Solutions Exercise sheet 12

1. Let V be vector space of dimension n over the field F, let $A, B \in \mathrm{Mat}_{n\times n}(F)$ be matrices corresponding to two linear transformations on V. Let V_A and V_B be the vector space V viewed as an $F[X]$ module using A and B respectively. i.e. the action of $x \in F[X]$ on $v \in V$ is defined as $X \cdot v := Av$ (or $X \cdot v = Bv$).

Show that V_A is isomoprhic to V_B as $F[X]$ modules if and only if $B = UAU^{-1}$ for some matrix $U \in \mathrm{GL}(n, F)$.

Solution:

Let $\varphi : V_A \to V_B$ be an $F[X]$-module isomorphism. This means φ is a bijection and for all $\mathbf{v}, \mathbf{v}' \in V$ and $f(X) \in F[X]$ we have

$$\varphi(\mathbf{v}+\mathbf{v}') = \varphi(\mathbf{v}) + \varphi(\mathbf{v}'), \quad \varphi(f(X)\mathbf{v}) = f(X)\varphi(\mathbf{v}).$$

Polynomials are sums of monomials and knowing multiplication by X determines multiplication by X^i for all $i \geqslant 1$, the above conditions on φ are equivalent to

$$\varphi(\mathbf{v}+\mathbf{v}') = \varphi(\mathbf{v}) + \varphi(\mathbf{v}'), \quad \varphi(c\mathbf{v}) = c\varphi(\mathbf{v}), \quad \varphi(X\mathbf{v}) = X\varphi(\mathbf{v})$$

for all $\mathbf{v}$ and $\mathbf{v}'$ in V and c in F. The first two equations say φ is F-linear and the last equation says $\varphi(A\mathbf{v}) = B\varphi(\mathbf{v})$ for all $\mathbf{v} \in V$. So $\varphi : V \to V$ is an F-linear bijection and $\varphi(A\mathbf{v}) = B\varphi(\mathbf{v})$ for all $\mathbf{v} \in V$. Since $V = F^n$, every F-linear map $\varphi : V \to V$ is a matrix transformation: for some $U \in \mathrm{Mat}_n(F)$,

$$\varphi(\mathbf{v}) = U\mathbf{v}.$$

Indeed, if there were such a matrix U then letting $\mathbf{v}$ run over the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ tells us the i-th column of U is $\varphi(\mathbf{e}_i)$, and the other way around define U to be the matrix

$$[\varphi(\mathbf{e}_1) \cdots \varphi(\mathbf{e}_n)] \in \mathrm{Mat}_{n\times n}(F)$$

having i-th column $\varphi(\mathbf{e}_i)$. Then φ and U have the same values on the $\mathbf{e}_i$'s and both are linear on F^n, so they have the same value at every vector in F^n. Since φ is a bijection, U is invertible, i.e., $U \in \mathrm{GL}_n(F)$. Now the condition $\varphi(A\mathbf{v}) = B\varphi(\mathbf{v})$ for all $\mathbf{v} \in V$ means

$$U(A\mathbf{v}) = B(U\mathbf{v}) \Longleftrightarrow A\mathbf{v} = U^{-1}BU\mathbf{v}$$

for all $\mathbf{v} \in V = F^n$. Letting $\mathbf{v} = \mathbf{e}_1, \ldots, \mathbf{e}_n$ tells us that A and $U^{-1}BU$ have the same i-th column for all i, so they are the same matrix: $A = U^{-1}BU$, so $B = UAU^{-1}$.

Conversely, suppose there is an invertible matrix $U \in \mathrm{GL}_n(F)$ with $B = UAU^{-1}$. Define $\varphi : V_A \to V_B$ by $\varphi(\mathbf{v}) = U\mathbf{v}$. The matrix U is invertible, so this is a bijection. It is also F-linear. To show

$$\varphi(f(X)\mathbf{v}) = f(X)\varphi(\mathbf{v})$$

for all $\mathbf{v} \in V$ and $f(X) \in F[X]$, it suffices by F-linearity to check

$$\varphi\left(X^i\mathbf{v}\right) = X^i\varphi(\mathbf{v})$$

for all $\mathbf{v} \in V$ and for $i \geqslant 0$. For this to hold, it suffices to check $\varphi(X\mathbf{v}) = X\varphi(\mathbf{v})$ for all $\mathbf{v} \in V$. This last condition says that $\varphi(A\mathbf{v}) = B\varphi(\mathbf{v})$ for all $\mathbf{v} \in V$. Since $B = UAU^{-1}$, i.e. $UA = BU$, so

$$\varphi(A\mathbf{v}) = U(A\mathbf{v}) = (UA)\mathbf{v} = (BU)\mathbf{v} = B(U\mathbf{v}) = B\varphi(\mathbf{v})$$

for all $\mathbf{v} \in V$.

