Answers to the Algebra Qualifying Exam
January 1993

1. i) $B \cong G/A \supseteq HA/A \cong H/(H \cap A) \cong H$. Thus B contains a subgroup isomorphic to H. For the example, let $A = \langle a \rangle$ and $B = \langle b \rangle$ both be cyclic of order 2 so that G is a fours group. If $H = \langle ab \rangle$, then $|H| = 2$ and $H \cap A = 1 = H \cap B$.

ii) By the above, $|H|$ divides $|B|$. Furthermore, $A \cong G/B \supseteq HB/B \cong H/(H \cap B)$. Thus $|H/(H \cap B)|$ divides $|A|$. But the latter two numbers are relatively prime, since $|H/(H \cap B)|$ divides $|B|$, so $|H/(H \cap B)| = 1$ and $H = H \cap B \subseteq B$.

2. i) This is the usual argument with a little care. By assumption, $I_m = Kf(x)$ with $f(x) = \cdots + ax^m$ and $0 \neq a \in E$. We show by induction on $\deg g(x)$ that if $g \in I$, then g is an R-multiple of $f(x)$. If $\deg g < m$, then $g(x) = 0 = 0f(x)$. If $\deg g = m$, then $g \in I_m = Kf$. Since $K \subseteq R$, this case also follows. Finally, let $g = \cdots + bx^n$ have degree $n > m$. Now $a^{-1}b \in E$ and since $n > m$ we have $a^{-1}bx^{n-m} \in R$. Thus $h(x) = g(x) - (a^{-1}bx^{n-m})f(x) \in I$ and this has lower degree than g. By induction, h is a multiple of f, and hence so is g.

ii) The map $I_m \to K$ given by $g(x) \mapsto g(0)$ is a K-linear transformation. Since $\dim_K I_m > 1$, there must be a nontrivial kernel.

iii) Since I is not principal, $\dim_K I_m > 1$ by (i) and hence, by (ii), there is a polynomial $0 \neq f(x) \in I_m$ with $f(0) = 0$. Write $f(x) = ax^n + \cdots + bx^m$ with $1 \leq n \leq m$ and $0 \neq a, b \in E$. Now observe that $f(x) = ax \cdot g(x)$ where $g = x^{n-1} + \cdots + a^{-1}bx^{m-1}$. Notice that $g \in R$ and $ax \in R$. Also $\deg g = m - 1$ so $g \notin I$. Since I is prime and $ax \cdot g = f \in I$, it follows that $ax \in I$. But $\deg ax = 1$, so $m = 1$.

3. i) Say $f(x) = x^n + ax^{n-1} + \cdots$. Then $f(x+\sqrt{2}) = (x+\sqrt{2})^n + a(x+\sqrt{2})^{n-1} + \cdots = x^n + (n\sqrt{2} + a)x^{n-1} + \cdots$. Since $a \in \mathbb{Q}$ and $\sqrt{2}$ is irrational, we conclude that $n\sqrt{2} + a$ is not rational.

ii) Let α be a complex root of $f(x)$. Then $K[\alpha] \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$ and $|\mathbb{Q}[\alpha] : \mathbb{Q}| = n$ since f is irreducible. Also $K[\alpha] \supseteq K \supseteq \mathbb{Q}$ and $|K : \mathbb{Q}| = 2$. Since n is given to be odd, it follows that $|K[\alpha]\colon\mathbb{Q}|$ is divisible by $2n$. Hence $|K[\alpha] : K| \geq n$. Finally, note that $\beta = \alpha - \sqrt{2}$ is a root of $f(x+\sqrt{2})$ over K and since $K[\beta] = K[\alpha]$, we have $|K[\beta] : K| \geq n = \deg f(x+\sqrt{2})$. This surely implies that $f(x+\sqrt{2})$ is irreducible over K.

iii) We know that $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$ where $\sigma\colon \sqrt{2} \mapsto -\sqrt{2}$ and extend σ to an automorphism of $K[x]$. Then $f(x+\sqrt{2})^\sigma = f(x-\sqrt{2})$ is also an irreducible polynomial in $K[x]$. Furthermore, $g(x) = f(x+\sqrt{2})f(x-\sqrt{2})$ is fixed under σ, so g is indeed a monic polynomial over $\mathbb{Q}$. (This fact is given and need not be proved.) Suppose g has a nontrivial factorization $g(x) = h(x)k(x)$ with h and k monic polynomials in $\mathbb{Q}[x]$. Then view this as a factorization in $K[x]$. Since $g(x) = f(x+\sqrt{2})f(x-\sqrt{2})$ is the unique factorization of g into monic irreducibles in $K[x]$, it follows that $h(x) = f(x+\sqrt{2})$ and $k(x) = f(x-\sqrt{2})$ or vice versa. But $f(x+\sqrt{2}) \notin \mathbb{Q}[x]$ by (i), so we have a contradiction.

4. Remember $\mathbb{C}$ is algebraically closed of characteristic 0. Let λ be an eigenvalue of Z and let $W = \{ v \in V \mid Zv = \lambda v \}$. Then W is a nonzero subspace of V and, since Z commutes with X and Y, we see that W is invariant under X, Y, Z. By assumption, $W = V$ and Z is the scalar transformation λI. If $\dim V = n$, then by taking traces, we have $n\lambda = \operatorname{tr} Z = \operatorname{tr}(XY) - \operatorname{tr}(YX) = 0$ so, since the characteristic is zero, it follows that $\lambda = 0$ and hence $Z = 0$. But then X and Y are commuting linear transformations, so they have a common eigenvector v_0. Since $\mathbb{C}v_0$ is invariant under X, Y, Z, it follows that $V = \mathbb{C}v_0$ has dimension 1.

5. Let $A = \sum_{i=1}^n v_i\mathbb{Z}$ so that A is an additive abelian subgroup of V. Note that A is clearly a finitely generated abelian group, generated by $v_1, \ldots, v_n$. By the Fundamental Theorem of Abelian Groups, A is a direct sum of cyclic groups, say $A = \cdot\sum_{i=1}^m \langle w_i \rangle$ where each $0 \neq w_i \in V$. Of course $\langle w_i \rangle = w_i\mathbb{Z}$ and the goal is to show that the w_i's are $\mathbb{Q}$-linearly independent. Thus suppose $\sum w_i q_i = 0$ with $q_i \in \mathbb{Q}$. By multiplying by a nonzero integer, we can clear denominators in the q_i's and hence we can assume that all $q_i \in \mathbb{Z}$. But then $w_i q_i \in \langle w_i \rangle$ and, since the cyclic groups direct sum, we must have $w_i q_i = 0$ for all i. But $0 \neq w_i \in V$ and V is a vector space over $\mathbb{Q}$, so this forces $q_i = 0$ for all i.