1. Let $R$ be a commutative ring with $1 \neq 0$.

(a) Let $e$ be an idempotent in $R$, which means that $e^2 = e$. Prove that the intersection of the ideals $(e)$ and $(1 - e)$ is $0$. 1 is also an idempotent: $(1 - e)^2 = 1 - 2e + e^2 = 1 - e$. If $a \in (e)$, then $a = ae$ (write $a = re$ for some $r$ and use $e^2 = e$). Likewise, if $a \in (1 - e)$ then $a = a(1 - e)$. Plugging the first into the second equation gives $a = a(1 - e) = ae(1 - e) = a(e - e^2) = 0$.

(b) Let $e$ be an idempotent in $R$. Prove that $R$ is isomorphic (as a ring) to $R/(e) \times R/(1 - e)$.

1 is an $R$-linear combination of $1 - e$ and $e$, in other words, $R = (1 - e) + (e)$. Exercise (a) says that this sum is direct. Then it suffices to show that $(1 - e)$ resp. $(e)$ is isomorphic (as a ring) to $R/(e)$ resp. $R/(1 - e)$. This can be proven quickly: There is a natural homomorphism $R \to (e)$ sending $r$ to $re$. It is onto, its kernel is $(1 - e)$, and hence $R/(1 - e) \cong (e)$. Likewise $R/(e) \cong (1 - e)$.

There are other ways to prove this too: There is a natural homomorphism from $R$ to $R/(e) \times R/(1 - e)$, sending $r$ to $(r + (e), r + (1 - e))$, and it is injective by exercise (a). Showing that it is surjective can be done in the same way as in the proof of the next exercise.

(c) If $M$ is an $R$-module, prove that $M \cong eM \oplus (1 - e)M$.

The natural homomorphism $\phi : M \to eM \oplus (1 - e)M$ sends $m$ to $(em, (1 - e)m)$. It is injective because if $em$ and $(1 - e)m = m - em$ are both zero then $m$ is zero. To show that $\phi$ is surjective, take an element of $eM \oplus (1 - e)M$, and write it of the form $(em_1, (1 - e)m_2)$ for some $m_1, m_2 \in M$. Now observe that this element equals $\phi(em_1 + (1 - e)m_2)$.

Remark: You may wonder: how would someone guess a formula like $em_1 + (1 - e)m_2$? The answer is that the map “multiplying by $e$” is a projection (i.e. a map that equals its own square), and likewise “multiplying by $1 - e$” is a projection as well. So we view the multiplication by $e$ resp. $1 - e$ as projections on subspaces/submodules/subrings/etc and we can use these two projections to write our ring (in ex (b)) or our module (in ex (c)) as a direct sum with two components. Whenever you want to end up in one of these two components, you just have to apply the correct projection (either multiply by $e$ or by $1 - e$). If you apply this principle then the proof comes quickly.

(d) Suppose that $R$ is a finite ring, and suppose that every element $e \in R$ satisfies the equation $e^2 = e$. Prove that $R$ is isomorphic to $(\mathbb{Z}/(2))^r$ for some $r$. 1
If $R$ has one resp. two elements, then we’re done (with $r = 0$ resp. $r = 1$). If $R$ has more than 2 elements, then $R \setminus \{0, 1\}$ is not empty, so take $e$ in there. This $e$ is an idempotent, so $R \cong R/(e) \times R/(1-e)$, and since $e \notin \{0, 1\}$ it follows that each of $R/(e)$ and $R/(1-e)$ has strictly fewer elements than $R$. Now the result follows by induction.

2. Let $V$ be a vector space of dimension 3 over $\mathbb{Z}/(3)$. How many bases $b_1, b_2, b_3$ does $V$ have?

We can pick $b_1$ to be any element of $V - \text{SPAN}({})$ giving $3^3 - 1$ choices.
We can pick $b_2$ to be any element of $V - \text{SPAN}(b_1)$ giving $3^3 - 3$ choices.
We can pick $b_3$ to be any element of $V - \text{SPAN}(b_1, b_2)$ giving $3^3 - 3^2$ choices.

Answer: $(3^3 - 1)(3^3 - 3)(3^3 - 3^2)$ distinct bases.