2. Let R be a non-zero commutative ring with $0 \neq 1$. Show that if $R^n \simeq R^m$ as R-modules then $m = n$.

Solution:

Let $M := R^m$, $N := R^m$ and let I be a maximal ideal of R. Let $V = M/IM$. Here we denote by

$$IM = \left\{\sum_{i=1}^{k} a_i x_i | a_i \in I, x_i \in M, k \in \mathbb{N}\right\}$$

i.e all finite I-linear combinations of elements of M. It is easy to verify that V is a vector space over the field $K = R/I$ where the scalar multiplication is defined via $(r + I)(x + IM) = rx + IM$ for $r + I \in K$ and $x + IM \in M/IM$. This is well defined since if $r \in I$ or $x \in IM$ then $rx \in IM$, and hence $(r + I)(x + IM) = IM$.

Now one can also see that if $\{x_i\}$ is a basis of M over R, then $\bar{x_i} = x_i + IM$ is a basis of $V = M/IM$. Hence V is a vector space of dimension m over K. Similarly we get that N/IN is a vector space of dimension n.

The isomorphism of $R^m = M \simeq N = R^n$ restricts to an isomorphism of $IM \simeq IN$ and we get an induced isomorphism $M/IM \simeq N/IN$. Since M/IM and I/IN are isomorphic finite dimensional vector spaces, they have the same dimension and we get that $m = n$.

3. Let R be a ring, let M be an R-module and let N be a submodule of M. Prove:

(a) If M is finitely generated, then M/N is finitely generated.

(b) If N and M/N are finitely generated, then M is finitely generated.

(c) If N and M/N are free R-modules, then M is a free R-module.

Solution: Let $\varphi : M \to M/N, m \mapsto m + N$ denote the quotient map.

We will prove the following more general statements:

(a') If M has a generating subset of cardinality r, then so does M/N.

(b') If N and M/N have generating subsets of cardinalities respectively r and s, then M has a generating subset of cardinality $r + s$.

(c') If N and M/N have bases of cardinalities respectively r and s, then M has a basis of cardinality $r + s$.

Proof. (a') The images in M/N of a generating subset of M generate M/N, since the canonical morphism from M to M/N is surjective. In particular, M/N is finitely generated if M is.

(b') Let $(n_1, \ldots, n_r)$ be a generating family of N, and let $(m_1, \ldots, m_s)$ be a family of elements of M such that $(\varphi(m_1), \ldots, \varphi(m_s))$ generate M/N. Let us show that the family $(m_1, \ldots, m_s, n_1, \ldots, n_r)$ generates M.

Let $m \in$ M. By hypothesis, $\varphi(m)$ is a linear combination of $\varphi(m_1), \ldots, \varphi(m_s)$. There thus exist elements $a_i \in$ R such that $\varphi(m) = \sum_{i=1}^{s} \varphi(m_i) a_i$. Consequently, $n = m - \sum_{i=1}^{s} m_i a_i$ belongs to N and there exist elements $b_j \in$ R such that $n = \sum_{j=1}^{r} n_j b_j$. Then $m = \sum_{i=1}^{s} m_i a_i + \sum_{j=1}^{r} n_j b_j$ is a linear combination of the m_i and of the n_j.

(c') Moreover, let us assume that $(n_1, \ldots, n_r)$ be a basis of N and that $(\varphi(m_1), \ldots, \varphi(m_s))$ be a basis of M/N; let us show that $(m_1, \ldots, m_s, n_1, \ldots, n_r)$ is a basis of M. Since we already proved that this family generates M, it remains to show that it is free. So let $0 = \sum_{i=1}^{s} m_i a_i + \sum_{j=1}^{r} n_j b_j$ be a linear dependence relation between these elements. Applying φ, we get a linear dependence relation $0 = \sum_{i=1}^{s} \varphi(m_i) a_i$ for the family $\varphi(m_i)$. Since this family is free, one has $a_i = 0$ for every i. It follows that $0 = \sum_{j=1}^{r} n_j b_j$; since the family $(n_1, \ldots, n_r)$ is free, $b_j = 0$ for every j. The considered linear dependence relation is thus trivial, as was to be shown.

4. Let R be a PID. Show that every submodule N of a free R-module M of rank n is finitely generated with at most n generators.

Hint: Apply Exercise **3**.

Solution:

It suffices to show that every submodule N of R^n is free of rank $\leqslant n$; and we will prove this by induction on n.

If $n = 0$, then $R^n = 0$, hence $\mathrm{N} = 0$ so that N is a free R-module of rank 0.

Assume that $n = 1$. Then N is an ideal of R. If $\mathrm{N} = 0$, then N is free of rank 0. Otherwise, since R is a PID, there exists a nonzero element $r \in R$ such that $\mathrm{N} = (r)$. Since R is a domain, the map $a \mapsto ra$ is an isomorphism from R to N, so that N is free of rank 1.

