1. a. Suppose $G$ is a subgroup of $A = \text{Alt}_7$. Then $|A : G| = (7!/2)/(2^3 \cdot 3^2 \cdot 7) = 5$. By the $n!$-Theorem, $A$ must have a proper normal subgroup of index $\leq 5!$. But $A$ is simple and $|A| > 5!$, so this is a contradiction.

b. By the Sylow theorems, $n_3 \equiv 1(3)$ and $n_3 | 2^3 \cdot 7$. The possibilities are $n_3 = 1, 4, 7$ or 28. Since $G$ is simple, we cannot have $n_3 = 1$. If $n_3 = 4$, then the $n!$-Theorem implies that $G$ has a proper normal subgroup of index $\leq 4!$. But $G$ is simple and $|G| > 4!$, so this is impossible. Next, if $n_3 = 7$, then the $n!$-Theorem and the simplicity of $G$ imply that $G$ is embedded isomorphically in $S = \text{Sym}_7$. Furthermore, if $A = \text{Alt}_7$, then $A \triangleleft S$ implies that $(G \cap A) \triangleleft G$ with $|G : G \cap A| \leq 2$. Since $G$ is simple, we conclude that $G = G \cap A$, so $G \subseteq A$ and this contradicts the conclusion of part (a). Thus we can only have $n_3 = 28$.

2. a. We know that $M/M^2 \triangleleft R/M^2$ and that $(R/M^2)/(M/M^2) \cong R/M$ is a field since $M$ is maximal. Let $\theta: R/M^2 \to R/M$ denote the corresponding epimorphism. If $e$ is an idempotent in $R/M^2$, then $e(1-e) = 0$ implies that $\theta(e)\theta(1-e) = 0$. But $R/M$ has no zero divisors, so either $\theta(e) = 0$ or $\theta(1-e) = 0$. In the first case, we have $e \in \ker \theta = M/M^2$. But every element in $M/M^2$ has square 0, so $e = e^2 = 0$. On the other hand, if $\theta(1-e) = 0$ then, since $1 - e$ is also an idempotent, the above yields $1 - e = 0$ and hence $e = 1$.

b. Let $\sim: M \to M/M^2$ denote the natural $R$-module homomorphism. Since $R$ is Noetherian, $M$ is a finitely generated $R$-module, say $M = m_1 R + m_2 R + \cdots + m_k R$. Then $M/M^2 = M = \bar{m}_1 R + \bar{m}_2 R + \cdots + \bar{m}_k R$. But $M$ acts trivially on the module $M/M^2$, so this yields $M/M^2 = M = \bar{m}_1(R/M) + \bar{m}_2(R/M) + \cdots + \bar{m}_k(R/M)$ and $M/M^2$ is a finite-dimensional vector space over the field $R/M$.

c. If $R = K[x_1, x_2, \ldots, x_t]$, then the Hilbert Nullstellensatz implies that the field $R/M$ is a finite algebraic extension of $K$. In other words, $\dim_K R/M < \infty$. Furthermore, the Hilbert Basis Theorem implies that $R$ is Noetherian so, by (b), we know that $M/M^2$ is a finite-dimensional $R/M$-vector space. Thus $M/M^2$ is also a finite-dimensional $K$-vector space. Since $\theta: R/M^2 \to R/M$ is a $K$-linear transformation with kernel $M/M^2$, we conclude that $\dim_K R/M^2 = \dim_K M/M^2 + \dim_K R/M < \infty$.

3. a. Say $\alpha^m \in F$ with $m > 0$ and write $m = qn + r$ where $q$ and $r$ are nonnegative integers with $r < n$. Then $\alpha^r = \alpha^m/(\alpha^n)^q \in F$, so the minimality of $n$ implies that $r = 0$ and $n|m$.

b. Suppose $\text{char } F = p > 0$ and that $p|n$. Say $n = pt$. Then the minimality of $n$ implies that $\beta = \alpha^t \in E \setminus F$ and $\beta^p = \alpha^n \in F$. Now $\beta$ is a root of the polynomial $x^p - \beta^p \in F[x]$ and this polynomial is equal to $(x - \beta)^p \in E[x]$. Since $\beta \notin F$, the minimal polynomial of $\beta$ over $F$ must be a divisor of $x^p - \beta^p$ of degree larger than 1, and hence it has $\beta$ as a multiple root. In particular, $\beta$ is not separable over $F$, so $E$ is not separable over $F$ and this contradicts the assumptions.

