Daniel Gardiner
Math 122, PSET 5 Answer Key (With thanks to David Jackson-Hanen, who provided the code and proofs for $1.b$, $2, 3$ and 4.)

1. Let : $V \to V$ be a nilpotent matrix with k its degree of nilpotency (i.e. k is the minimal n s.t. $T^n = 0$), and define $W_i = Im(T^i)$. I claim that if $W_i \neq 0$, then $dim(W_{i+1}) < dim(W_i)$.

   Proof: Clearly $Ker(T^i) \subset Ker(T^{i+1})$, as if $T^i(v) = 0$ for some $v \in V$, then $T^{i+1}(v) = T(T^i(v)) = T(0) = 0$. I claim that $Ker(T^i) \neq Ker(T^{i+1})$; this will then imply that $Ker(T^{i+1})$ has strictly greater dimension than $Ker(T^i)$.

   To see this, note that $W_i \neq 0$ implies that $i < k$. Now, $T^{k-1} \neq 0$, as k was the minimal n such that $T^n = 0$, so there exists $v \in V$ s.t $T^{k-1}(v) \neq 0$. Hence, $T^{k-1}(v) = T^i(T^{k-1-i}(v)) \neq 0$, but $T^k(v) = T^{i+1}(T^{k-1-i}(v)) = 0$, so $T^{k-1-i}(v) \in KerT^{i+1}$, but $T^{k-1-i}(v)$ is not in $KerT^i$ (note that since $k > i$, the map T^{k-1-i} makes sense).

   Hence, since above we showed that $Ker(T^i) \subset Ker(T^{i+1})$, we have that $dim(Ker(T^{i+1})) > dim(Ker(T^i))$, so applying Rank-Nullity to the operators T^i and T^{i+1}, we get $dim(V) - dim(W_{i+1}) > dim(V) - dim(W_i)$, implying that $dim(W_i) > dim(W_{i+1})$, as desired.

   Note: You have to be careful with restriction maps. A common argument was generally to note that since T is nilpotent, T is not invertible, so T has some non-trival kernel, so iterating T progressively reduces the dimension. But this doesn't use the full power of T's nilpotency, and so can not possibly work: consider $T : \mathbb{R}^3 \to \mathbb{R}^3$, where T is projection onto the $x - y$ plane, which has non-trival kernel, but its iterates do not keep reducing the dimension. Another common error was an invalid proof by contradiction; assuming the opposite is fine, but the contrapositive of the statement of the proof is that $dim(W_{i+1}) = dim(W_i)$ for *some* i; some people implicitly assumed that this had to be true $\forall i$ without making any additional arguments.

   For the second part of the argument, note that since the dimensions of W_i are monotonically decreasing and the dimension of W_1 is less than n, we must have dim $W_n = 0$, or $W_n = \{0\}$, implying that T^n is the zero map.

2. Let v_1 and v_2 be two linearly independent eigenvectors of T with eigenvalue λ. Extend them to a basis $(v_1, v_2 \dots v_n)$ of V. With respect to this basis, the first column of the matrix for T has a λ in the first row and zeroes elsewhere, and the second column has a λ in the second row of the the second column and zeroes elsewhere. Thus expanding the determinant along the first column and then the second, we see that $\det(xI - T) = (x - \lambda)^2 P(x)$, where the degree of $P(x)$ is equal to $n-2$. Thus λ is a repeated root of the characteristic polynomial.

   Conversely, he matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has 1 as a repreated root in its characteristic polynomial, and yet cannot have two linearly independent eigenvectors. One way to see this is to note that since the only possible eigenvalue of A is 1, if it had two linearly independent

eigenvectors, it would have to be conjugate to the identity matrix, which it certainly is not (note that $I \in Z(GL_n(V))$.

3. We note that $(xI - A)^t = (xI)^t - A^t = xI - A^t$. We therefore have

$$\det\,(xI - A) = \det\,(xI - A)^t = \det\,(xI - A^t).$$

We used here that det A=det A^t. The easiest way to prove this is to use the "permutation sum" definition of the determinant. Let (a_{ij}) be the componenets of A, and let $b_{ij} = a_{ji}$, the components of A^t. Expanding out, we have

$$\det\,A = \sum_{\sigma} \text{sign}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} = \sum_{\sigma^{-1}} \text{sign}(\sigma^{-1}) a_{\sigma^{-1}(1)1} a_{\sigma^{-1}(2)2} \dots a_{\sigma^{-1}(n)n}$$

$$= \sum_{\sigma} \text{sign}(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \dots b_{n\sigma(n)} = \det\,A^t$$

where we used both the fact that sign(σ)=sign(σ^{-1}) for any permutation, and also that summing over all the inverse permutations is the same as summing over all the permuations (since all inverse permuations are permuatations and vice versa.)

