Answers to Algebra Qualifying Exam
August 1992

1. We proceed by induction on $|P|$, the result being trivial when $|P| = 1$. Assume $|P| > 1$, let Z be a central subgroup of P of order p and let $^-\colon P \to \bar{P} = P/Z$ be the natural epimorphism. Then $\bar{z} = [\bar{x}, \bar{y}]$. Furthermore, if M is a normal subgroup of $\bar{P}$ containing $\bar{z}$ and if N is its complete inverse image in P, then $N \triangleleft P$ and $z \in N$. Thus, by assumption, $x \in N$ and therefore $\bar{x} \in \bar{N} = M$. We can now apply induction to $\bar{P}$ and conclude that $\bar{x} = 1$. Thus x is contained in the central subgroup Z, so $z = [x, y] = 1$. Finally, $z = 1$ is contained in the identity subgroup which is normal in P, so $x \in \langle 1 \rangle$ and $x = 1$.

2. Clearly $Q = (x^2) = x^2R = \{\, a_2x^2 + a_4x^4 + a_5x^5 + \cdots + a_nx^n \mid a_i \in K \,\}$ and let $P = x^2R + x^3R = \{\, a_2x^2 + a_3x^3 + a_4x^4 + \cdots + a_nx^n \mid a_i \in K \,\}$. Then $P > Q$ and $P^2 < Q$, so Q is not a power of P. Furthermore, if $f = b_0 + b_2x^2 + \cdots + b_nx^n \in \sqrt{Q}$, then some power of f is in Q. From this it follows that $b_0 = 0$, so $f \in P$ and hence $P = \sqrt{Q}$. Finally suppose $gh \in Q$ with $g = c_0 + c_2x^2 + \cdots + c_nx^n$ and $h = d_0 + d_2x^2 + \cdots + d_mx^m$. If $g \notin \sqrt{Q} = P$, then $c_0 \neq 0$ and $gh = c_0d_0 + (c_0d_2 + d_0c_2)x^2 + (c_0d_3 + d_0c_3)x^3 + \cdots$. Since $gh \in Q$, we have $c_0d_0 = 0$ so $d_0 = 0$, and $c_0d_3 + d_0c_3 = 0$ so $d_3 = 0$. Thus $h \in Q$ and Q is primary.

3. (i) Let α be a root of $f(x)$ in some extension field of E. Then the degrees satisfy $(E[\alpha] : Q) = (E[\alpha] : E)(E : Q) < \infty$ and we can let $g(x) \in Q[x]$ be the minimal polynomial for α over Q. Since $g(\alpha) = 0$, $g(x) \in E[x]$ and $f(x)$ is the minimal polynomial for α in $E[x]$, it follows that $f(x) \mid g(x)$ in $E[x]$. Conversely if $h(x) \in Q[x]$ is divisible by $f(x)$ in $E[x]$, then $h(\alpha) = 0$. Thus $h(x) \in g(x)Q[x]$ and we conclude that $h(x)$ is not irreducible and monic unless $h(x) = g(x)$.

(ii) If E is a splitting field over Q, then E/Q is Galois with Galois group G since Q has characteristic 0. Then G permutes the polynomials in $E[x]$ and we let $h(x)$ be the product of the distinct G-conjugates of $f(x)$. Since $E^G = Q$, it is clear that $h(x) \in Q[x]$, so $g(x) \mid h(x)$ since $h(\alpha) = 0$. On the other hand, $f(x) \mid g(x)$, so $f(x)^\sigma \mid g(x)$ for any $\sigma \in G$. Hence each of the distinct irreducible $f(x)^\sigma$ factors of $h(x)$ divides $g(x)$ and therefore $h(x) \mid g(x)$. Since $g(x)$ and $h(x)$ are monic, this implies that $h(x) = g(x)$ so $g(x) = f(x)^{\sigma_1} f(x)^{\sigma_2} \cdots f(x)^{\sigma_k}$ and $\deg g(x) = k \deg f(x)$.

(iii) We want E not to be a splitting field over Q, say $E = Q[\alpha]$ where α is the real cube root of 2. If ω is a primitive cube root of 1, then $(E[\omega] : E) = 2$, since E is a real field. Let $\beta = \omega\alpha$ be another cube root of 2. Then $\beta \in E[\omega]$ and β is not real, so the minimal polynomial $f(x)$ for β over E has degree 2. On the other hand, β satisfies $g(x) = x^3 - 2$ which is irreducible over Q by Eisenstein's criterion. Since $\deg f = 2$ does not divide $\deg g = 3$, we have an appropriate example.

4. (i) Set $u = w - kv$ where $k = B(v, w)B(v, v)^{-1} \in K$. Then $B(v, u) = B(v, w) - k\,B(v, v) = 0$ so, by assumption, $0 = B(u, v) = B(w, v) - k\,B(v, v) = B(w, v) - B(v, w)$.

(ii) Suppose there exists $v \in V$ with $B(v, v) \neq 0$. Let $W = \{\, w \in V \mid B(v, w) = 0 \,\} = \{\, w \in V \mid B(w, v) = 0 \,\}$. Since W is the kernel of the linear functional $V \to K$ given by $w \mapsto B(v, w)$ and since $v \notin W$, it follows that $V = Kv \oplus W$. Let $x, y \in W$. If $B(x, x) \neq 0$, then $B(x,y) = B(y,x)$ by (i) above. If $B(x,x) = 0$, then $B(v+x, v+x) = B(v,v) \neq 0$ and (i) yields $B(x,y) = B(v+x,y) = B(y,v+x) = B(y,x)$. Thus B is symmetric on W and since W and v are perpendicular, we see that B is symmetric on $V = Kx \oplus W$.

5. (i) Say $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts trivially on Ω. Then $(a,b) = (1,0)g \in K(1,0)$, so $b = 0$. Similarly $(c,d) = (0,1)g \in K(0,1)$, so $c = 0$. Furthermore, $(a,d) = (1,1)g \in K(1,1)$, so $a = d$. Since $\det g = 1$, we have $a^2 = 1$ so $a = \pm 1$. Thus $g = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and both these matrices do act trivially on Ω.

(ii) We will show that every one-dimensional subspace is in the orbit of $K(1,0)$. By clearing denominators and eliminating common factors, we see that every one-dimensional subspace contains a vector (r,s) with r and s relatively prime integers. Thus there exist integers x, y with $rx - sy = 1$ and we set $g = \begin{pmatrix} r & s \\ y & x \end{pmatrix}$. Then g is an integer matrix with $\det g = rx - sy = 1$, so $g \in G$. Since $(1,0)g = (r,s)$, transitivity is proved.