Sample questions with answers.

1. Let M be a finitely generated module over a PID R. Let $m \in M$. The annihilator of m is the set of all $r \in R$ with $rm = 0$. The annihilator of M is the of all $r \in R$ for which $rm = 0$ for all $m \in M$. Show that there exists $m \in M$ whose annihilator is equal to the annihilator of M.

   ANSWER: If M contains a non-torsion element m then m has the same annihilator as M (namely $\{0\}$). If M is torsion then M is isomorphic to a module of the form $R/(a_1) \oplus \cdots \oplus R/(a_k)$ with $a_1|a_2|\cdots|a_k$. Now take $m \in R/(a_1) \oplus \cdots \oplus R/(a_k)$ for which the last entry, the one in $R/(a_k)$, is 1. Then a_k divides any $r \in R$ for which $rm = 0$. But a_k also annihilates all of M since $a_1|\cdots|a_k$. So $\mathrm{Ann}(m) = (a_k) = \mathrm{Ann}(M)$.

2. Let M be $\mathbb{Q}[x]$-module, and a $\mathbb{Q}$-vector space of dimension n. Let (f) be the annihilator of M. Show that the degree of f is n if and only if M is a cyclic $\mathbb{Q}[x]$-module.

   ANSWER: M must be a torsion $\mathbb{Q}[x]$-module since its $\mathbb{Q}$-dimension is finite. Then M is isomorphic to a module of the form $R/(a_1)\oplus\cdots\oplus R/(a_k)$ with $a_1|a_2|\cdots|a_k$. Then the annihilator (f) equals (a_k). If M is cyclic then $k = 1$ and M is isomorphic to $R/(a_k) = R/(f)$ which has $\mathbb{Q}$-dimension degree(f). If M is not cyclic, then the dimension of M is the sum of the degrees of the a_i, this sum is larger than the degree of $a_k = f$.

3. Let $\mathbb{F}_2$ be the field with 2 elements and let $R = \mathbb{F}_2[x]$. Up to isomorphism, how many R-modules exist with precisely 8 elements?

   ANSWER: We look for $a_1|a_2|\cdots a_k$ with $a_i \in R$. The sum of the degrees must be 3, that way the dimension of the module as $\mathbb{F}_2$-vector space is 3, so that there are $2^3 = 8$ elements. Case 1: $k = 1$ and a_1 has degree 3. This gives 2^3 possible values for a_1. Case 2: $k = 2$. Then a_1 must have degree 1 (2 cases) and a_2 must have degree two, and be divisible by a_1, so it must be $g \cdot a_1$ for some linear polynomial g (2 cases) (total for Case 2 is $2 \cdot 2$ cases). Case 3: $k = 3$. Then $a_1 = a_2 = a_3$ is linear (2 cases). Total for Cases 1,2,3 is $2^3 + 2 \cdot 2 + 2 = 14$.

4. For $a, b \in \mathbb{Z}$ let $v = (a, b)$ in the abelian group $\mathbb{Z} \times \mathbb{Z}$. Show that the quotient group $\mathbb{Z} \times \mathbb{Z}/ < v >$ is cyclic if and only if $\gcd(a, b) = 1$.

   ANSWER: The $\mathbb{Z}$-module $\mathbb{Z} \times \mathbb{Z}$ has rank 2 and the $\mathbb{Z}$-module $< v >$ has rank d with $d = 0$ if $v = 0$ and $d = 1$ if $v \neq 0$. Then the quotient group has rank $r = 2 - d$ as $\mathbb{Z}$-module. By the classification theorem of $\mathbb{Z}$-modules, this quotient group is isomorphic to $\mathbb{Z}^r \oplus \mathbb{Z}/(a_1) \oplus \cdots \oplus R/(a_k)$ with $a_1|a_2|\cdots|a_k$. Now $r > 0$ so the only way this group is cyclic is when $r = 1$ (i.e. $d = 1$, so $v \neq 0$) and $k = 0$ (i.e. no torsion). It remains to show, for $v \neq 0$, that $\mathbb{Z} \times \mathbb{Z}/ < v >$ is torsion-free if and only if $\gcd(a, b) = 1$. If the gcd is $d \neq 1$, then let w be v divided by d. Then $w \notin < v >$ and

$dv \in < v >$ so w is torsion in $\mathbb{Z}\times\mathbb{Z}/ < v >$. If the gcd is 1, and if $w \notin < v >$ then any non-zero integer multiple of w will not be in $< v >$ either, so $\mathbb{Z} \times \mathbb{Z}/ < v >$ is torsion-free.

