August 2004
Algebra Qualifying Exam

1A) Let $T : \mathbb{C}^5 \longrightarrow \mathbb{C}^5$ be a linear transformation whose characteristic polynomial is $-x^5+x^3$. List all possible Jordan canonical forms of T.
Answer: We know that $-(x^5 - x^3) = -x^3(x^2 - 1) = -x^3(x + 1)(x - 1)$. The first possibility is that of the matrix with invariant factor $x^3(x + 1)(x - 1)$. This is

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

The other possible invariant factors are $x, x^2(x + 1)(x - 1)$ and $x, x, x(x + 1)(x - 1)$

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

1B) Suppose A is a real symmetric matrix with the property that each negative eigenvalue has even multiplicity. Show that A has a (real) square root B (i.e. $B^2 = A$).
Answer: Consider the Jordan Canonical Form of A which exists as a real symmetric matrix has real eigenvalues. It is diagonalizable and even more so can be done with an orthogonal basis. (Look up this proof in standard linear algebra text). Thus the JCF of this matrix is diagonal. So all we need to show is that a $2n \times 2n$ diagonal block has a root (which is just a scalar multiple of the identity, cI_{2n} where $c < 0$). We reduce the problem even further by noting that for $c < 0$ we have that $cI_{2n} = \sqrt{|c|}^2(-I_{2n})$. Thus we need to find a square root of $-I_{2n}$.

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

In the 4×4 case we have that

$$\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

And thus we take a matrix with n diagonal blocks of $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

2A) Prove that a group of order 1806 has a normal subgroup of order 903.
Answer: First we factor $1806 = 2 \cdot 3 \cdot 7 \cdot 43$ Let L, P, Q, R be the Sylow p-subgroups of G for $l, p, q, r = 2, 3, 7$ and 43 respectively.

By the Sylow Theorems, there is only one Sylow 43–subgroup (Note $43k+1$ divides $2\cdot 3\cdot 7$ and so $k=0$), so R is normal.
Then We prove that LR, PR, QR are subgroups of G as follows:
Fact: If $A\leq G$ and $B\lhd G$ then $A\cap B\lhd A$ and $AB\leq G$.
Solution: Obviously $A\cap B\leq A$. To prove its normality, let $a\in A$, $x\in A\cap B$. Then $axa^{-1}\in B$ as $B\lhd G$. Trivially, $axa^{-1}\in A$. Thus, for all $a\in A$ and $x\in A\cap B$ we have $axa^{-1}\in A\cap B$ and so $A\cap B\lhd A$. To prove $AB\leq G$ let a and $a_1\in A$, $b,b_1\in B$. Then $(ab)(a_1b_1)^{-1}=abb_1^{-1}a_1^{-1}\in AB$ because $\left(bb_1^{-1}\right)a_1^{-1}=a_1^{-1}b_2$ for some $b_2\in B$.

Thus if we have a subgroup of order 903 then it is normal by the following:
Fact: Any index two subgroup is normal.
Proof: Let $H\leq G$ such that $[G:H]=2$. If $a\notin H$ then by hypothesis $G=H\cup aH$ and $AH\cap H=\emptyset$. Also, $G=H\cup Ha$ with $Ha\cap H=\emptyset$. Thus, $aH=Ha$, $a\notin H$. But clearly $aH=Ha$ for all $a\in H$. Thus for all $g\in G$, $gH=Hg$ proving that H is normal in G.

Okay, these are nice facts, to use for another day, but 301 is not prime as I have recently learned. Now consider the following facts: For references see Dummitt Foote p.107 (ed II) or Grove Thm 5.4:

(1) Suppose $K\lhd G$. Then G is solvable if and only if both K and G/K are solvable. (Grove)

(2) The finite group G is solvable if and only if for every divisor n of $|G|$ such that $\left(n,\frac{|G|}{n}\right)=1$, G has a subgroup of order n. (Due to P. Hall, generalization of Sylow).

We know that the Sylow 43-subgroup S is normal in G and is solvable as it is abelian. Now consider G/S. The order of G/S is 42. We show this is solvable. Consider that in G/S the Sylow 7-subgroup is unique and thus normal and as abelian is solvable. Thus $(G/S)/Sylow\ 7$ has size 6. And any group of size 6 is solvable. So working backwards we know that S and G/S are solvable and so G is solvable.

