EPFL - Fall 2024	Domenico Valloni
Rings and modules	**Exercises**
Sheet 3 - Solutions	

Exercise 1. Computing a presentation of an R module M means explicitly determining an exact sequence of the form $R^{\oplus t} \xrightarrow{\eta} R^{\oplus s} \xrightarrow{\varepsilon} M \longrightarrow 0$. Do the following computations.

(1) Compute a presentation of the $\mathbb{Z}$-module
$$M := \mathbb{Z}(2,9) + \mathbb{Z}(4,3) + \mathbb{Z}(6,8) \subseteq \mathbb{Z} \oplus \mathbb{Z}.$$

(2) Let $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ be the ring of 2×2-matrices over $\mathbb{Z}$. Compute a presentation of the left R-module
$$M := R\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} + R\begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} \subseteq R.$$

Proof. (1) We define a surjective morphism $\varepsilon : \mathbb{Z}^3 \to M$ by $e_1 \mapsto (2,9)$, $e_2 \mapsto (4,3)$, $e_3 \mapsto (6,8)$. Then we calculate generators of the kernel:

(a_1, a_2, a_3) is mapped to zero if and only if the following two equations are satisfied:
$$2a_1 + 4a_2 + 6a_3 = 0$$
$$9a_1 + 3a_2 + 8a_3 = 0$$
From the first equation we find $a_1 = -2a_2 - 3a_3$. Substituing for a_1 in the second equation gives us $15a_2 = -19a_3$. This implies that $a_2 = -19t$, $a_3 = 15t$ for $t \in \mathbb{Z}$. This gives that $a_1 = -2(-19t) - 3(15t) = -7t$. We conclude that a presentation is given by
$$\mathbb{Z} \xrightarrow{\eta} \mathbb{Z}^3 \xrightarrow{\varepsilon} M \to 0$$
where the first map is $\eta : t \mapsto (-7t, -19t, 15t)$

(2) We define a surjective morphism $\varepsilon : R^2 \to M$ by
$$e_1 \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \, e_2 \mapsto \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}$$
and we are interested in calculating generators of the kernel. I.e., we calculate the solution set of the matrix equation
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2a + 2\beta & 3\alpha \\ 2c + 2\delta & 3\gamma \end{pmatrix} = 0$$
Hence the kernel consits of the elements $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$ such that $a = -\beta$, $c = -\delta$, $\alpha = \gamma = 0$. I.e., the elements of the form
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} 0 & -a \\ 0 & -c \end{pmatrix}\right).$$

Thus, the map $\eta : R \to R^2$ defined by
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\right)$$
gives a presentation $R^{\oplus t} \xrightarrow{\eta} R^{\oplus s} \xrightarrow{\varepsilon} M \to 0$ of M.

□

Exercise 2. Do the following:

(1) Calculate the Smith normal form of the following matrix over $\mathbb{Z}$.

$$\begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix}$$

(2) (i) Find a direct sum of cyclic $\mathbb{Z}$-modules isomorphic to the $\mathbb{Z}$-module M with generators e_1, e_2, e_3, e_4 and relations

$$\begin{aligned} e_1 - 2e_2 + 2e_3 - e_4 &= 0 \\ 9e_1 - 6e_2 - 8e_3 + e_4 &= 0 \\ e_1 + 2e_3 + 5e_4 &= 0 \end{aligned}$$

[*Hint/Remark:* By definition, M is the quotient of the free $\mathbb{Z}$-module on 4 generators $\bigoplus_{i=1}^{4} \mathbb{Z}e_i$ by the submodule generated by $e_1 - 2e_2 + 2e_3 - e_4$, $9e_1 - 6e_2 - 8e_3 + e_4$ and $e_1 + 2e_3 + 5e_4$. Notice that in the quotient, $e_1, \dots, e_4$ then satisfy exactly these relations.]