5. Let R be a PID, and let $\phi : R^n \to R^n$ be a homomorphism of R-modules. Show that for some d there is a surjective homomorphism $\phi_2 : R^n \to R^d$ with the same kernel as ϕ.

   ANSWER: Let M be the image of ϕ. Then M is a finitely generated R-module. M is torsion-free because it is contained in the torsion-free module R^n. Thus, by the classification theorem, M is isomorphic to R^d for some d. Composing this isomorphism with ϕ we obtain an onto homomorphism from R^n to R^d with the same kernel as ϕ.

6. Let R be a PID and let M be a finitely generated R-module. Show that the following are equivalent:

   (a) M is not cyclic.

   (b) There exists a surjective R-module homomorphism

   $$\phi : M \to R/I \times R/I$$

   for some ideal $I \subsetneq R$.

   ANSWER: By the classification theorem, M can (up to isomorphism) be written as $R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_k)$ for some $a_1|a_2| \cdots |a_k$ with a_1 not a unit (otherwise you could simply delete the term $R/(a_1)$ since it would be trivial). Cyclic means: $r \leq 1, k = 0$ or $r = 0, k \leq 1$. So not cyclic means (3 cases): (i) $r \geq 2$, or (ii) $r = 1, k = 1$, or (iii) $k \geq 2$. In case (i), take $I = 0$, and take the projection to the first two coordinates in R^r. In case (ii), M is $R \times R/(a_1)$ and we have a surjective homomorphism to $R/I \times R/I$ where $I = (a_1)$. In case 3, there is a natural surjective homomorphism to $R/(a_1) \times R/(a_2)$, from which there is a natural surjective homomorphism to $R/(a_1) \times R/(a_1)$.
   Conversely, if M is cyclic, say generated by m, and if ϕ were surjective, then $\phi(m)$ would generate $R/I \times R/I$ (which is not cyclic, leading to a contradiction).

7. Let $f(x)$ and $g(x)$ be two polynomials in $\mathbb{R}[x]$ of degree 3. Suppose that $f'(x) > 0$ and $g'(x) > 0$ for every $x \in \mathbb{R}$. Prove that $\mathbb{R}[x]/(f(x))$ and $\mathbb{R}[x]/(g(x))$ are isomorphic as rings.

   ANSWER: The fact that the degree is odd implies that $f(x)$ has at least one real root, and the fact that the derivative is always positive implies that there is a most one real root. So over the real numbers, f factors as $f_1 f_2$ with f_i irreducible of degree i. Then by the Chinese Remainder Theorem, $\mathbb{R}[x]/(f(x))$ is isomorphic to $\mathbb{R}[x]/(f_1) \times \mathbb{R}[x]/(f_2)$ which is isomorphic to $\mathbb{R} \times \mathbb{C}$. The same is also true for $\mathbb{R}[x]/(g(x))$.
   Note: we used the fact that if $f_2 \in \mathbb{R}[x]$ has no real roots, then $\mathbb{R}[x]/(f_2)$

is isomorphic to $\mathbb{C}$. To see this, let $\alpha \in \mathbb{C}$ be one of the two roots of f_2. Sending x to α gives a homomorphism from $\mathbb{R}[x]$ to $\mathbb{C}$ whose kernel is precisely (f_2). Thus we get an injective (then also surjective since both are $\mathbb{R}$-vector spaces of the same dimension 2) homomorphism from $\mathbb{R}[x]/(f_2)$ to $\mathbb{C}$.

8. Let V be an $\mathbb{R}$-vector space of dimension n. Let $\phi : V \to V$ be a linear map for which $\phi^3(v) = \phi^2(v)$ for all $v \in V$. Prove that there exists a basis $b_1, \ldots, b_n$ of V for which $\phi(b_i) \in \{0, b_i, b_{i-1}\}$ for every $i = 1, \ldots, n$.

