Problem 1 (12.1.2).

Proof. (a) Let \( \varphi : N \to R^n \) sending \( \sum r_i x_i \mapsto (r_i) \). Since the \( x_i \)'s are linearly independent and generate \( N \), every element of \( N \) can be uniquely written as \( r_1 x_1 + \ldots + r_n x_n \). Hence \( \sum r_i x_i = \sum r'_i x_i \) implies \( r_i = r'_i \) and thus \( \varphi \) is well-defined. Surjectivity is clear. Since \( \ker \varphi = \{0\} \), \( \varphi \) is bijective.

Let’s show now that \( M/N \) is torsion. Let \( y + N \) be any non-zero coset. The set \( \{y, x_1, \ldots, x_n\} \) must be linearly dependent since the \( x_i \)'s are assumed to form a maximal set of linearly independent elements of \( M \).

Thus there exist \( r, r_i \in R \) such that \( r y + r_1 x_1 + \ldots + r_n x_n = 0 \). This means \( r(y + N) = 0 \) in \( M/N \). Since this is true (with possibly different \( r \)'s) for all non-zero cosets \( y + N \) of \( M/N \), we conclude that \( M/N \) is torsion.

(b) Clearly the rank of \( M \) is at most \( n \). Let \( \{y_1, \ldots, y_{n+1}\} \) be an arbitrary set of \( n + 1 \) distinct elements in \( M \). Since \( M/N \) is a torsion module, there exist \( r_i \in R \) with \( r_1 y_1 + \ldots + r_{n+1} y_{n+1} \in N \). The elements \( r_i y_i \) are \( n + 1 \) elements in \( N \), and since \( N \) has rank \( n \), there is some linear combination of the \( r_i y_i \)'s equal to 0. This can be viewed as a linear combination of the \( y_i \)'s, showing that the \( y_i \)'s are linearly dependent. Thus every set consisting of \( n + 1 \) elements of \( M \) is linearly dependent, hence \( M \) has rank \( n \).

\[ \square \]

Problem 2 (12.1.5).

Proof. \((-x) \cdot 2 + 2 \cdot x = 0 \). So \( \{2, x\} \) is not linearly independent, hence is not a basis for \( M \).

For any \( a, b \in M \) we have \((-a)b + b \cdot a = 0 \), which means that \( a \) and \( b \) are linearly dependent. Thus \( M \) has rank 1. If \( M \) were free of rank 1, there would exist \( m \in M \) such that \( M = Rm \). But then there would exist \( r, r' \in R \) such that \( 2 = rm \) and \( x = r'm \). Then \( m|2 \) and \( m|x \) in \( R \), which would imply \( m = \pm 1 \notin M \).

\[ \square \]

Problem 3 (12.1.16).

Proof. Let \( \{x_1, \ldots, x_n\} \) be a set of generators for \( M \). Consider \( R^n \) with basis \( e_i \) (so \( e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \) with 1 in \( i \)th position) and \( R \)-module homomorphism \( R^n \to M \) sending \( e_i \mapsto x_i \). This is clearly surjective, since any element of \( M \) can be written as \( \sum r_i x_i \), and the elements \( (r_1, \ldots, r_n) \in R^n \) then maps to \( \sum r_i x_i \).

Conversely if such a surjective homomorphism exists, then the images of the \( e_i \)'s form a set of generators for \( M \).

(a) If \( M \) is finitely generated, then there is \( n \) and a surjective homomorphism \( \varphi : R^n \to M \). Composing with the surjective map \( M \to N \), this yields a surjective homomorphism \( R^n \to N \), and by the above this implies that \( N \) is finitely generated.

(b) \( R = \mathbb{Q}[x_1, \ldots, x_n, \ldots] \) is clearly finitely generated as an \( R \)-module (with generator 1). Consider the submodule (ideal) \( I = (x_1, \ldots, x_n, \ldots) \). Assume \( I \) is finitely generated, say by polynomials \( p_1, \ldots, p_m \). Each \( p_i \) involves finitely many of the variables \( x_j \). Hence all \( p_i \)'s collectively can only involve variables \( x_1, \ldots, x_N \) for some fixed large enough \( N \).

By assumption \( x_{N+1} \) is an \( R \)-linear combination of the \( p_i \)'s, so in particular, an \( R \)-linear combination of \( x_1, \ldots, x_N \). Write \( x_{N+1} = x_1 f_1 + \ldots + x_N f_N \). Evaluate this at \( e_{N+1} \) which consists of 0 in every position except 1 in position \( N + 1 \). The LHS is then simply 1, while the RHS is 0. Contradiction.
Problem 4.

Proof. The matrix $A$ defines a map $F^n \to F^n$ which clearly extends the map $R^n \to R^n$.

If $(\det A) \not= 0$, then $A$ is injective as a map $F^n \to F^n$. In particular then $A$ is injective as a map restricted to $R^n$.