3. Let $V$ be a vector space of dimension 4, and let $\phi : V \rightarrow V$ be a linear map. A vector $v \in V$ is called a cyclic vector if $v, \phi(v), \phi^2(v), \phi^3(v)$ is a basis of $V$. Suppose that $v$ is a cyclic vector, and let $B$ be the basis $v, \phi(v), \phi^2(v), \phi^3(v)$. Write down the format of the matrix of $\phi$ with respect to the basis $B$. What is meant here is that of the 16 entries in the matrix, 12 entries can be determined from the information given in this exercise; write down those 12 entries. The remaining 4 entries, the ones whose value can not be determined from the data in this exercise, indicate each of those with a $\ast$.

Take the first basis element, apply $\phi$, write it as a linear combination of our basis (weights will be: 0,1,0,0) and we have the first column of our matrix. Likewise, the second column has entries 0,0,1,0 and the third has 0,0,0,1. For the fourth column, we have to write $\phi(\phi^3(v))$ as a linear combination of our basis, but if we know nothing about $\phi$ then the weights will be unknown: $\ast, \ast, \ast, \ast$.

\[
\begin{pmatrix}
0 & 0 & 0 & \ast \\
1 & 0 & 0 & \ast \\
0 & 1 & 0 & \ast \\
0 & 0 & 1 & \ast \\
\end{pmatrix}
\]

4. If in addition to what was given in the previous question, if we also know that $\phi^4 + 3\phi^3 + 2\phi^2 + \phi = 0$, can you then fill in the $\ast$’s?

Now when we take the image of the last basis vector under $\phi$, we can write it as a linear combination of our basis. Result:

\[
\begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & -1 \\
0 & 1 & 0 & -2 \\
0 & 0 & 1 & -3 \\
\end{pmatrix}
\]

Bonus: Can you explain if there is a relation between the definition of “cyclic vector” and the definition of “cyclic” in the context of modules?
7. Let $V = \mathbb{R}[x]_{< 5}$ be the set of all polynomials in $\mathbb{R}[x]$ of degree $< 5$ (TYING ERROR: the handout had 5 instead of $< 5$). Let $\Psi : V \to V$ be the map $\Psi(f) = f + f'$. Give the matrix of $\Psi$ w.r.t. the standard basis $1, x, \ldots, x^4$. Explain why this matrix is not diagonalizable.

Example: $d$ is a unit integer for which $\phi(d) = 5$. Explain why this matrix is not diagonalizable.

6. Do Ex 2 from 11.3.

Let $b_0, \ldots, b_5$ denote $x^0, \ldots, x^5$ and let $d_0, \ldots, d_5$ denote the corresponding dual basis (so $d_i(b_j) = \delta_{i,j}$).

(a) $E$ sends $b_i$ to $3^i$ and so $E = \sum_{i=0}^{5} 3^i d_i$.

(b) $\phi$ sends $b_i$ to $1/(i + 1)$ and so it equals $\sum_{i=0}^{5} \frac{1}{i+1} d_i$.

(c) $\phi$ sends $b_i$ to $1/(i + 3)$ and so it equals $\sum_{i=0}^{5} \frac{1}{i+3} d_i$.

(d) $\phi$ sends $b_i$ to $i 5^{i-1}$ and so it equals $\sum_{i=0}^{5} i 5^{i-1} d_i$ (same as $\sum_{i=1}^{5} i 5^{i-1} d_i$).

If $M$ were diagonalizable, then $M - I$ would be diagonalizable as well (because $P I P^{-1}$ is diagonal for any invertible matrix $P$), but $M - I$ is not diagonalizable because $(M - I)^5 = 0$ while $M - I \neq 0$ (if $D$ is diagonal with entries in $\mathbb{R}$, then $D^5 = 0$ iff $D = 0$).

5. Let $V = \mathbb{R}[x]_{< 5}$ be the set of all polynomials in $\mathbb{R}[x]$ of degree $< 5$ (TYING ERROR: the handout had 5 instead of $< 5$). Let $\Psi : V \to V$ be the map $\Psi(f) = f + f'$. Give the matrix of $\Psi$ w.r.t. the standard basis $1, x, \ldots, x^4$. Explain why this matrix is not diagonalizable.