(ii) Explicitly give 'nice' generators of M, in terms of the original generators e_1, e_2, e_3, e_4. Here, $f_1, \dots, f_s$ are 'nice' generators if the relations they satisfy are generated by relations of the form $m_i f_i = 0$, where $m_1, \dots, m_s \in \mathbb{Z}$ are integers.

Proof. (1) We follow the algorithm for using row and column operations to produce the Smith normal form of a matrix.

Step 1a: Ensure that the $(1,1)^{\text{th}}$ entry is the principal generator for the ideal generated by the entries of the first row and column. In this case it is already true, so we move on.

Step 1b: Use that property to remove all other entries in the first column by adding a multiple of the first row to subsequent rows. Then remove all other entries in the first row by adding a multiple of the first column to later columns:

$$\begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 9 & 1 \\ 0 & 12 & 2 \\ 0 & -26 & 0 \\ 0 & 10 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 2 \\ 0 & -26 & 0 \\ 0 & 10 & 6 \end{pmatrix}$$

Step 2a: Ensure the $(2,2)^{\text{th}}$ entry is the principal generator for the ideal generated by the second row and column. In this case we must swap the second and third columns.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 2 \\ 0 & -26 & 0 \\ 0 & 10 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \\ 0 & 0 & -26 \\ 0 & 6 & 10 \end{pmatrix}$$

Step 2b: Remove other non-zero entries in the second row and column.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \\ 0 & 0 & -26 \\ 0 & 6 & 10 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \\ 0 & 0 & -26 \\ 0 & 0 & -26 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -26 \\ 0 & 0 & -26 \end{pmatrix}$$

Step 3: Tidy up the resulting matrix to obtain Smith normal form:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -26 \\ 0 & 0 & -26 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -26 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 26 \\ 0 & 0 & 0 \end{pmatrix}$$

(2) (i) In terms of the generators $e_1, \dots, e_4$ of M given in the exercise the surjection $\mathbb{Z}^4 \to M$ defined by these generators has kernel K spanned by

$$\begin{pmatrix} 1 \\ -2 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 9 \\ -6 \\ -8 \\ 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 \\ 0 \\ 2 \\ 5 \end{pmatrix}.$$

So K is the image of the linear map $\mathbb{Z}^3 \to \mathbb{Z}^4$ given by the matrix

$$\begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix}$$

As discussed in section 4.1 of the lecture notes, multiplying a matrix to the left and right with invertible matrices doesn't change the isomorphism type of the cokernel. Hence M is isomorphic to the cokernel of the Smith normal form of the above matrix, i.e.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 26 \\ 0 & 0 & 0 \end{pmatrix}$$

The cokernel of this matrix is $\overbrace{\mathbb{Z}/\mathbb{Z}}^{=0} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \oplus \mathbb{Z}$, so we obtain

$$M \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \oplus \mathbb{Z}.$$

(ii) We want to find the elements of M which correspond to the canonical generators of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \oplus \mathbb{Z}$ (i.e. the vectors with precisely one component equal to 1 and 0's everywhere else). Write

$$A := \begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix}, \quad D := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 26 \\ 0 & 0 & 0 \end{pmatrix}$$

We have found invertible matrices $P \in \mathrm{GL}_4(\mathbb{Z})$ and $Q \in \mathrm{GL}_3(\mathbb{Z})$ such that

$$PAQ = D$$

We can rephrase this as a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}^3 \arrow[r, "f_A"] & \mathbb{Z}^4 \arrow[d, "f_P"] \\
\mathbb{Z}^3 \arrow[u, "f_Q"] \arrow[r, "f_D"'] & \mathbb{Z}^4
\end{tikzcd}$$

where f_B denotes the linear map associated to the matrix B. We then have that f_P induces an isomorphism

$$\overline{f_P} : M = \operatorname{coker}(f_A) \to \operatorname{coker}(f_D)$$

However, it is clear that a nice basis for $\operatorname{coker}(f_D)$ is given by the classes of $(e_2, \dots, e_4)$, so a nice basis for $M = \operatorname{coker}(f_A)$ is given by the classes of

$$(f_{P^{-1}}(e_2), f_{P^{-1}}(e_3), f_{P^{-1}}(e_4))$$

Thus, we simply have to compute P^{-1} (i.e. the inverse of the operations we did on the rows) and take the last three columns of this matrix as this nice basis. Thus we have to find P, and for this we need to keep track of the *line* operations we performed on A to find the Smith normal form. By revisiting the solution of (1), this gives