Conversely, if $A$ is injective as a map $R^n \to R^n$, then the induced map $A : F^n \to F^n$ is injective, so $\det A \not= 0$ (from linear algebra).

Assume not $\det A$ is a unit. In particular, $\det A \not= 0$ and $A$ is injective. We have to verify surjectivity. The adjoint matrix $A^*$ has entries equal to determinants of submatrices of $A$, hence has entries in $R$. Recall that $AA^* = (\det A)I_n$. If $\det A$ is a unit, it follows that $A$ is invertible and the inverse matrix $A^{-1}$ has entries in $R$. Thus for any $y \in R^n$ we have $A(A^{-1}y) = y$ and $A^{-1}y \in R^n$, thus the map $A : R^n \to R^n$ is bijective.

If $A$ is bijective as a map $R^n \to R^n$, then it is bijective as a map $F^n \to F^n$ hence $\det A$ is a unit (from linear algebra).

Problem 5.

Proof. (1) Yes. Let $I$ be a maximal ideal of $R$. Consider the submodule $IM = \{a_1m_1 + \ldots + a_nm_n \mid a_i \in I, \ m_i \in M\}$. Then $M/IM$ is a vector space over $R/I$, which is a field since $I$ is maximal.

Now if $B = \{x_1, \ldots, x_n\}$ is a basis of $M$, consider $B + IM \subset M/IM$. Since $B$ spans $M$, $B + IM$ spans $M/IM$. Indeed if $m + IM \in M/IM$, then write $m = \sum r_ix_i$ (we can do this since $\{x_i\}$ is a basis for $M$), then $m + IM = \sum (r_i + I)(x_i + IM)$.

Suppose now $\sum_{i=1}^n (r_i + I)(x_i + IM) = IM$. Then $\sum_{i=1}^n r_ix_i \in IM$, hence $\sum r_ix_i = \sum a_ix_i$ for some $a_i \in I$.

From the linear independence of $B$ we conclude $r_i = a_i \in I$, so $r_i + I = I$. Thus $B + IM$ is a basis for $M/IM$ as a $R/I$-vector space. But then for any basis $B$, the set $B + IM$ must have a fixed cardinality equal to the dimension of $M/IM$ as a $R/I$-vector space, so $|B|$ is the same for different bases.

(2) Yes. Since $M \cong R^n$ we will prove the result for $R^n$. Let $F$ be the fraction field of $R$. Then $R^n$ is an additive subgroup of $F^n$. Consider $T = \{x_1, \ldots, x_k\} \subset R^n$ over $F$. If this is linearly independent over $F$ it is clearly also linearly independent over $R$. Assume the converse: that $T$ is linearly independent over $R$. If it were linearly dependent over $F$, we would have $\sum_{i=1}^k s_i r_i x_i = 0$ for some $r_i \in R$ and nonzero $s_i \in R$. Multiplying by $s = s_1 \cdots s_k$ gives us a linear dependence relation with coefficients in $R$, which thus have to be 0 (since we assume $T$ is linearly independent over $R$ and $R$). Since $R$ is an ID this implies $r_i = 0$. Thus $T$ is linearly independent over $F$.

Since $F^n$ has no linearly independent set (over $F$) of size more than $n$, neither can $R^n$ have a linearly independent subset of size larger than $n$.

(3) No. Take $M = R$ free of rank 1 over itself. Any non-unit of $R$ is not a basis for $R$ (think of $2 \in \mathbb{Z}$ over $\mathbb{Z}$, it generates the submodule $2\mathbb{Z} \neq \mathbb{Z}$).
(4) Yes. From (1), if $S$ is a generating set, then $S + IM$ is a generating set for $M/IM$ as a $R/I$-vector space. For vector spaces, such a generating set must have size at least equal to the dimension $n$. Thus $n \leq |S + IM| = |S|$.

(5) Yes. Take a generating set $S$ of size $n$. Combining arguments from (2), we have that $S$ generates $F^n$ as a $F'$-vector space, where $F'$ is the fraction field of $R$. Since $\dim_{F'} F^n = n$, $S$ must be a basis. In particular it is linearly independent over $R$ and hence a basis.

(6) Yes. Let $B = \{x_1, \ldots, x_n\}$ be a generating set of linearly independent vectors. Every $m \in M$ can be written as $m = r_1x_1 + \ldots + r_nx_n$ for some $r_i \in R$. This representation is unique, otherwise it gives a nontrivial linear combination of the $x_i$’s that is 0, contradicting linear independence. Thus $B$ is a basis.

(7) No. Consider $\mathbb{Z}$ as a module over itself. $\{2\}$ is a 1-element set, so linearly independent, but does not extend to a basis of $\mathbb{Z}$.

(8) No. Again, consider $M = \mathbb{Z}$ viewed as module over itself $R = \mathbb{Z}$. Then $\{2, 3\}$ is a generating set that does not contain a basis.

\qed