Thus A and A^t have the same characteristic polynomial, and hence the same roots. They need not have the same eigenvectors: $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has eigenvector $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, which is not an eigenvector of $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

4. Let v be an eigenvector of A with eigenvalue c. We have

$$1 \cdot v = A^n v = c^n v$$

where the second step follows from repeatedly applying A to the eigenvector v. Thus $c^n = 1$. Note that the equation $x^n = 1$ can have at most n solutions in $\mathbb{C}$, and $e^{2\pi i/n}$ has n distinct integer powers, all of which satisfy this equation. Thus c must be one of those powers.

5. **Claim:** Every orthonormal set of n vectors in $\mathbb{R}^n$ is a basis.
Proof: Note first that it suffices to show that any orthonormal set of n vectors in $\mathbb{R}^n$ is linearly independent, as since any linearly independent set can be extended to a basis, a set of n linearly independent vectors in an n dimensional vector space must in fact be a basis for that space.

With that in mind, denote our orthonormal set $(v_1, v_2, \dots, v_n)$ and assume that $c_1 v_1 + \dots + c_n v_n = 0$ for scalars $c_i \in \mathbb{R}$. Then, fixing any v_i and taking the inner product of both sides with v_i gives $< c_1 v_1 + \dots + c_n v_n, v_n >=< 0, v_n > \Rightarrow < c_1 v_1, v_i > + \dots + < c_i v_i, v_i > + \dots + <$

$c_n v_n, v_i >= 0 \Rightarrow c_i < v_i, v_i >= 0 \Rightarrow c_i = 0$, where we have used the bilinearity of our inner product as well as the orthonormality of the v_k to simplify our expression.

Hence, our orthonormal set is linearly independent, and the size of this set is the same as the dimension of our vector space, so the set forms a basis.

6. **Claim:** O_n and SO_n are subgroups of $GL_n(\mathbb{R})$ and $[O_n : SO_n] = 2$.
Proof: $1 : O_n$ is a subset of $GL_n(\mathbb{R})$ because if $A \in O_n$, then $det(A) = \pm 1$, so $A \in GL_n(\mathbb{R})$.
$2 : O_n$ is closed under multiplicaiton as if $A \in O_n$ and $B \in O_n$, then $< AB(v), AB(v) >=< Av, Av >=< v, v >$.
$3 : O_n$ is closed under inverstion, as if $A \in O_n$, $A^t = A^{-1}$, and since $A^{tt} = A$, $(A^t)^{-1} = A \Rightarrow A^t \in O_n$.
Hence, O_n inherits associativity from $GL_n(\mathbb{R})$, and since it is closed under inversion and multiplication, it must contain the identity element as well. Thus O_n is a subgroup.

Now note that we have a map $det : O_n \longrightarrow < \pm 1 >$, where det is the determinant map, with kernel SO_n. Thus, SO_n is a subgroup of O_n and hence of $GL_n(\mathbb{R})$ as well. Moreover, since this homomorphism is surjective, we can apply the First Isomorphism Theorem to get that $O_n/SO_n \cong < \pm 1 >$, implying that $[O_n : SO_n] = 2$.

7. Recall from class that any $A \in SO_3(\mathbb{R})$ has some non-zero eigenvector v with eigenvalue 1. Moreover, since $A \in O_3$ as well, A preserves dot product and so preserves the plane perpendicular to v. If we take an orthonormal basis for this plane (e_1, e_2) and extend this to a basis (v, e_1, e_2) for V, we see that with respect to this basis, the matrix for A has first column $(1, 0, 0)$, so applying the fact that $A(e_1)$ and $A(e_2)$ are orthogonal to v, We get that $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{bmatrix}$, implying that $1 = det(A) = ad - bc$, which implies that we can restrict A to the plane spanned by e_1 and e_2 to recover a map in SO_2, namely a rotation by some angle θ. In other words, A is uniquely determined by the vector v and the rotation by θ so, parametrizing the unit circle in P in terms of radians by the angle from e_1 (i.e viewing it as the open interval $[0, 2\pi)$ we get a set bijection between matrices A whose first column is v and points on the unit circle in P by taking such a matrix to the co-ordinate in the unit circle in P with angle θ from e_1. Since we have characterized such an A as uniquely determined by the angle of rotation θ our mapping is certainly injective, and surjectivity is clear as well.

Note: Just a note on efficieny: many people came up with pages and pages of computations, explicitly writing out the bijection in terms of all sorts of ugly co-ordinates. The above proof was really all that was necessary: just showing that you understand how the set bijection works suffices.

8. **Claim:** Any finite group G of rotations about the origin is cyclic.
Proof: If G is trivial (i.e. just the identity element), then certainly G is cyclic. Otherwise, since G is a finite group, it must have some rotation by smallest angle. Call this rotation g,

and denote its minimal angle of rotation θ. Now let h be any element in G, where α is its angle of rotation, Then, applying the Euclidean Algorithm, we can write $\alpha = m\theta + r$ for some $r \leq 0 < \theta$. But G is a group, and rotation by $m\theta$ is just g^m, so in particular $x = h * (g^m)^{-1}$ is in G. But from above, x is rotation by r, and θ was the minimal angle of rotation $\Rightarrow r = 0$, which implies that θ divides α, and so $h \in < g >$. Hence, G is cyclic, generated by g.

