Answers to the Algebra Qualifying Exam
August 1998

1. (a) Since $\langle 1\rangle \neq N \triangleleft G$ and G is finite, we can choose $\langle 1\rangle \neq M \subseteq N$ with M minimal normal in G. Then $M \subseteq \operatorname{soc}(G)$, so $N \cap \operatorname{soc}(G) \supseteq M \neq \langle 1\rangle$.

(b) Let $S = \operatorname{soc}(G)$ so that S is a characteristic subgroup of G. Since $\operatorname{soc}(S) \subseteq S$, we have $\operatorname{soc}(\operatorname{soc}(G)) \subseteq \operatorname{soc}(G)$. Furthermore, $\operatorname{soc}(S)$ is characteristic in S, so $\operatorname{soc}(S) \triangleleft G$. Now let N be any minimal normal subgroup of G. By definition, $N \subseteq S$ and then $\langle 1\rangle \neq N \triangleleft S$. In particular, part (a) implies that $N \cap \operatorname{soc}(S) \neq \langle 1\rangle$. But $N \cap \operatorname{soc}(S)$ is a normal subgroup of G and N is minimal normal in G, so we must have $N \cap \operatorname{soc}(S) = N$ and $N \subseteq \operatorname{soc}(S)$. In other words, $\operatorname{soc}(S)$ contains all the generators of S, namely all the minimal normal subgroups of G, so $\operatorname{soc}(S) \supseteq S$ and we have the reverse inclusion.

(c) Assume that $G = \operatorname{soc}(G)$ and let M be a minimal normal subgroup of G. Suppose $\langle 1\rangle \neq H \triangleleft M$. We compute the normalizer of H in G. For this, let N be any minimal normal subgroup of G. If $N \neq M$, then $N \not\supseteq M$, so $M \cap N \neq M$ and hence $M \cap N = \langle 1\rangle$. This implies that N centralizes M, so N centralizes and hence normalizes H. On the other hand, if $M = N$, then we are given $H \triangleleft M = N$ and again N normalizes H. In other words, $\mathbb{N}_G(H)$ contains all of the generators of $\operatorname{soc}(G) = G$, namely all the minimal normal subgroups of G. It follows that $\mathbb{N}_G(H) = G$, so $H \triangleleft G$. But $\langle 1\rangle \neq H \subseteq M$ and M is minimal normal in G, so we must have $H = M$ and therefore M is simple.

2. (a) If $r, s \in I_q$, then $(r+s)q = rq + sq \in R + R \subseteq R$ and $r + s \in I_q$. Furthermore, if $r \in R$ and $s \in I_q$, then $(rs)q = r(sq) \in R{\cdot}R \subseteq R$ and $rs \in I_q$. Since $0 \in I_q$, it follows that I_q is an ideal of R.

(b) We know that each R_M is a subring of F containing R, so $\bigcap_M R_M \supseteq R$. For the reverse inclusion, let $q \in \bigcap_M R_M$ and consider the ideal I_q of R. If $I_q \neq R$, then I_q is contained in some maximal ideal of R, say N. But $q \in R_N$, so we have $q = a/b$ with $a \in R$ and $b \in R \setminus N$. Thus $bq = a \in R$, so $b \in I_q \subseteq N$, a contradiction. It follows that $I_q = R$, so $1 \in I_q$ and $q = 1{\cdot}q \in R$.

(c) If $\alpha = a + b\sqrt{-3}$, then $N(\alpha) = |\alpha|^2 = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2$. Thus $\alpha \neq 0$ implies that $N(\alpha)$ is a positive integer. Furthermore $N(\alpha) = 1$ implies that $\alpha = \pm 1$ and $N(\alpha) = 2$ cannot occur. From $q = (1 - \sqrt{-3})/2$ we see that $q \notin R$ and that $2 \in I_q$. From $q = 2/(1 + \sqrt{-3})$, it follows that $1 + \sqrt{-3} \in I_q$. Since $q \notin R$, we know that $1 \notin I_q$.

Suppose that $I_q = \alpha R$ is a principal ideal. Then $1 + \sqrt{-3} = \alpha\beta$ for some $\beta \in R$, so taking norms yields $4 = N(1 + \sqrt{-3}) = N(\alpha)N(\beta)$. But $N(\alpha) \neq 1$ since $I_q \neq R$, and as we observed, $N(\alpha) \neq 2$. Thus $N(\alpha) = 4$ and $N(\beta) = 1$, so $\beta = \pm 1$ and $\alpha = \pm(1 + \sqrt{-3})$. Similarly, $2 \in I_q$, so $2 = \alpha\gamma$ for some $\gamma \in R$. Since $N(2) = 4$, the same argument shows that $\alpha = \pm 2$, a contradiction.

3. (a) Let α be a root of $h(x)$ in the algebraic closure of F. Since $h(x)$ is irreducible in $F[x]$, it follows that $\deg h(x) = |F(\alpha) : F|$. Furthermore, $h(x)$ divides $g(x)$, so $0 = g(\alpha) = f(\alpha^n)$, and since $f(x)$ is irreducible, we have $\deg f(x) = |F(\alpha^n) : F|$. Finally, $\deg h(x) = |F(\alpha) : F| = |F(\alpha) : F(\alpha^n)|{\cdot}|F(\alpha^n) : F| = |F(\alpha) : F(\alpha^n)|{\cdot}\deg f(x)$, and thus $\deg f(x)$ divides $\deg h(x)$.

