August 1993
Algebra Qualifying Exam

1A) Determine all A that have distinct eigenvalues and $A^2 = 3A - 2I$.
Answer: $A^3 = 3A - 2I \implies (A - I)(A - 2I) = 0$ so the minimal polynomial is either $x - 1$, $x - 2$, or $(x - 1)(x - 2)$. In all 3 of these cases, the matrices are diagonalizable. Thus up to similarity the following are possibilities:

$$[1], \ [2], \text{ or } \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

1B) If $A = \begin{bmatrix} 6 & -2 \\ -2 & 3 \end{bmatrix}$, find an orthogonal matrix P such that $P^{-1}AP$ is diagonal.
Answer: A has eigenvalues coming from $(6 - x)(3 - x) - 4 = x^2 - 9x + 14 = (x - 2)(x - 7) = 0$ and thus we have eigenvalues of 2 and 7. The corresponding eigenvectors are $\frac{1}{\sqrt{5}}\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ and $\frac{1}{\sqrt{5}}\begin{bmatrix} -2 \\ 1 \end{bmatrix}$.

2A) Let $\alpha = \sqrt{3 + 2\sqrt{3}}$. Find the minimal polynomial for α, the Galois closure of $\mathbb{Q}(\alpha)$, and the Galois group of the Galois closure over $\mathbb{Q}$.
Answer: (a) $\alpha^2 = 3+2\sqrt{3}$ and so $(\alpha^2 - 3) = 2\sqrt{3}$ and so $(\alpha^2 - 3)^2 = 12$. Thus we have minimal polynomial $m_\alpha(x) = \alpha^4 - 6\alpha^2 - 3$. (b) $x = \pm\sqrt{3 \pm 2\sqrt{3}}$ and so $K = \mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}, \sqrt{3 - 2\sqrt{3}}\right)$. (c) We note that $m_\alpha(x)$ is irreducible by Eisenstein and so we will have Galois group $G \leq S_4$. For its size we have that

$$\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}\right) \leq \mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}, \sqrt{3 - 2\sqrt{3}}\right)$$

with

$$\begin{aligned} & \left[\mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}, \sqrt{3 - 2\sqrt{3}}\right) : \mathbb{Q}\right] \\ = & \left[\mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}, \sqrt{3 - 2\sqrt{3}}\right) : \mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}\right)\right]\left[\mathbb{Q}\left(\sqrt{3 + 2\sqrt{3}}\right) : \mathbb{Q}\right] \\ = & \ 2 \cdot 4 = 8 \end{aligned}$$

As $m_\alpha(x)$ has two real roots and two complex nonreal roots we know that we have a four cycle and a 2 cycle. These generate the group and one can show that it is isomorphic to the dihedral group of order 8.

2B) Let $f(x) = x^3 - 2$. Find the Galois groups over
(a) $\mathbb{Q}$
(b) $\mathbb{F}_7$
(c) $\mathbb{F}_9$
Answer: (a) The splitting field is $\mathbb{Q}\left(\sqrt[3]{2}, i\right)$ which is degree 6 and so $G = S_3$. (b) By direct calculation $f(0) = 5$, $f(1) = 6$, $f(2) = 6$, $f(3) = 4$, $f(4) = 6$, $f(5) = 4$, and $f(6) = 4$ we know that $f(x)$ is irreducible. $f(x)$ splits over $\mathbb{F}_7[x] / \langle x^3 - 2\rangle$ and as this is a degree 3 extension we know that $G = \mathbf{Z}_3$.
(c) Over $\mathbb{F}_3$ we have that $x^3 - 2 = x^3 + 1 = (x + 1)(x + 1)(x + 1) = x^3 + 3x^2 + 3x + 1 = x^3 + 1$. And so $G = \{1\}$ is trivial.

3A) Show that a finite group G generated by a and b of both order 2 is dihedral of order $2m$ for some $m \in \mathbb{Z}^+$.
Answer: Recall that $D_m = \langle \sigma, \tau : \sigma^m = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1}\rangle$. First we note that as G is a finite group there is some $m \in \mathbb{Z}$ such that $(ab)^m = 1$. Also $a^2 = b^2 = 1$. Let $ab = \sigma$ and $b = \tau$. Then $\sigma^m = \tau^2 = 1$. Now we need to check the other relation.

$$\sigma\tau = abb = a = b(ba) = \tau\sigma^{-1}.$$

3B) How many groups are there of order 63?
Answer: 4 (2 abelian and 2 nonabelian). We prove this by first considering the following facts:

i) Let H and K be subgroups of G. The number of distinct ways of writing each element of the set HK in the form hk, $h \in H$ and $k \in K =$ is $|H \cap K|$. If $|H \cap K| = 1$ then it is unique. ($|HK| = \frac{|H|\,|K|}{|H \cap K|}$).

ii) If H and K are normal in G and $H \cap K = 1$ then $HK \cong H \times K$, the direct sum.

iii) Let H and K be groups and let φ be a homomorphism from K into $Aut\,(H)$. Let $\cdot$ denote the (left) action of K on H determined by φ. Let G be the set of ordered pairs (h,k) with $h \in H$ and $k \in K$ and define the multiplication on G :

$$(h_1,k_1)\,(h_2,k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

This muliplication makes G into a group of order $|G| = |H|\,|K|$. It also makes $H \lhd G$ and $H \cap K = 1$. For all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

iv) Suppose G is a group with subgroups H and K such that $H \lhd G$ and $H \cap K = 1$. Let $\varphi : K \to Aut\,(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular if $G = HK$ with H and K satisfying $H \lhd G$ and $H \cap K = 1$, then G is the semidirect product of H and K.

