January 2005
Algebra Qualifying Exam

1A) If $A = \begin{bmatrix} 1 & 4 & -2 \\ 4 & 1 & -2 \\ -2 & -2 & -2 \end{bmatrix}$ find an orthogonal matrix P so that $P^{-1}AP$ is diagonal.

Answer: First we note that this is a symmetric matrix and thus has real eigenvalues. Next we compute the eigenvalues.

$$\begin{vmatrix} 1-x & 4 & -2 \\ 4 & 1-x & -2 \\ -2 & -2 & -2-x \end{vmatrix} = (1-x)\left[(1-x)(-2-x)-4\right]$$
$$-4\left[4(-2-x)-4\right]+(-2)\left[-8+2(1-x)\right]$$
$$= -\left(x^3-27x-54\right)$$

We see that -3 is a root. Thus $x^3-27x-54=(x-6)(x+3)(x+3)$. Thus we have eigenvalues 6 and -3 (mult.2). We solve for the eigenvectors and get $(1,1,-1/2)$, $(1,0,2)$, and $(0,1,2)$. Thus

$$\begin{bmatrix} 6 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1/2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{bmatrix} A \begin{bmatrix} 4/9 & 5/9 & -4/9 \\ 4/9 & -4/9 & 5/9 \\ -2/9 & 2/9 & 2/9 \end{bmatrix}$$

However, we also need that P is orthogonal. In our case we need that $AA^T=I$. Thus we need to do the gram-schmidt orthogonalization process to our eigenvectors. Final answer:

$$\begin{pmatrix} \frac{\sqrt{5}}{5} & \frac{-4\sqrt{5}}{25} & \frac{2}{3} \\ 0 & \frac{\sqrt{5}}{5} & \frac{2}{3} \\ \frac{2\sqrt{5}}{5} & \frac{2\sqrt{5}}{25} & -\frac{1}{3} \end{pmatrix}$$

1B) Let F be a field. Let $\beta := \{e_1, e_2, e_3\}$ be the standard basis of F^3. Let $T : F^3 \to F^3$ be the linear transformation such that $T(e_1)=0$, $T(e_2)=e_1$, and $T(e_3)=e_2+e_3$. Find all linear transformations $U : F^3 \to F^3$ such that we have $UT=0$ and the range of TU is $R(TU)=\{\alpha e_1 : \alpha \in F\}$.

Answer: As we have chosen a matrix, we may write down a linear transformation as a matrix

$$Tv = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}$$

Now we need to find U:

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Thus $x_{11}=0$, $x_{21}=0$, $x_{31}=0$ and $x_{12}+x_{13}=0$, $x_{22}+x_{23}=0$, $x_{32}+x_{33}=0$. Thus we have the matrix

$$\begin{bmatrix} 0 & x_{12} & -x_{12} \\ 0 & x_{22} & -x_{22} \\ 0 & x_{32} & -x_{32} \end{bmatrix}$$

However we must satisfy the last requirement also:

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & x_{12} & -x_{12} \\ 0 & x_{22} & -x_{22} \\ 0 & x_{32} & -x_{32} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{pmatrix} 0 & x_{22} & -x_{22} \\ 0 & x_{32} & -x_{32} \\ 0 & x_{32} & -x_{32} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}$$

and thus $R(TU)=\{\alpha e_1\}$ if $x_{32}=-x_{32}=0$. And so our final answer is

$$\begin{pmatrix} 0 & x_{22} & -x_{22} \\ 0 & x_{32} & -x_{32} \\ 0 & 0 & 0 \end{pmatrix}$$

2A) If G is a nonabelian group show that the center $Z=Z(G)$ of G is properly contained in an abelian subgroup of G.
Answer: Take $x \notin Z$. We know there is such an x as G is nonabelian. Now consider the group ZH where $H=\langle x\rangle$, the cyclic group generated by x. We know that ZH is a subgroup as Z is a normal subgroup. Now we need to show that it is abelian. We know that $ZH=\{zh : z \in Z \text{ and } h \in H\}$. Now take $x,y \in ZH$. We need to show that $xy=yx$. We know that $xy=(z_1h_1)(z_2h_2)=(z_1z_2h_1h_2)=(z_1z_2h_2h_1)=z_2z_1h_2h_1=z_2h_2z_1h_1=yx$ as all elements of H commute with each other as it is abelian and all elements of Z commute with everything.

2B) List at least 9 groups of order 16 that are not pairwise isomorphic.
Answer: First we consider the abelian groups of a group G with $|G|=2^4$. These groups are thus

$$\mathbb{Z}_{16},\ \mathbb{Z}_8 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4 \oplus \mathbb{Z}_4,\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Thus we have 5 so far. Then we have the dihedral group of order 16, the generalized quaternion group of order 16, $D_8 \times \mathbb{Z}_2$, $Q_8 \times \mathbb{Z}_2$.