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

so

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ -1 & 3 & 1 & 1 \end{pmatrix}.$$

Thus, a nice basis is given by the images of $f_1 := e_2 + 3e_4$, $f_2 := e_3 + e_4$ and $f_3 = e_4$. In M, they satisfy the relations $2f_1 = 0$, $26f_2 = 0$ (and f_3 satifies no non-trivial relation).

□

Exercise 3. Let $R = \mathbb{Q}[x]$. Find a direct sum of cyclic R-modules isomorphic to the R-module with generators e_1, e_2 and relations

$$x^2 e_1 + (x+1)e_2 = 0$$
$$(x^3 + 2x + 1)e_1 + (x^2 - 1)e_2 = 0$$

.

Proof. As before, we get a homomorphism $R^2 \to M$ with kernel K, which is given by the image of the map $R^2 \to R^2$ defined by the matrix

$$\begin{pmatrix} x^2 & x^3 + 2x + 1 \\ x + 1 & x^2 - 1 \end{pmatrix}$$

We put this into Smith normal form. We have that the ideal $(x^2, x+1) = 1$ and $1 \times x^2 + (1-x)(1+x) = 1$. The first step in the algorithm therefore tells us to multiply from the left by the matrix

$$\begin{pmatrix} 1 & 1-x \\ -(x+1) & x^2 \end{pmatrix}.$$

We get

$$\begin{pmatrix} 1 & 1-x \\ -(x+1) & x^2 \end{pmatrix}\begin{pmatrix} x^2 & x^3+2x+1 \\ x+1 & x^2-1 \end{pmatrix} = \begin{pmatrix} 1 & 3x+x^2 \\ 0 & -(3x^2+3x+x^3+1) \end{pmatrix}$$

By an elementary column operation this gives:

$$\begin{pmatrix} 1 & 0 \\ 0 & -(x+1)^3 \end{pmatrix}$$

So this means that there is a different set of generators f_1 and f_2 of M that satisfies the relations: $f_1 = 0$ and $(x+1)^3 f_2 = 0$, hence:

$$M \cong \mathbb{Q}[x]\big/(x+1)^3$$

$\square$

Exercise 4. Give an example of an infinitely generated $\mathbb{Z}$-module which is *not* an (infinite) direct sum of copies of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for various choices of n.

Proof. We claim that an example is given by $\mathbb{Q}$ as a $\mathbb{Z}$-module. Indeed, assume for sake the of contradiction that $\mathbb{Q} \cong \mathbb{Z}^{\oplus I} \oplus \bigoplus_i \mathbb{Z}/n_i$ for some set I and some $n_i \geq 2$. Since $\mathbb{Q}$ is torsion-free we see that the sum of $\mathbb{Z}/n_i$ is empty. To prove that $\mathbb{Q}$ is not a free module, we observe that every two cyclic (isomorphic to $\mathbb{Z}$) submodules of $\mathbb{Q}$ intersect. Indeed, let p_1/q_1 and p_2/q_2 be two rational number belonging to two different cyclic modules. Then $p_1p_2 = q_1p_2 \cdot p_1/q_1 = p_1q_2 \cdot p_2/q_2$ is an element in the intersection. Therefore, if $\mathbb{Q}$ is free, then it must be generated by a single element, i.e. $\mathbb{Q} \cong \mathbb{Z}$, which of course is a contradiction.