Let $\Delta$ denote the basis elements as $b_0, \ldots, b_4$ (so $b_4 = x^4$). Now $b_i \mapsto 1 b_i + i b_{i-1}$ and that produces a 1 on the diagonal, with an $i$ above it.

\[
M := \begin{pmatrix}
1 & 1 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 0 \\
0 & 0 & 1 & 3 & 0 \\
0 & 0 & 0 & 1 & 4 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

If $M$ were diagonalizable, then $M - I$ would be diagonalizable as well (because $P I P^{-1}$ is diagonal for any invertible matrix $P$), but $M - I$ is not diagonalizable because $(M - I)^5 = 0$ while $M - I \neq 0$ (if $D$ is diagonal with entries in $\mathbb{R}$, then $D^5 = 0$ iff $D = 0$).

7. Let $M$ be an $n$ by $n$ matrix with integer entries, with non-zero determinant $D$, and let $M^{-1} \in \text{Mat}_{n,n}(\mathbb{Q})$ be its inverse. Let $d$ be the smallest positive integer for which $d M^{-1} \in \text{Mat}_{n,n}(\mathbb{Z})$. Prove that $d | D$ and $D | d^n$. Give an example where $D$ is not equal to $\pm d$.

Since $M \in \text{Mat}_{n,n}(\mathbb{Z})$, its cofactor matrix $B$ will also be in $\text{Mat}_{n,n}(\mathbb{Z})$, and Theorem 30 tells us that $MB = BM = DI$. So $B = M^{-1}$. Now $D M^{-1}$ and $d M^{-1}$ are both in $\text{Mat}_{n,n}(\mathbb{Z})$, so any $\mathbb{Z}$-linear combination will be in $\text{Mat}_{n,n}(\mathbb{Z})$ as well. Using the fact that $\gcd(D, d)$ is a $\mathbb{Z}$-linear combination of $D$ and $d$, we see that $\gcd(D, d) M^{-1}$ is an integer in $\text{Mat}_{n,n}(\mathbb{Z})$. By the minimality of $d$, we see $\gcd(D, d) = d$ and hence $d | D$.

If $d M^{-1}$ has integer entries, then its determinant is an integer, but its determinant is $\det(dI) \det(M^{-1}) = d^n / D$, so $D$ divides $d^n$.

Example: $M = 2I$ with $n > 1$.

Remark: $d | D | d^n$ implies that $d$ and $D$ have the same set of prime-divisors. That can also be derived in another way, using the fact that $M$ is a unit in $\text{Mat}_{n,n}(\mathbb{Z}/(p))$ if and only if $\det(M)$ is a unit in $\mathbb{Z}/(p)$.
8. Let $R = \mathbb{Q}[x, y]$ and $I = (x, y)$. Show that $I$ is not a free $R$-module.

The module $R$ has rank 1 as an $R$-module, and hence so does $I$. So if $I$ were a free $R$-module, then it would have to be a principal ideal, $I = (f)$ for some $f$. Then $x = r_1 f$ and $y = r_2 f$ for some $r_1, r_2 \in R$. Then $0 = \deg_y(x) = \deg_y(r_1) + \deg_y(f)$ and $0 = \deg_x(y) = \deg_x(r_2) + \deg_x(f)$. So $\deg_x(f) \leq 0$ and $\deg_y(f) \leq 0$, hence $f$ is a constant. If $f = 0$ then $(f) = (0)$ and if $f$ is a non-zero constant, then $(f) = R$, but in either case, $(f)$ is not $I$, and we have a contradiction.

9. Let $M$ be a finitely generated $R$-module, and suppose that $M$ is torsion (i.e. $M = \text{Tor}(M)$). Suppose that $R$ is a PID. For $m \in M$, denote $\text{Ann}(m) = \{ r \in R | rm = 0 \}$ and $\text{Ann}(M) = \{ r \in R | \forall m \in M rm = 0 \}$. Prove that there exists $m \in M$ with $\text{Ann}(m) = \text{Ann}(M)$.

By the classification of finitely generated modules over a PID, $M$ is isomorphic to a module of the form $R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_l)$, where $r$ must be 0 since $M$ is torsion, and $a_1 | a_2 | \cdots | a_l$. Then $(a_i) \subseteq \text{Ann}(M)$ since $a_i$ vanishes in $R/(a_i)$ for each $i$. Now take $m = (0, 0, \ldots, 0, 1)$. Then $(a_l) \subseteq \text{Ann}(M) \subseteq \text{Ann}(m) = (a_l)$.