Answers to the Algebra Qualifying Exam
January 1994

1. (i) Suppose $P \subseteq N \subseteq M \triangleleft G$. Then P is a Sylow p-subgroup of M, so the Frattini argument implies that $G = M\mathbb{N}_G(P) = MN = M$

(ii) Since $G' \triangleleft G$, we have $G' \cap N \triangleleft N$. Furthermore, G' is abelian, so $G' \cap N \triangleleft G'$. Thus $M = \mathbb{N}_G(G' \cap N) \supseteq \langle N, G' \rangle$. Now note that G/G' is abelian, so $M/G' \triangleleft G/G'$ and hence $M \triangleleft G$. But $M \supseteq N$, so part (i) implies that $M = G$, and hence $G' \cap N \triangleleft G$.

2. (i) Let $r \neq 0$ be a nonunit of R. Then rR is a nonzero ideal of R not containing 1, so rR is proper. Thus $rR \subseteq M$, where M is a maximal ideal and $M \neq 0$. But any maximal ideal is prime, so $M = P$ is the unique nonzero prime and $r \in P$, as required.

(ii) If Q is a nonzero ideal then, since R is Noetherian, the Lasker-Noether theorem implies that $Q = Q_1 \cap Q_2 \cap \cdots \cap Q_k$ is a finite intersection of primary ideals, each corresponding to a different prime. But there is only one nonzero prime, so $Q = Q_1$ is P-primary. The latter means that

$$\text{rad } Q = \sqrt{Q} = \{r \in R \mid r^m \in Q \text{ for some } m\} = P$$

so P/Q is a nil ideal. Again, since R is Noetherian, any nil ideal is nilpotent. Thus P/Q is nilpotent, and $P^n \subseteq Q$ for some integer n.

(iii) Assume that $P = (\pi)$ is the principal ideal generated by π. Let $0 \neq r \in R$, set $Q = rR = (r)$, and note that (ii) implies that $P^n \subseteq Q$ for some integer n. Let n be minimal with this property. Then $\pi^n \in rR$, so $\pi^n = rs$ for some ring element s. If s is a unit, then $r = s^{-1}\pi^n$ and we are done. If s is not a unit, then $s \in P$ by (i), so $s = \pi t$. Hence $\pi^n = rs = r\pi t$, so cancelling $\pi \neq 0$ in this domain yields $\pi^{n-1} = rt$. But then $P^{n-1} \subseteq rR$, and this contradicts the minimality of n.

3. Note that $(x^8 + x^4 + 1)(x^4 - 1) = x^{12} - 1$, so every root of f is a 12th root of unity. Furthermore, we have

$$\begin{aligned} x^{12} - 1 &= (x^6 - 1)(x^6 + 1) \\ &= (x^3 - 1)(x^3 + 1)(x^2 + 1)(x^4 - x^2 + 1) \\ &= (x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1) \\ &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) \end{aligned}$$

where $\Phi_n(x)$ is the nth cyclotomic polynomial. Thus

$$f(x) = \Phi_3(x)\Phi_6(x)\Phi_{12}(x) = (x^2 + x + 1)(x^2 - x + 1)(x^4 - x^2 + 1).$$

Of course, this can be verified directly. It follows that the splitting field E of f over $\mathbb{Q}$ is equal to $\mathbb{Q}[\epsilon]$, where ϵ is a primitive 12th root of unity. Thus $G = \text{Gal}(E/\mathbb{Q})$ is isomorphic to the multiplicative group of units of $\mathbb{Z}/12\mathbb{Z}$, that is $G = \{1, 5, 7, 11\}$. Furthermore, since

$$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12},$$

we see that G is an elementary abelian group of order 4 and $|E : \mathbb{Q}| = |G| = 4$. Finally, since the three cyclotomic factors of f are distinct irreducibles, G is transitive on the roots of each of these and hence G has three orbits on the roots of f.

4. If A is diagonalizable, we can assume it is diagonal. Then $K[A]$ consists of diagonal matrices and therefore this set contains no nonzero nilpotent matrix.

For the converse, let $f(x) = k_0 + k_1 x + \cdots + x^n$ be the minimal monic polynomial satisfied by A. Thus $0 = k_0 I + k_1 A + \cdots + A^n$ in $K[A]$, but no such expression of smaller degree in A is 0. Since K is algebraically closed, $f(x) = \prod_1^n (x - \alpha_i)$ factors into linear factors. Suppose that two of the roots of f are equal, say $\alpha_1 = \alpha_2$ and let $g(x) = f(x)/(x - \alpha_1) = \prod_2^n (x - \alpha_i)$. Note that $\deg g < \deg f$ and that $f(x)$ divides $g(x)^2$. It follows that $g(A) = \prod_2^n (A - \alpha_i I)$ is a nonzero element of $K[A]$ but that $g(A)^2 = 0$, and this cannot occur since $K[A]$ has no nonzero nilpotent elements. Thus the minimal polynomial of A has distinct roots and therefore A is diagonalizable.

5. (i) Suppose $g, h \in \mathrm{gp}(I)$. Then $1 - g$ and $1 - h$ are in the right ideal I, so $1 - g^{-1} = -(1 - g)g^{-1}$ and $1 - gh = (1 - g)h + (1 - h)$ are also in I. Thus g^{-1} and gh are in $\mathrm{gp}(I)$, so $\mathrm{gp}(I)$ is closed under inverses and products. Furthermore, $1 - 1 = 0 \in I$, so $1 \in \mathrm{gp}(I)$ and $\mathrm{gp}(I)$ is a subgroup of G.

(ii) Let $x \in G$ and $g \in \mathrm{gp}(I)$. Then $1 - g \in I \triangleleft \mathbb{Z}[G]$, so $1 - x^{-1}gx = x^{-1}(1 - g)x \in I$ and $x^{-1}gx \in \mathrm{gp}(I)$.

(iii) Finally, assume that I is a right ideal with $\mathrm{gp}(I) = G$. If $\alpha \in I$ and $g \in G = \mathrm{gp}(I)$, then $1 - g \in I$, so $g\alpha = \alpha - (1 - g)\alpha \in I$. This shows that I is closed under left multiplication by any $g \in G$. But every element of $\mathbb{Z}[G]$ is a $\mathbb{Z}$-linear sum of such groups elements, so we conclude that $\mathbb{Z}[G]I \subseteq I$.