An other way to show that $\mathbb{Q} \ncong \mathbb{Z}^{\oplus I}$ for any I, is to notice that the endomorphism $(\cdot 2) : a \mapsto 2a$ is surjective on $\mathbb{Q}$, but not on $\mathbb{Z}^{\oplus I}$.

$\square$

Exercise 5. Let $R = \mathbb{Z}[x]$ and consider the matrix $A = \begin{pmatrix} 2 & x \\ 0 & 0 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(R)$.

(1) Show that A is not equivalent to a diagonal matrix. The equivalence that we consider here is the one introduced in the lectures, that is, up to left or right multiplication by an invertible matrix.
(2) Show that the cokernel of the map $A : R^{\oplus 2} \to R^{\oplus 2}$ is isomorphic to a direct sum of cyclic R-modules, but is not isomorphic to an R-module of the form $R^{\oplus m} \oplus \bigoplus_{i=1}^n R/(a_i)$ where $a_1, \dots, a_n \in R \setminus \{0\}$.
(3) Show that $(2, x)$ is not isomorphic to a direct sum of cyclic R-modules.

Proof. (1) We will show that A is not equivalent to a diagonal matrix. Suppose that $A' = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ is equivalent to A. Then $\mathrm{rank}(A') = \mathrm{rank}(A) = 1$ and therefore $\lambda_i = 0$

for $i=1$ or $i=2$. By multiplying from the left and the right by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we may assume that $\lambda_2 = 0$ (and denote $\lambda = \lambda_1$ from now on). Then there exists invertible matrices $S = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$ and $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$ such that $SA = A'T$, i.e.

$$\begin{pmatrix} 2s_{11} & xs_{11} \\ 2s_{21} & xs_{21} \end{pmatrix} = \begin{pmatrix} \lambda t_{11} & \lambda t_{12} \\ 0 & 0 \end{pmatrix}$$

Since $\mathbb{Z}[x]$ is a UFD, the equality $2s_{11} = \lambda t_{11}$ and $xs_{11} = \lambda t_{12}$ implies that there exists some $t' \in \mathbb{Z}[x]$ such that $t_{11} = 2t'$ and $t_{12} = xt'$. Since the units of $\mathbb{Z}[x]$ are precisely ± 1, we obtain $\pm 1 = \det(T) = t_{11}t_{22} - t_{12}t_{21} = 2t't_{22} - xt't_{21}$. This implies that the ideal $(2, x)$ contains 1, a contradiction.

(2) Let M be the cokernel of $A : \mathbb{Z}[x]^2 \to \mathbb{Z}[x]^2$. It is straightforward to see that $M \cong \mathbb{Z}[x]/(2,x) \oplus \mathbb{Z}[x]$, which is a direct sum of cyclic R-modules. Suppose by contradiction that there exist $a_1, ..., a_n \in \mathbb{Z}[x] \setminus \{0\}$ and $m \geq 0$ such that

$$\mathbb{Z}[x]/(2,x) \oplus \mathbb{Z}[x] \cong (\mathbb{Z}[x])^{\oplus m} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}[x]/(a_i).$$

Then the torsion-submodules of the LHS and RHS must be isomorphic, i.e.

$$\mathbb{Z}[x]/(2,x) \cong \bigoplus_{i=1}^{n} \mathbb{Z}[x]/(a_i).$$

But thus the annihilators of the LHS and the RHS must agree. For the LHS the annihilator is $(2, x)$, while for the RHS it is $\bigcap_{i=1}^{n}(a_i)$. But as $\mathbb{Z}[x]$ is a UFD, the latter is a principal ideal (generated by the least common multiple of the a_i's), while the former isn't principal. This is the desired contradiction.