(b) Let E be a splitting field of $g(x)$ over F. Suppose $h(x)$ and $k(x)$ are irreducible factors of $g(x)$ in $F[x]$, and choose α and β in the algebraic closure of E with $h(\alpha) = 0$ and $k(\beta) = 0$. As above, we know that $g(\alpha) = 0 = g(\beta)$, so $\alpha, \beta \in E$, and furthermore $f(\alpha^n) = 0 = f(\beta^n)$. Since $f(x)$ is irreducible in $F[x]$, the latter implies that there exists an F-isomorphism $\sigma\colon F(\alpha^n) \to F(\beta^n)$ with $\sigma(\alpha^n) = \beta^n$. Note that E is the splitting field of $g(x)$ over $F(\alpha^n)$ and it is also the splitting field of $g(x)$ over $F(\beta^n)$. Furthermore, since $g(x) \in F[x]$, $g(x)$ maps to $g(x)$ under the natural extension $\sigma\colon F(\alpha^n)[x] \to F(\beta^n)[x]$. The uniqueness of splitting fields now implies that σ extends to an F-isomorphism $\tau\colon E \to E$. Now $\alpha, \beta \in E$ and $\tau(\alpha)^n = \tau(\alpha^n) = \sigma(\alpha^n) = \beta^n$. Thus $\tau(\alpha) = \varepsilon\beta$ for some nth root of unity ε and, by assumption, $\varepsilon \in F$. In particular, $F(\varepsilon\beta) = F(\beta)$, and τ yields an F-isomorphism from $F(\alpha)$ to $F(\beta)$. Finally, since $h(x)$ and $k(x)$ are irreducible in $F[x]$, we conclude that $\deg h(x) = |F(\alpha) : F| = |F(\beta) : F| = \deg k(x)$, as required.

4. (a) Let $\{u_1, u_2, \ldots, u_r\}$ be a basis for U, so that $\dim U = r$, and define the map $T\colon V \to K^r$ by $T(v) = ((u_1, v), (u_2, v), \ldots, (u_r, v))$. Then T is a linear transformation and $\ker T = U^\perp$ since any vector perpendicular to a basis for U is perpendicular to all of U. Since $\dim \operatorname{im} T \le \dim K^r = r$, we conclude that $\dim V = \dim \operatorname{im} T + \dim \ker T \le r + \dim U^\perp = \dim U + \dim U^\perp$.

(b) Since the form is nonsingular, we have $0 = V^\perp = U^\perp \cap X^\perp$. Thus $U^\perp \dotplus X^\perp$ is a direct sum contained in V, and $\dim U^\perp + \dim X^\perp = \dim(U^\perp \dotplus X^\perp) \le \dim V$.

(c) Write $V = U \dotplus X$, a direct sum of U and some complementary subspace X. By (a) and (b), we have $\dim U^\perp + \dim X^\perp \le \dim V \le \dim X + \dim X^\perp$, so $\dim U^\perp \le \dim X$. Thus $\dim U + \dim U^\perp \le \dim U + \dim X = \dim(U \dotplus X) = \dim V$, and by (a) again, we have the reverse inequality $\dim V \le \dim U + \dim U^\perp$.

5. (a) In both parts, we view A additively. By assumption, $A = B \dotplus X$ where X is a complementary subgroup. In particular, if $B \subseteq C \subseteq A$, then the modular law implies that $C = A \cap C = (B + X) \cap C = B + (X \cap C)$. Furthermore, $B \cap X = 0$ implies that $B \cap (X \cap C) = 0$. Thus $C = B \dotplus (X \cap C)$.

(b) Since $\bar{A} = A/B$ is a finite abelian group, we know that $\bar{A} = \bar{C}_1 \dotplus \bar{C}_2 \dotplus \cdots \dotplus \bar{C}_n$, where each $\bar{C}_i$ is cyclic. Let $B \subseteq C_i \subseteq A$ with $C_i/B = \bar{C}_i$. Then, by assumption, $C_i = B \dotplus X_i$ for some complementary subgroup X_i. If $X = X_1 + X_2 + \cdots + X_n$, then we claim that $A = B \dotplus X$. First, $\bar{A} = \bar{C}_1 \dotplus \bar{C}_2 \dotplus \cdots \dotplus \bar{C}_n$, implies that $A = C_1 + C_2 + \cdots + C_n = (B + X_1) + (B + X_2) + \cdots + (B + X_n) = B + X$. Second, if $a \in B \cap X$, then $a \in B$ and $a = x_1 + x_2 + \cdots + x_n \in X_1 + X_2 + \cdots + X_n$. Since $a \in B$, we have $\bar{a} = 0$, and then $0 = \bar{a} = \bar{x}_1 + \bar{x}_2 + \cdots + \bar{x}_n \in \bar{C}_1 \dotplus \bar{C}_2 \dotplus \cdots \dotplus \bar{C}_n$. Thus, each $\bar{x}_i = 0$, so $x_i \in B \cap X_i = 0$ and $a = x_1 + x_2 + \cdots + x_n = 0$. We conclude that $B \cap X = 0$ and hence that $A = B \dotplus X$.