Conisder $\left(903,\frac{1806}{903}\right)=1$ and thus G has a subgroup of order 903. It is normal by above argument for index 2. (This is the hammer to smash an ant technique)

Another way to consider this problem is as follows: We know that $n_{43}=1$ and so $Syl(43)\lhd G$. Now consider the Sylow 7-subgroup. Then $n_7=1,8,15,22,29,36,...,7k+1$. We also know that $n_7|2\cdot 3\cdot 7\cdot 43$. If $n_7=1$ then $Syl(7)\lhd G$ and so $Syl(3)\cdot Syl(7)\leq G$ as $Syl(7)$ is normal and thus as $Syl(43)$ is normal we have $Syl(3)\cdot Syl(7)\cdot Syl(43)\leq G$. If $n_7\neq 1$ then the only other possibility is $n_7=43$. Thus we know that $[G:N_G(Syl(7))]=43$, the index of the normalizer of the Sylow 7-subgroup in G. Thus $|N_G(Syl(7))|=42$. Thus as $N_G\leq G$ we know that there is a Sylow 3-subgroup subgroup, $Syl(3)\leq N_G(Syl(7))$. Thus we know that $Syl(3)Syl(7)\leq G$ (Grove Theorem 2.6 Isomorphism theorem). Thus there is a subgroup of Size 21 in G, call it Q. Thus as $R=Syl(43)\lhd G$ we have that $QR=RQ\leq G$. As $|QR|=903$ it is a normal subgroup.

2B) List up to isomorphism, all the abelian groups of order 9. For any two such groups G_1 and G_2, determine the order of the group $Hom(G_1,G_2)$.
Answer: By the fundamental theorem of finite abelian groups, there are two groups (up to isomorphism) of order 9

$$\mathbb{Z}_9 \text{ and } \mathbb{Z}_3\oplus\mathbb{Z}_3$$

For $Hom(\mathbb{Z}_9, \mathbb{Z}_9)$ we need only consider possible images of a generator $\bar{1}$. We can have the following: $\bar{1} \to 0$, $\bar{1} \to \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$, or $\bar{8}$. Thus $|Hom(\mathbb{Z}_9, \mathbb{Z}_9)| = 9$. For $Hom(\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3)$ we know that $Hom(\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3) \cong Hom(\mathbb{Z}_9, \mathbb{Z}_3) \oplus Hom(\mathbb{Z}_9, \mathbb{Z}_3)$.We have that $\bar{1} \to (\bar{0}, \bar{0})$, $\bar{1} \to (\bar{0}, \bar{1})$, $\bar{1} \to (\bar{1}, \bar{0})$, $\bar{1} \to (\bar{1}, \bar{1})$, $\bar{1} \to (\bar{0}, \bar{2})$, $\bar{1} \to (\bar{2}, \bar{0})$, $\bar{1} \to (\bar{2}, \bar{1})$, $\bar{1} \to (\bar{1}, \bar{2})$, $\bar{1} \to (\bar{2}, \bar{2})$. The order of the group is nine, or we see that $|Hom(\mathbb{Z}_9, \mathbb{Z}_3)| = 3$ and so we also know that it is $3 \cdot 3 = 9$. Thus $|Hom(\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3)| = 9$. For $Hom(\mathbb{Z}_3 \oplus \mathbb{Z}_3, \mathbb{Z}_9) \cong Hom(\mathbb{Z}_3, \mathbb{Z}_9) \oplus Hom(\mathbb{Z}_3, \mathbb{Z}_9)$ we have to send the generator of $\mathbb{Z}_3$ to an element of order 3 in $\mathbb{Z}_9$. The only choices are $0, 3$, and 6. Thus $|Hom(\mathbb{Z}_3, \mathbb{Z}_9)| = 3$ and thus $|Hom(\mathbb{Z}_3 \oplus \mathbb{Z}_3, \mathbb{Z}_9)| = 9$. Lastly, we have that

$$Hom(\mathbb{Z}_3 \oplus \mathbb{Z}_3, \mathbb{Z}_3 \oplus \mathbb{Z}_3) \cong Hom(\mathbb{Z}_3, \mathbb{Z}_3)^4$$

Thus the order is 3^4. Another way to think of this last one is all 2×2 matrices over $\mathbb{Z}_3$ of which there are 81.

3A) Let S be a subring of $\mathbb{R}$ with unit. We assume that for any $x \in S$ there is $\varepsilon > 0$ such that $S \cap (x - \varepsilon, x + \varepsilon) = \{x\}$. Show that S is $\mathbb{Z}$.
Answer: Suppose there is a $y \in S$ such that $y \notin S$. Consider $\lceil y \rceil = N \in S$. Then $N - y \in S$ and $N - y < 1$. For any $k \in \mathbb{Z}$ we have $(N - y)^k \in S$. Given any $\varepsilon > 0$ there is a k such that $(N - y)^k < \varepsilon$. Let $x \in S$. Assume we are given $\varepsilon > 0$. There is a k such that $x - (N - y)^k \in (x - \varepsilon, x + \varepsilon)$. Thus $S \cap (x - \varepsilon, x + \varepsilon) \neq \{x\}$ and we have a contradiction.