9. **Claim:** Let $m : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be a rigid motion: i.e. $|m(x) - m(y)| = |x - y| \forall x, y \in \mathbb{R}^n$. Then m is a bijection.
Proof: We start by showing injectivity. If $m(x) = m(y)$, then $|m(x) - m(y)| = 0 \Rightarrow |x - y| = 0 \Rightarrow x = y$. So surjectivity is the more difficult case. We present three possible proofs below (there are many ways to show this.)
Preface: For all of these proofs, note that it suffices to consider rigid motions which fix the origin, because if $m(0) = c$, then translation by $-c$ which we denote t_{-c} is certainly a rigid motion which is a bijection, so m is a bijection if and only if $t_{-c} \circ m$ is, and $t_{-c} \circ m$ is a rigid motion that fixes the origin.

Proof 1: Artin's Proof: From the preface, m is a rigid motion that fixes the origin, so by Artin Prop.4.5.16, m is left-multiplication by some orthogonal matrix A. Since $O_n \subset GL_n(\mathbb{R})$, A is invertible and so defines a bijection and in particular a surjection.
Remark: So yeah that's probably a bit "cheap" but Artin's argument is actually very nice and just goes to show the rewards of reading the book.

Proof 2: A Topological Argument: Again, note that it suffices to consider rigid motions m which fix the origin. I claim that such an m maps origin centered circles bijectively to themselves. To see this, let let $S = \{x \mid |x - 0| = d\}$ be such a circle; then for any $x \in S, |m(x) - 0| = |m(x) - m(0)| = |x - 0|$, so certainly $m(S) \subset S$, so we can restrict m to a map from S to itself. I will show that in fact $m(S) = S$, i.e. that the restriction is surjective. Assume otherwise; then there is some a not in $m(S)$. S is compact, so $m(S)$ is compact and so in particular $m(S)$ is closed, implying that its complement is open. Thus, there is some ball of radius $\epsilon > 0$ about a that does not meet $m(S)$. Now define an infite sequence as follows: let $x_1 = m(a), x_2 = m(x_1), \ldots, x_n = m(x_{n-1}), \ldots$. Then all of the x_i are in $m(S)$, so they are at least ϵ away from a. Moreover, I claim that if $i \neq j$, then $|x_i - x_j| \geq \epsilon$, as if $i \neq j$, without loss of generality let $i > j$; then $|x_i - x_j| = |m^i(a) - m^j(a)| = |m^{i-j}(a) - a| \geq \epsilon$, since $m^{i-j}(a) \in m(S)$ but a is not. Hence, we have constructed an infinite sequence of points in S that has no convergent subsequence (since all terms stay at least ϵ apart), a contradiction since S is compact. Since we have now shown that m maps origin centered circles surjectively onto themselves, given any $y \in \mathbb{R}^n$, we can consider the circle P of radius $|y|$, noting that $m(P) = P$, so in particular y has some pre-image on this circle. Hence, m is surjective.
Remark: Yeah so obviously this is an algebra class and not a toplogy class, but most people hopefully have seen some of these terms in $23, 25, 55, 101$, or 131 so I figured I'd present it anyways.
Proof 3: Circle Argument: I received some variants of this argument, which I will not type out in full. Essentially, the idea is to pin down any y by realizing it as the unique intersection of $n + 1$ spheres by essentially taking $n + 1$ well-chosen points in the image and building a

sphere around each point that hits y. A little bit of hand waving (and perhaps induction or some other nice trick) argues that y is the only thing in the intersection of these $n+1$ spheres and so now that we've charcaterized y *uniquely*, we can take the pre-image of these $n+1$ points take the spheres around these pre-images, intersect them, and then the unique thing in their intersection has to map to y. However, this only works if your $n+1$ points are *carefully* chosen (for example, you might not want them to be co-planar). To do this properly I really feel like you need some induction (perhaps on the local dimension of the circle), which gets messy, but the advantage of the argument is that it's the least technologically sophisticated of the above. At any rate, I was fairly generous giving credit for such an argument.

10. **Claim:** Let $A : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, be a linear map. Then A is a reflection if and only if its eigenvalues are 1 and -1 and its eigenvectors are orthogonal.
Proof: Assume that A is a reflection. Note that A is a linear operator, so it has to fix 0, so it is a reflection about some line through the origin. Take any vector v on this line; then v is an eigenvector with eigenvalue 1. Now consider any vector w orthogonal to v. Then since v is on the line of reflection, w gets mapped to $-w$ under the transformation (one way to see this is to use a change of co-ordinates so that you are reflecting about the x-axis), so w is an eigenvector with eigenvalue -1. On the other hand, if A has two orthogonal eigenvectors v, w with eigenvalues 1 and -1 respectively, then with respect to the basis (v,w), $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, so $A^tA = I$ implying that $A \in O_2$, and $det(A) = -1$ so A is a reflection.