c. Let $f(x) \in F[x]$ be the minimal monic polynomial of $\alpha$ over $F$ and suppose that $\deg f(x) = r$. Since $\alpha$ satisfies $x^n - \alpha^n \in F[x]$, it follows that $f(x)$ divides $x^n - \alpha^n$, so $r \leq n$ and each root of $f(x)$ in the algebraic closure of $E$ is of the form $\varepsilon \alpha$, where $\varepsilon$ is an
nth root of unity. In particular, the product of the \( r \) roots of \( f(x) \) must be equal to \( \delta \alpha^r \), where \( \delta \) is also an \( n \)th root of unity. Note that this product is plus or minus the constant coefficient of the polynomial \( f(x) \in \mathbb{F}[x] \) and hence it is contained in \( F \). In other words, \( \delta \alpha^r \in F \subseteq E \). Since \( \delta \alpha^r \in E \) and \( 0 \neq \alpha \in E \), we have \( \delta \in E \) and then, by assumption, \( \delta \in F \). With this, \( \delta \alpha^r \in F \) implies that \( \alpha^r \in F \), and the minimality of \( n \) yields \( r = n \). Since \( E = F[\alpha] \), we conclude that \( |E : F| = \deg f(x) = n \), as required.

4. a. Suppose \( A = \text{diag}(a_1, a_2, \ldots, a_n) \) and define the real diagonal matrices \( B = \text{diag}(b_1, b_2, \ldots, b_n) \) and \( C = \text{diag}(c_1, c_2, \ldots, c_n) \) as follows. If \( a_i > 0 \), set \( b_i = \sqrt{a_i} \) and \( c_i = 0 \), while if \( a_i \leq 0 \), set \( b_i = 0 \) and \( c_i = \sqrt{-a_i} \). Then for each \( i \), we have \( b_ic_i = 0 \) and \( a_i = b_i^2 - c_i^2 \), so \( BC = CB = 0 \) and \( A = B^2 - C^2 \).

b. Since \( A \) is a real symmetric matrix, we know that it has real eigenvalues and that it can be diagonalized by a real matrix. In other words, there exists a real invertible matrix \( P \) with \( P^{-1}AP \) a real diagonal matrix. By (a), we can write \( P^{-1}AP = U^2 - V^2 \) where \( U \) and \( V \) are real matrices satisfying \( UV = VU = 0 \). Set \( B = PUP^{-1} \) and \( C = PVP^{-1} \). Since conjugation is an algebra automorphism of the matrix ring, we then have \( A = B^2 - C^2 \) and \( BC = CB = 0 \).

c. Let \( v \neq 0 \) be a real eigenvector for \( B \) corresponding to the given real eigenvalue \( \lambda \neq 0 \). That is, \( Bv = \lambda v \) and \( v = \lambda^{-1}Bv \). Since \( CB = 0 \), we have \( Cv = C(\lambda^{-1}Bv) = \lambda^{-1}(CB)v = 0 \). In other words, \( v \) is also an eigenvector for \( C \), but with eigenvalue 0. Finally, \( Av = (B^2 - C^2)v = \lambda^2v - 0v = \lambda^2v \). Since \( v \neq 0 \), this says that \( \lambda^2 > 0 \) is an eigenvalue for \( A \) with \( v \) as a corresponding eigenvector.

5. a. \( DM(x^n) = D(x^{n+1}) = (n+1)x^n \) and \( MD(x^n) = M(nx^{n-1}) = nx^n \). Thus \( (DM - MD)(x^n) = (n+1)x^n - nx^n = x^n = I(x^n) \). Since \( DM - MD \) and \( I \) agree on the basis \( \{1, x, x^2, \ldots\} \), they are identical.

b. Suppose the set \( \{M^iD^j\} \) is \( K \)-linearly dependent. Then there are field elements \( a_{i,j} \) so that \( (*) \sum_{j=k}^{\ell} \sum_{i} a_{i,j} M^iD^j = 0 \) and \( a_{i,k} \neq 0 \) for some subscript \( i \). Note that \( D^k(x^k) = k! \) and hence \( D^j(x^k) = 0 \) for all \( j > k \). Thus, applying the expression \( (*) \) to \( x^k \) yields \( 0 = \sum_{i} a_{i,k} M^i(k!) = \sum_{i} k!a_{i,k}x^i \). But \( K \) has characteristic 0, so \( k! \) is not 0 in \( K \) and hence we must have \( a_{i,k} = 0 \) for all \( i \), a contradiction.

c. We proceed by induction on \( t \). If \( t = 0 \) then \( DM^t = D \) is certainly in the \( K \)-linear span of \( L \). Now suppose that the result holds for some \( t \geq 0 \). Then, by (a), \( DM^{t+1} = DM \cdot M^t = (I + MD) \cdot M^t = M^t + M \cdot DM^t \). It is clear that \( M^t \) is in the linear span of \( L \) and, by induction, so is \( DM^t \). Furthermore, from the nature of \( L \), it is clear that the span of \( L \) is closed under left multiplication by \( M \) and hence \( M \cdot DM^t \) is in this span. Consequently, so is \( DM^{t+1} = M^t + M \cdot DM^t \), and the induction step is proved.