(3) Suppose by contradiction that $\varphi : (2,x) \xrightarrow{\cong} \bigoplus_{i \in I} M_i$ is an isomorphism, where $\{M_i\}_{i \in I}$ is a family of cyclic R-modules. For all $i \in I$, let $f_i \in (2,x)$ be such that $\varphi(f_i)$ is a generator of M_i. Then $f_i f_j$ is in the intersection $\varphi^{-1}(M_i) \cap \varphi^{-1}(M_j)$, while the intersection $M_i \cap M_j$ inside $\bigoplus_{i=1}^{n} M_i$ is equal to 0. Therefore all but one of the M_i's must be trivial. But then $(2,x)$ is principal, which is a contradiction as well.

□

Exercise 6. Show that an exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$$

of R-modules induces an exact sequence

$$0 \longrightarrow \mathrm{Tors}(M) \longrightarrow \mathrm{Tors}(N) \longrightarrow \mathrm{Tors}(L)\ ,$$

but not necessarily an exact sequence

$$0 \longrightarrow \mathrm{Tors}(M) \longrightarrow \mathrm{Tors}(N) \longrightarrow \mathrm{Tors}(L) \longrightarrow 0\ .$$

Proof. It is clear that any homomorphism ϕ takes torsion to torsion, hence the sequence is well defined. Since restriction of an injection obviously is injective it is sufficient to check exactness in the middle.

Let $f : M \to N$ and $g : N \to L$ be the morphisms in question. Since $g \circ f = 0$, the same is true for the restriction to any submodules. Let $n \in \mathrm{Ker}(\mathrm{Tors}(g))$, there exists an $m \in M$ such that $f(m) = n$, we need to show that $m \in \mathrm{Tors}(M)$. Since there exists $r \in R$ not zero-divisor such that $0 = rn = f(rm)$ we have $rm \in \mathrm{Ker}(f)$, but f is injective. Hence $rm = 0$ and $m \in \mathrm{Tors}(M)$.

We have a surjection of $\mathbb{Z}$-modules $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, but it does not induce a surjection on torsion submodules. □

Exercise 7. Let $M \in \mathrm{Mat}(n \times n, k)$ for a field k. Show that there is a basis with respect to which M is block diagonal with blocks of the form

$$\begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \ddots & 0 & a_1 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & 0 & a_{d-2} \\ 0 & 0 & \dots & 1 & a_{d-1} \end{pmatrix}$$

Hint: M acts naturally on some n-dimensional k-vector space V. Consider V as a $k[x]$-module via $f \cdot v = f(M)(v)$ and use the classification of finitely generated modules over a PID.

Proof. As k is a field, $k[x]$ is a PID. Also, V is finite dimensional over k, so it is finitely generated (by a k-basis) over $k[x]$. Therefore the structure theorem says that $V \cong k[x]^{\oplus l} \oplus \bigoplus_{i=0}^{m} k[x]/(f_i)$ for some monic polynomials f_i of degree d_i. As V is finite dimensional over $k \subset k[x]$, and $k[x]$ itself is not, we see that $l = 0$. Decompose V into $\oplus_{i=0}^{m} V_i$ where $V_i \cong k[x]/(f_i)$, noting that V_i is d_i-dimensional as a k-vector space. Note that M preserves each V_i as it is a sub-$k[x]$-module of V. Thus if we choose a basis of V which is a union of bases of the V_i, the matrix of ϕ is block diagonal with blocks corresponding to the V_i. We now show that if we choose these bases in a particular way, we get the required form.

The action of M on V_i corresponds under this isomorphism to the k-linear map "multiplication by x" on $k[x]/(f_i)$. We choose the basis of V_i to be the elements which correspond via the isomorphism to the elements $\{1, x, \dots, x^{d_i - 1}\}$ of $k[x]/(f_i)$. It is clear that these span, and are linearly independent. If we define a_i by $f_i(x) = x^{d_i} - \sum_{j=0}^{d_i - 1} a_j x^j$ then the matrix of the linear map given by multiplication by x on $k[x]/(f_i)$ has the required form. □