3B) Let R be a commutative ring with 1 that satisfies the descending chain condition for ideals. Show that every element of R is either a unit or a zero divisor. (Hint: If not, choose $r \in R$ such that r is neither a unit nor a zero divisor, and with $\langle r \rangle$ minimal in that respect. Consider $\langle r^2 \rangle$.)
Answer: Take any nonzero $r \in R$. Consider the descending chain or ideal

$$\langle r \rangle \supseteq \left\langle r^2 \right\rangle \supseteq \cdots \supseteq \langle r^n \rangle$$

We know there is some n such that for all $k \geq n$ we have $\langle r^n \rangle = \left\langle r^k \right\rangle$ and more specifically that $\langle r^n \rangle = \langle r^{n+1} \rangle$. Assume that r is not a zero divisor. Then we have that $r^n = ar^{n+1}$ for some $a \in R$. Thus as r is not a zero divisor we get that $1 = ar$ and thus we have found an inverse for r.

4A) Determine the Galois group of the following polynomial $f(x) = x^3 + x + 1$.
Answer: If we reduce $f(x)$ mod 2 then we see that $f(0) = f(1) = 1$ and know that f is irreducible. Next we note that $f'(x) = 3x^2 + 1$ and so has no local maximum or minimum. Therefore there is only one real zero and two nonreal complex roots. Therefore we have a two cycle and a three cycle and therefore generate all of S_3.

4B) Let K be the splitting field of the polynomial $x^4 - 3$ over $\mathbb{Q}$. Prove that $[K : \mathbb{Q}] = 8$ and K is generated by by a single root α of the polynomial. Then show that the Galois group $Gal(K/\mathbb{Q})$ is non-abelian.
Answer: First we note that $x^4 - 3$ is irreducible by the Eisenstein criterion with $p = 3$. We know that $\sqrt[4]{3}$ is a root of the polynomial as $\left(\sqrt[4]{3}\right)^4 - 3 = 0$. We know that $\mathbb{Q}\left(\sqrt[4]{3}\right)$ has $\left[\mathbb{Q}\left(\sqrt[4]{3}\right) : \mathbb{Q}\right] = 4$. Over $\mathbb{Q}\left(\sqrt[4]{3}\right)$, we have that

$$\begin{aligned} x^4 - 3 &= \left(x^2 - \sqrt{3}\right)\left(x^2 + \sqrt{3}\right) \\ &= \left(x + \sqrt[4]{3}\right)\left(x - \sqrt[4]{3}\right)\left(x + i\sqrt[4]{3}\right)\left(x - i\sqrt[3]{4}\right) \end{aligned}$$

Thus the splitting field is $\mathbb{Q}\left(\sqrt[4]{3}, i\right)$ and has degree

$$\left[\mathbb{Q}\left(\sqrt[4]{3}, i\right) : \mathbb{Q}\left(\sqrt[4]{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{3}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8$$

We also note that $x^4 - 3$ has two real and two nonreal complex roots. One element of the Galois group is complex conjugation. Another is the 4 cycle of all of the roots. However, the complex conjugation does not commute with the 4 cycle. The group is isomorphic to D_8, the dihedral group of order 8.

5A) Let $S = \mathbb{R}[x, y, z]$ and let M be the ideal of S generated by x, y, z. Show that M is not a free S-module. Can M be generated by two elements?
Answer: First we note that if M is free the basis would have size at least 2. For if b is a basis for M then we have that $f(x, y, z)\, b = x$ and $g(x, y, z)\, b = y$ and $h(x, y, z)\, b = z$. As z is an irreducible polynomial this is only possible for $b = z$ and $h(x) = 1$ (or scalar multiples). But then it is not possible to write $f(x)\, z = x$. Thus the basis must be at least of size two. Thus if it has size ≥ 2 then we know that there are $f_1(x, y, z)$ and $f_2(x, y, z)$, ... such that $M \cong S^n = \langle f_1 \rangle R \oplus \langle f_2 \rangle R \oplus \cdots$ but we know that $\langle f_1 \rangle \cap \langle f_2 \rangle \neq 0$ as $f_2 f_1 \in \langle f_1 \rangle$ and $f_1 f_2 \in \langle f_2 \rangle$.

5B) Decompose the abelian group with presentation

$$A = \langle a, b, c : 4a + 8b + 12c = 8a - 4b + 16c = 0 \rangle$$

into a product of cyclic groups.
Answer: We use the relations and do a smith normal form computation.

$$\begin{pmatrix} 4 & 8 & 12 \\ 8 & -4 & 16 \end{pmatrix} \longrightarrow \begin{pmatrix} 4 & 8 & 12 \\ 0 & -20 & -8 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & -20 & -8 \end{pmatrix} \longrightarrow \begin{pmatrix} 4 & 0 & 0 \\ 0 & -8 & -20 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 8 & 20 \end{pmatrix} \longrightarrow \begin{pmatrix} 4 & 0 & 0 \\ 0 & 8 & 4 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$$

Thus $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}$ as it has one free generator.