   ANSWER: $\phi^3 - \phi^2 = 0$ so the polynomial $t^3 - t^2$ annihilates ϕ, and is thus a multiple of the minimal polynomial of ϕ. The roots of the minimal polynomial are the same as the roots of the characteristic polynomial. Those roots are the eigenvalues of ϕ. So all eigenvalues of ϕ are roots of $t^3 - t^2$, hence all eigenvalues are 0 or 1. Then we can take a basis for which the matrix is in Jordan normal form. This basis has the required property (to see this, write down Jordan blocks whose minimal polynomials are: t, t^2 and $t - 1$) (the factors of $t^3 - t^2$ that are powers of linear polynomials).

9. Let F be a field and M be an n by n matrix over F. Show that the following three are equivalent:

   (a) There is a non-trivial subspace $0 \neq W \subsetneq F^n$ with $Mw \in W$ for all $w \in W$.

   (b) M is similar to a matrix of the form

   $$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

   for some matrices A, B, C with entries in F (of sizes $m_1 \times m_1$, $m_1 \times m_2$, $m_2 \times m_2$ for some $m_1, m_2 > 0$).

   (c) The characteristic polynomial $f \in F[x]$ of M is reducible in $F[x]$.

   ANSWER:
   (a) $\Longrightarrow$ (b). Take a basis $b_1, \ldots, b_k$ of W and extend it (for a vector space, any independent set can be extended to a basis) to a basis $b_1, \ldots, b_n$ of F^n. The matrix of M with respect to this basis will have the correct form.
   (b) $\Longrightarrow$ (c). Similar matrices have the same characteristic polynomial, and the characteristic polynomial of the matrix in part (b) is the product of the characteristic polynomials of matrices A and C.
   (c) $\Longrightarrow$ (a). We can turn F^n into an $F[x]$-module as follows: If $g = g(x) \in F[x]$ and $v \in F^n$ then $g \cdot v := g(M)v$. Now take any non-zero v in F^n and let $g \in F[x]$ be its annihilator (the monic polynomial of minimal degree with $g \cdot v = 0$). Then $g|f$ because f annihilates any element of F^n due to the fact that $f(M) = 0$. Let d be the degree of g. Then the span of $v, Mv, M^2v, M^3v, \ldots$ has the following basis: $\{v, Mv, \ldots, M^{d-1}v\}$ (these must be linearly independent due to the minimality of the degree of g). If $d < n$ then we can take W as this span. If $d = n$, then the annihilator g

of v equals f. But f is reducible, say $f = f_1 f_2$. Now take $v' := f_2(v)$. Its annihilator is f_1, and so we can take W as the span of $v', Mv', M^2v', \ldots$, which has dimension equal to the degree of f_1.

10. Let M be an $\mathbb{F}_p[x]$-module of dimension 3 (dimension as $\mathbb{F}_p$-vector space). Suppose that M is not a cyclic module.

    (a) Let $r = x^p - x$ and let $m \in M$. Show that $r^2 m = 0$.

    (b) Must rm also be 0?

    ANSWER: M is isomorphic to $R/(a_1) \oplus \cdots \oplus R/(a_k)$ with $a_1 | a_2 | \cdots | a_k$. M is not cyclic, so $k > 1$. The dimension is 3, so $k \leq 3$. If $k = 3$ then $a_1 = a_2 = a_3 = x - c$ for some $c \in \mathbb{F}_p$. Every $c \in \mathbb{F}_p$ is a root of $x^p - x$ so a_3 (the annihilator of M) divides $r := x^p - x$. Then $rm = 0$ for all $m \in M$. The remaining case is $k = 2$. Then $a_1 = x - c$ for some $c \in \mathbb{F}_p$ and a_2 must have degree 2, and must be divisible by a_1, so $a_2 = (x - c)(x - d)$ for some $c, d \in \mathbb{F}_p$. If $c \neq d$ then a_2 divides $x^p - x$ and in that case, $rm = 0$ for all $m \in M$. But if $d = c$ then $a_2 = (x - c)^2$ and this does not divide $r = x^p - x = x(x - 1)(x - 2) \cdots (x - (p - 1))$. That means that if m corresponds to $(0, 1) \in R/(a_1) \oplus R/(a_2)$ then r does not annihilate m since r is not an element of the annihilator (a_2) of m.