Let now n be an integer $\geqslant 2$ and let us assume that for any integer $r < n$, every submodule of R^r is free of rank less or equal than r. Let N be a submodule of R^n. Let $f : R^n \to R$ be the linear form given by $(a_1, \ldots, a_n) \mapsto a_n$; it is surjective and its kernel is the submodule $\mathrm{M}_0 = R^{n-1} \times \{0\}$ of R^n. By induction, the ideal $f(\mathrm{N})$ of R is free of rank $\leqslant 1$. The submodule $\mathrm{N}_0 = \mathrm{N} \cap \mathrm{M}_0$ of M_0 is isomorphic to a submodule of R^{n-1}, so is free of rank $\leqslant n-1$ by our induction hypothesis.

Since the module $M_0 = \ker(f)$ is free of rank $\leqslant n-1$, and $f(N)$ is free of rank $\leqslant 1$, we have that N is free of rank $\leqslant n$ by Exercise **3**. part (c).

5. Let R be a commutative ring. An R-module M is called a *Noetherian* R-module if it satisfies the ascending chain condition on submodules, i.e., whenever

$$M_1 \subset M_2 \subset \cdots$$

is an increasing chain of submodules of M, then there is a positive integer m such that for all $k \geqslant m$ we have $M_k = M_m$.

Show that the following are equivalent for an R module M:

(a) M is a Noetherian R-module.

(b) Every non empty subset of modules of M contains a maximal element under inclusion.

(c) Every submodule of M is finitely generated.

Solution:

[(**5**.a) $\Rightarrow$ (**5**.c)] Let us assume that M is Noetherian, that is, any nonempty family of submodules of M admits a maximal element.

Let N be a submodule of M and consider the family $\mathcal{S}_N$ of all finitely generated submodules of N. This family is nonempty because the null module 0 belongs to $\mathcal{S}_N$. By hypothesis, $\mathcal{S}_N$ has a maximal element, say, N'. By definition, the R-module N' is a finitely generated submodule of N and no submodule P of N such that $\mathrm{N}' \subsetneq \mathrm{P}$ is finitely generated. For every $m \in \mathrm{N}$, the R-module $\mathrm{P} = \mathrm{N}' + \mathrm{R}m$ satisfies $\mathrm{N}' \subset \mathrm{P} \subset \mathrm{N}$ and is finitely generated; by maximality of N', one has $\mathrm{P} = \mathrm{N}'$, hence $m \in \mathrm{N}'$. This proves that $\mathrm{N}' = \mathrm{N}$, hence N is finitely generated.

[(**5**.c) $\Rightarrow$ (**5**.b)] Let us assume that every submodule of M is finitely generated. Let $\{\mathrm{M}_n\}_{n\in\mathbf{N}}$ be an increasing sequence of submodules of M. Let $\mathrm{N} = \bigcup \mathrm{M}_n$ be the union of these modules M_n.

Since the family is increasing, N is a submodule of M. By hypothesis, N is finitely generated. Consequently, there exists a finite subset $S \subset \mathrm{N}$ such that $\mathrm{N} = \langle \mathrm{S} \rangle$. For every $s \in \mathrm{S}$, there exists an integer $n_s \in \mathrm{N}$ such that $s \in \mathrm{M}_{n_s}$; then $s \in \mathrm{M}_n$ for any integer n such that $n \geqslant n_s$. Let us set $v = \sup(n_s)$, so that $\mathrm{S} \subset \mathrm{M}_v$. It follows that $\mathrm{N} = \langle S \rangle$ is contained in M_v. Finally, for $n \geqslant v$, the inclusions $\mathrm{M}_v \subset \mathrm{M}_n \subset \mathrm{N} \subset \mathrm{M}_v$, for $n \geqslant v$ show that $\mathrm{M}_n = \mathrm{M}_v$. Hence we have shown that the sequence $\{\mathrm{M}_n\}$ is stationary.

[(**5**.b) $\Rightarrow$ (**5**.a)] Let us assume that any increasing sequence of submodules of M is stationary and let $\{\mathrm{M}_i\}_{i\in\mathrm{I}}$ be a family of submodules of M indexed by a nonempty set I.

Assuming by contradiction that this family has no maximal element, we are going to construct from the family $\{\mathrm{M}_i\}$ a strictly increasing sequence of submodules of M. Fix $i_1 \in \mathrm{I}$. By hypothesis, M_{i_1} is not a maximal element of the family $\{\mathrm{M}_i\}$, so that there exists $i_2 \in \mathrm{I}$ such that $\mathrm{M}_{i_1} \subsetneq \mathrm{M}_{i_2}$. Then M_{i_2} is not maximal neither, hence the existence of $i_3 \in \mathrm{I}$ such that $\mathrm{M}_{i_2} \subsetneq \mathrm{M}_{i_3}$ and we can continue on like this. Hence, we obtain a strictly increasing sequence $\{\mathrm{M}_{i_n}\}_{n\in\mathbf{N}}$ of submodules of M, hence the desired contradiction.

6. Show that if R is a PID then every nonempty set of ideals of R has a maximal element and that R is Noetherian.

Solution: Let I be an ideal of R. Since R is a PID, the ideal I is principal and hence finitely generated. Hence by question **5**. we obtain that R is Noetherian (by part (a)) and every nonempty set of ideals of R has a maximal element under inclusion (by part (b)).