3A) Let $m,n \in \mathbb{Z}\backslash\{0,1\}$ be distinct square free integers. Show that the rings R_m and R_n are not isomorphic.
Answer: We just consider the case when $m,n \equiv 2,3$ and leave 1 as a similar exercise. Assume that $m \neq n$. Conisder any ring homomorphism from $R_m \to R_n$. We know that $0 \mapsto 0$. Also we have that $1 \mapsto 1$. This is true as $\varphi(1)=\varphi(1^2)=\varphi(1)\varphi(1)$ and thus must be 1 or 0. Thus $\varphi(m)=\varphi(1+\cdots+1)=\varphi(1)+\cdots+\varphi(1)=m$ or 0. Now we consider the fact that $\varphi(m)=\varphi\left(m^{1/2}m^{1/2}\right)=\varphi\left(m^{1/2}\right)\varphi\left(m^{1/2}\right)$. The image of $m^{1/2}$ is of the form $a+b\sqrt{n}$ for integers a and b. Thus $\varphi(m)=(a+b\sqrt{n})(a+b\sqrt{n})=a^2+2ab\sqrt{n}+b^2n=m$. Thus either a or $b=0$ as $\sqrt{n}$ is square free and m is an integer. If $a=0$ then $m=b^2n$ but this is not possible as $b^2|m$ and m is square free. If $b=0$ then $m=a^2$ which is also not possible. Thus they cannot be isomorphic.

3B) If D is a division ring set $G=D\backslash\{-1\}$. If $a,b \in G$ define $a*b=ab+a+b$. Show that $*$ is a binary operation on G and show that $(G,*)$ is a group.

Answer: To show that $*$ is a binary operation we must show that the operation is closed as a binary operation is a operatornametion $* : G \times G \to G$. Consider $a, b \in G$. Then we need to check that $ab + a + b \neq -1$. Assume that $ab + a + b = -1$. This implies that $a(b+1) + b = -1$ which implies that $a(b+1) = -1 - b = -(b+1)$ and thus $a = -1$. This is a contradiction as we have assumed that $-1 \notin G$. Next we show that it is a group.

- $a * 0 = 0 + a + 0 = a = 0 * a$ and thus 0 is the identity.
- We need b such that $a * b = 0$. Take $b = (a+1)^{-1}(-a)$ and see that

$$\begin{aligned} a * b &= a(a+1)^{-1}(-a) + a + (a+1)^{-1}(-a) \\ &= (a+1)(a+1)^{-1}(-a) + a = -a + a = 0 \end{aligned}$$

  Similarly, for $b * a$.

- Lastly, we show associativity:

$$\begin{aligned} a * (b * c) &= a * (bc + b + c) = abc + ab + ac + a + bc + b + c \\ &= abc + ac + bc + a + b + c = (ab + a + b)c + (a + b) + c \\ &= (a * b) * c \end{aligned}$$

4A) List all monic irreducible polynomials $f(x) \in \mathbb{F}_4[x]$ that have degree 3.
Answer: We let $\mathbb{F}_4$ be the field with the 4 element set $\{0, 1, t, t+1\}$ such that $t^2 + t + 1 = 0$. A degree 3 polynomial is one such that $x^3 + ax^2 + bx + c$ is irreducible with $a, b, c \in \mathbb{F}_4$. Clearly $c \neq 0$ or we have a reducible linear factor of x. For the others, we first eliminate polynomials that are reducible over $\mathbb{F}_2$. These include

$$\begin{aligned} &x^3 + x^2 + x + 1,\ x^3 + tx^2 + tx + 1,\ x^3 + (t+1)x^2 + (t+1)x + 1, \\ &x^3,\ x^3 + x^2,\ x^3 + x^2 + x,\ x^3 + x,\ x^3 + 1,\ x^3 + x^2 + (t)x + t, \\ &x^3 + tx^2 + x + t,\ x^3 + (t+1)x^2 + x + t + 1, \end{aligned}$$

If f is irreducible over $\mathbb{F}_4[x]$ then $\mathbb{F}_4[x]/(f)$ is a field isomorphic to $\mathbb{F}_{64}$. We know that any finite field F with $p^n = 2^6$ elements is the splitting field of $x^{2^6} - x \in F_p[x]$. The polynomial $x^{p^n} - x$ is precisely the product of all distinct polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all divisors of n. This proposition can be used to produce irreducible polynomials over $\mathbb{F}_p$ recursively. For example the irreducible quadratics over $\mathbb{F}_2$ are the divisors of

$$\frac{x^4 - x}{x(x-1)}$$

which gives the single polynomial $x^2 + x + 1$. Similarly, the irreducible cubics over this field are divisors of

$$\frac{x^8 - x}{x(x-1)} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

which factors into the two cubis $x^3 + x + 1$ and $x^3 + x^2 + 1$. The irreducible quartics are given by dividing $x^{16} - x$ by $x(x-1)$ and the irreducible quadratic $x^2 + x + 1$ above and then factoring into irreducible quartics:

$$\frac{x^{16} - x}{x(x-1)(x^2 + x + 1)} = (x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$$

