Answers to the Algebra Qualifying Exam
August 1996

1. (a) It clearly suffices to assume that $N \cap M = 1$. Let A be a normal abelian subgroup of G. Then AN/N is a normal abelian subgroup of G/N, so it is central by $(*)$. Hence the commutator group $[AN, G]$ is contained in N and therefore $[A, G] \subseteq N$. Similarly, $[A, G] \subseteq M$, so $[A, G] \subseteq N \cap M = 1$ and A is central in G.

(b) Again, let A be a normal abelian subgroup of G and note, as above, that $[A, G] \subseteq N$. Indeed, since $A \triangleleft G$, we have $[A, G] \subseteq A$, so $[A, G]$ is abelian. Hence it is a normal abelian subgroup of N. The assumption on N now implies that $[A, G] = 1$ and therefore $A \subseteq \mathbb{Z}(G)$.

(c) Let G be a finite p-group with property $(*)$ and let $Z = \mathbb{Z}(G)$. If $G \neq Z$, then the nontrivial p-group G/Z has a central subgroup A/Z of order p. Then $A \triangleleft G$, $A \supseteq Z$ and A/Z is cyclic. The latter implies that A is abelian, and then $(*)$ implies that $A \subseteq Z$, a contradiction. Thus $G = Z$ is abelian.

2. (a) If $^- : R \to R/P$ is the natural homomorphism and if $x \in R$, then certainly $\bar{x}^n = \bar{x}$. In particular, if $\bar{x} \neq 0$, then since $\bar{R}$ is a domain, we have $\bar{x}^{n-1} = 1$. Thus $\bar{x}$ is invertible with inverse $\bar{x}^{n-2}$ and hence $\bar{R}$ is a field. Furthermore, all elements of $\bar{R}$ are roots of the polynomial $\zeta^n - \zeta$ and this polynomial has at most n roots. Thus $|\bar{R}| \leq n$.

(b) If N is the intersection of all prime ideals of R, then we know that N is the set of nilpotent elements of R. Now if $x \in R$ with $x^2 = 0$, then $0 = x^n = x$, since $n \geq 2$, so $x = 0$. This shows that there are no nontrivial nilpotent elements, and hence $N = 0$.

(c) If R is Noetherian, then it has only finitely many minimal primes, say these are $P_1, P_2, \ldots, P_k$. Furthermore, $\bigcap_1^k P_i = N = 0$ by the above, so R embeds in the direct sum of the rings R/P_i. Since each R/P_i is finite and $k < \infty$, we conclude that R is finite.

3. (a) Notice that $\beta = \alpha^3$ is a square root of -3. Furthermore, since $x^6 - 1 = (x^3-1)(x^3+1) = (x^3-1)(x+1)(x^2-x+1)$, the primitive 6th roots of 1 are $(1 \pm \sqrt{-3})/2 = (1 \pm \beta)/2$ and hence they belong to $E = \mathbb{Q}[\alpha]$.

(b) If $\omega \in E$ is a primitive 6th root of 1, then $E = \mathbb{Q}[\alpha]$ contains the set $\{\, \omega^i \alpha \mid i = 0, 1, \ldots, 5 \,\}$ of all roots of $x^6 + 3$. Furthermore, E is clearly generated over $\mathbb{Q}$ by these distinct roots, so $E/\mathbb{Q}$ is Galois. (Alternately, without noting that the roots are distinct, just observe that $E/\mathbb{Q}$ is normal and hence Galois since $\mathbb{Q}$ has characteristic 0.)

(c) Since $x^6+3 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion for the prime 3, it follows that $|E : \mathbb{Q}| = 6$. In particular, if G is the Galois group of this extension, then $|G| = 6$ and hence there are only two possibilities for the isomorphism class of G. It is either cyclic or the symmetric group of degree 3. Now note that G has at least two distinct elements of order 2, namely σ given by $\alpha \mapsto -\alpha$ and complex conjugation τ. These are clearly different since α is not purely imaginary. Hence G is not cyclic, so $G \cong \mathrm{Sym}_3$ and therefore G has three subgroups of order 2. It follows that there are precisely three intermediate fields F with $|E : F| = 2$, that is with $|F : \mathbb{Q}| = 3$.

4. (a) Since V is finite dimensional and $v \neq 0$, we can choose n maximal with $v, vT, \ldots, vT^{n-1}$ linearly independent. Thus $vT^n = a_0 v + a_1 vT + \cdots + a_{n-1} vT^{n-1}$ for suitable scalars a_i. If W is the subspace of V spanned by $v, vT, \ldots, vT^{n-1}$, then we see that $WT \subseteq W$. Thus $WT^k \subseteq W$ for all k, and therefore W contains all vT^k. But the latter vectors span V and therefore $W = V$. Hence $\mathcal{B} = \{ v, vT, \ldots, vT^{n-1} \}$ is a linearly independent set which spans V, so it is a basis. Furthermore, the matrix of T with respect to this basis has the required form since $vT^i \cdot T = vT^{i+1}$ for $0 \leq i \leq n-2$ and $vT^{n-1} \cdot T = \sum_0^{n-1} a_j (vT^j)$.

(b) Since $\{ v, vT, \ldots, vT^{n-1} \}$ is linearly independent, it is clear that if $vf(T) = 0$ for some nonzero polynomial f, then f must have degree $\geq n$. In particular, the minimal polynomial of T has degree $\geq n = \dim V$. But $n = \dim V$ is the degree of the characteristic polynomial of T, and this polynomial is divisible by the minimal polynomial. Thus the two monic polynomials have the same degree n and must be identical.

5. (a) Say $|E : F| = 3$. Then E is a 3-dimensional vector space over F. For each $e \in E$ let $T_e \colon E \to E$ denote right multiplication by e. Then T_e is an F-linear transformation, so by fixing a basis for E, we have $T_e \in \mathrm{M}_3(F)$. Furthermore, the map $\theta \colon e \mapsto T_e$ is easily seen to be an F-algebra homomorphism which is one-to-one. Thus $\theta(E)$ is a 3-dimensional subspace of $\mathrm{M}_3(F)$ and each nonzero member is invertible since $T_e T_{e^{-1}} = T_{e^{-1}} T_e = T_1 = I$, the identity matrix. Thus (i) implies (ii) and, of course, (ii) implies (iii) is trivial.

(b) Use the given notation. Since the characteristic polynomial of AB^{-1} has degree 3, if it is not irreducible, then it must have a linear factor. Thus AB^{-1} has an eigenvalue $\lambda \in F$ so $\lambda I - AB^{-1}$ is singular. Hence so is $(\lambda I - AB^{-1})B = \lambda B - A$, and this nontrivial linear combination of A and B is not invertible. Since A and B are F-linearly independent, $\lambda B - A \neq 0$.

Finally, suppose V is a 2-dimensional subspace of $\mathrm{M}_3(F)$ all of whose nonzero members are invertible and let $\{ A, B \}$ be a basis for V. By the above, the characteristic polynomial $f(x)$ of AB^{-1} must be irreducible over F. In particular, if α is a root of $f(x)$, then since $f(x)$ has degree 3, it follows that $E = F[\alpha]$ is a field extension of degree 3 over F. Thus (iii) implies (i), as required.