Proof: As $H \lhd G$ we know that $HK \leq G$. Every element of HK can be written uniquely by (i) in the form hk for some $h \in H$ and $k \in K$. Thus the map $kh \to (h,k)$ is a set bijection from HK onto $H \rtimes K$. Check that this is a homomorphism. Thus as it is one-to-one and onto, it is an isomorphism.

Now we can prove our results. As $63 = 3^2 7$ we know that by the Sylow theorems there is a unique Sylow 7-subgroup of order 7. There are either 1 or 7 Sylow 3-subgroups. The Sylow 3-subgroups have size 9 and are either $\mathbb{Z}_9$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. The the Sylow 7-subgroup is normal as it is unique. $Aut\,(Syl\,(7)) \cong \mathbb{Z}_6$. The possible group homomorphisms from the Sylow 3-subgroups are the trivial (for both) which gives the direct product (this is the case where there is one Sylow 3-subgroup).

$$\begin{array}{ccl} \mathbb{Z}_9 & \to & \mathbb{Z}_6 \text{ both cyclic so possibilities are} \\ 1 & \mapsto & 0 \\ 1 & \mapsto & 3 \end{array}$$

Thus for any $a \in \mathbb{Z}_6$ we would have the three corresponding actions of $x \cdot a \mapsto a$ (trivial action which gives direct product) or $x \cdot a \mapsto 3a$ or Note that $5a = a^{-1}$ and so the action by conjugation is the same. So the only semidirect product we have is where $(h_1 k_1) + (h_2 k_2) = (h_1 + 3h_2, k_1 + k_2)$. Similarly for the Sylow 3-subgroup $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Thus there are a total of four, $\mathbb{Z}_9 \oplus \mathbb{Z}_7$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$, $\mathbb{Z}_7 \rtimes \mathbb{Z}_9$, and $\mathbb{Z}_7 \rtimes (\mathbb{Z}_3 \oplus \mathbb{Z}_3)$.

4A) $R = \mathbb{C}\,[x,y]$.

(a) Find a maximal ideal that does not contain xy.

(b) Find a prime ideal that is not maximal that does not contain xy.

Answer: (a) $\langle x - i, y + i \rangle$ (b) $\langle x + y \rangle$

4B) If A is a finitely generated $\mathbb{Z}$-module, describe $R \otimes_{\mathbb{Z}} A$ as completely as possible.

Answer: $A \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}^m$ where $n_i | n_{i+1}$ and m is the torsion free rank. Thus

$$\begin{aligned} R \otimes_{\mathbb{Z}} A &\cong R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}^m \\ &\cong R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_1} \times R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_2} \times ... \times R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_s} \times R \otimes_{\mathbb{Z}} \mathbb{Z}^m \\ &\cong R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_1} \times R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_2} \times ... \times R \otimes_{\mathbb{Z}} \mathbb{Z}_{n_s} \times R^m \\ &\cong R/n_1 R \times \cdots \times R/n_s R \times R^m \text{ (last step is hw prob Grove \#40 ch.4)} \end{aligned}$$

5A) (a) If R is a commutative ring, show that the set of nilpotent elements of R is an ideal in R.

(b) Prove or disprove: If R is an arbitrary ring, then the set of nilpotent elements is an ideal.

Answer: (a) $I = \{a : a^n = 0\}$ is an ideal. Let $a, b \in I$ then there is an m, n such that $a^m = b^n = 0$. Then we use the binomial expansion theorem we have that $(a-b)^{m+n} = 0$. Thus $a - b \in I$. Now take an arbitrary $r \in R$. Then $(ra)^m = r^m a^m = r^m 0 = 0$.

(b) Counterexample: Take $M_2(\mathbb{R})$ and let $x = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $y = \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}$. Then $x - y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $(x-y)^n \neq 0$ for all n. This is an element of order 2 which is just a reflection and so odd powers keep $x - y$ as $x - y$ and even powers give the identity matrix.

5B) Show that an ID with 1 satisfying the DCC (descending chain condition) for ideals must be a field.

Answer: Let $I = \langle x \rangle \trianglelefteq R$ be an ideal. Then as R is Artinian (DCC) we have $I \geq I^2 \geq I^3 \geq \cdots$ must terminate. So there is an n such that for all $k \geq n$ we have $I^n = I^k$. If $I^n = \langle x \rangle^n = \langle x^n \rangle = 0$ then we have that $x^n = 0$ but it cannot as R is an ID. If $I^n = I^{n+k}$ then in particular $I^n = I^{n+1}$. So $\langle x^n \rangle = \langle x^{n+1} \rangle$ and so there is an $r \in R$ such that $x^n = rx^{n+1}$ implies that $1 = rx$ and so $x \in U(R)$. Thus $\langle x \rangle = R$ for all $x \neq 0 \in R$ and so R is a field.