Now we try to adapt this for our needs. Thus the 4 irreducible degree 1 polynomials are x, $x+1$, $x+t$, and $x+t+1$ where $\mathbb{F}_4 = \{0,1,t,t+1\}$ where $t^2+t+1=0$, i.e. t is a root of x^2+x+1. Then we see that $x(x+1)(x+t)(x+t+1) = x^4+x$ (as expected). So our degree 3 irreducibles should be

$$\frac{x^{4^3}+x}{x^4+x} = x^{60}+x^{57}+\cdots+x^3+1$$

Thus there will be 20 irreducibles of degree 3. Now we write down some of the ones we know for sure and then divide them out of the product.

$$\begin{aligned} f_1 &= x^3+x+1 \\ f_2 &= x^3+tx+1 \\ f_3 &= x^3+(t+1)x+1 \\ f_4 &= x^3+tx^2+1 \\ f_5 &= x^3+x^2+1 \\ f_6 &= x^3+(t+1)x^2+1 \end{aligned}$$

Check: $f_1(0)=1$, $f_1(1)=1$, $f_1(t)=t^3+t+1=t(t^2)+t+1=t(t+1)+t+1=1$ and $f_1(t+1)=1$. Similarly for the others. Divide these out of x^{60} and continue. Or maybe there is a faster way. The final answer is:

x, $x+1, x+t$, $x+t+1$,
x^3+t, x^3+t+1, x^3+x+1, x^3+tx+1,
$x^3+(t+1)x+1$, x^3+x^2+1, x^3+x^2+x+t, $x^3+x^2+x+t+1$, $x^3+x^2+tx+t+1$,
$x^3+x^2+(t+1)x+t$, x^3+tx^2+1, $x^3+tx^2+x+t+1$, x^3+tx^2+tx+t,
$x^3+tx^2+t+1x+t$, $x^3+tx^2+(t+1)x+t+1$, $x^3+(t+1)x^2+1$,
$x^3+(t+1)x^2+x+t$, $x^3+(t+1)x^2+tx+t$, $x^3+(t+1)x^2+tx+t+1$,
$x^3+(t+1)x^2+(t+1)x+t+1$

4B) Suppose $F=\mathbb{Q}\left(\sqrt{2}\right)$ and $f(x)\in\mathbb{Q}[x]$ is a monic irreducible polynomial of odd degree n. Then (clearly) $f\left(x+\sqrt{2}\right)$ is also monic and of degree n in $F[x]$.

(a) Show that the coefficient of x^{n-1} in $f\left(x+\sqrt{2}\right)$ is irrational.

(b) Show that $f\left(x+\sqrt{2}\right)$ is irreducible in $F[x]$.

Answer: (a) To do this just substitute $x+\sqrt{2}$ into f and use binomial expansion theorem and check the degree n coefficient.

(b) Prove that for a polynomial $f(x)$ that any linear shift $f(ax+b)$ for $a,b\in F$, the field you are in is an automorphism. Thus as $f(x)$ as odd degree adding something of degree two will not make reducible. And so $f\left(x+\sqrt{2}\right)$ is irreducible in F.

5A) Suppose A and B are finitely generated abelian groups and that

$$A\oplus A\oplus A\cong B\oplus B\oplus B$$

Show that $A\cong B$.

Answer: By the fundamental theorem of finitely generated abelian groups we know that $A\cong\mathbb{Z}^n\oplus\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_t}$ where $n_i|n_{i+1}$. Thus $A\oplus A\oplus A\cong\mathbb{Z}^{3n}\oplus\mathbb{Z}_{n_1}^3\oplus\cdots\oplus\mathbb{Z}_{n_t}^3$. We know that $B\cong\mathbb{Z}^m\oplus\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_s}$. Thus $B\oplus B\oplus B\cong\mathbb{Z}^{3m}\oplus\mathbb{Z}_{m_1}^3\oplus\cdots\oplus\mathbb{Z}_{m_s}^3$. As $A\oplus A\oplus A\cong B\oplus B\oplus B$ we know that $\mathbb{Z}^{3m}\cong\mathbb{Z}^{3n}$ and thus $m=n$. We also know that we have $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_t} \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$. And thus by the fundamental theorem of finitely generated abelian groups we know that the expression is unique and thus $\mathbb{Z}_{n_i} \cong \mathbb{Z}_{m_i}$ and thus we have an isomorphism of A and B.

5B) Use Smith Normal Form to find all integer solutions to the system

$$\begin{aligned} x + y - z &= 6 \\ x + 2z &= 5 \end{aligned}$$

Answer: We reduce the matrix as follows:

$$\begin{bmatrix} 1 & 1 & -1 & 6 \\ 1 & 0 & 2 & 5 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & -1 & 6 \\ 0 & -1 & 3 & -1 \end{bmatrix} \rightarrow$$
$$\begin{bmatrix} 1 & 0 & 2 & 5 \\ 0 & -1 & 3 & -1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 2 & 5 \\ 0 & 1 & -3 & 1 \end{bmatrix}$$

Thus $x = 5 - 2z$ and $y = 1 + 3z$ for z any integer.