be a fifth submodule of \( V \), which does not exist. Similarly \( Y \) is simple. If there is an isomorphism \( \theta : X \rightarrow Y \), let \( S = \{x + \theta(x) \mid x \in X\} \). It is trivial to check that \( S \) is a submodule different from the original four, and this contradiction shows that \( X \) and \( Y \) are not isomorphic.

b. If \( \alpha \in \text{End}(V) \), then \( \alpha(X) \cong X \) or \( \alpha(X) = 0 \) since \( X \) is simple, and thus \( \alpha(X) = X \) or \( \alpha(X) = 0 \subseteq X \) since \( X \) is the only submodule of \( V \) isomorphic to \( X \) by (a). In other words, for all \( \alpha \in \text{End}(V) \), we have \( \alpha(X) \subseteq X \) and similarly, \( \alpha(Y) \subseteq Y \). Writing \( \alpha_X \) and \( \alpha_Y \) to denote the restrictions of \( \alpha \) to \( X \) and \( Y \), we now have the ring homomorphism \( \theta : \alpha \mapsto (\alpha_X, \alpha_Y) \) from \( \text{End}(V) \) into the external direct sum \( \text{End}(X) \oplus \text{End}(Y) \). This map is injective since only \( 0 \in \text{End}(V) \) annihilates both \( X \) and \( Y \) and it is surjective since given \( \beta \in \text{End}(X) \) and \( \gamma \in \text{End}(Y) \), we can define \( \alpha \) on \( V \) by \( \alpha(x + y) = \beta(x) + \gamma(y) \). (This is well defined because the sum \( V = X + Y \) is direct.) Finally, \( \text{End}(X) \) and \( \text{End}(Y) \) are division rings by Schur’s lemma since \( X \) and \( Y \) are simple.