EPFL - Fall 2024	Domenico Valloni
Rings and modules	**Exercises**
Sheet 1 - Solutions	

Exercise 1. (1) A simple module is a module that has only trivial submodules. Show that any simple module is cyclic.

(2) Let $m \in M$ be an element. We define the annihilator of m by

$$\operatorname{Ann}_R(m) = \{ r \in R \mid rm = 0 \}$$

We only write $\operatorname{Ann}(m)$ if it the base ring is clear from the context.

Show that $\operatorname{Ann}(m)$ is a left ideal of R and that the cyclic module Rm is isomorphic to the module $R/\operatorname{Ann}(m)$.

(3) Let M be a simple $k[x]$-module. Prove that $M \cong k[x]/(f)$ where f is an irreducible polynomial in $k[x]$ and (f) denotes the ideal generated by f.

(4) Which of the following $\mathbb{Z}$-modules are simple?
  (a) $\mathbb{Z}$
  (b) $\mathbb{Z}/6\mathbb{Z}$
  (c) $\mathbb{Z}/7\mathbb{Z}$

Proof. (1) If $M = 0$ then $M = R \cdot 0$ and the assertion is true. Otherwise let $m \in M \setminus \{0\}$. Then Rm is a left submodule of M. Since $Rm \neq 0$ and M is simple we conclude that $Rm = M$.

(2) We define a homomorphism of left R-modulues $\Phi_m : {}_RR \to Rm$ by $\Phi_m(r) = rm$. The kernel of Φ_m is by definition the set of elements $r \in R$ such that $rm = 0$, i.e., $\ker(\Phi_m) = \operatorname{Ann}(m)$. This proves that $\operatorname{Ann}(m)$ is a left ideal of R and that $Rm \cong R/\operatorname{Ann}(m)$.

(3) By (1) and (2), M is isomorphic to $k[x]/\operatorname{Ann}(m)$ for some $m \in M$. Let $\operatorname{Ann}(m) = (f)$ for some $f \in k[x]$ (recall that $k[x]$ is a PID); we need to prove that f is irreducible. To this end let g divide f, then $k[x] \cdot (g + (f))$ is a left $k[x]$-submodule of $k[x]/(f)$. Since by assumption $M \cong k[x]/(f)$ is simple we must have that $k[x] \cdot (g + (f)) = 0$ or $k[x] \cdot (g + (f)) = k[x]/(f)$, which implies that either f divides g or $(f, g) = (1)$. As g divides f, this means that either $g = f$ or $g = 1$ (up to multiplication by a unit). Thus f is irreducible.

(4) Notice that the $\mathbb{Z}$-submodules of $\mathbb{Z}/n\mathbb{Z}$ are exactly the ideals of $\mathbb{Z}/n\mathbb{Z}$ seen as a ring. Hence $\mathbb{Z}/n\mathbb{Z}$ is a simple $\mathbb{Z}$-module if and only if it has no non-zero proper ideals. As you know a commutative ring has no non-zero proper ideals if and only if it is a field, in particular only (c) gives a simple $\mathbb{Z}$-module.

□

Exercise 2. Let R be a ring, M a left R-module and $m \in M$.

(1) In the previous exercise you proved that $\operatorname{Ann}(m)$ is a left ideal of R. Give an example to show that $\operatorname{Ann}(m)$ might *not* be a two sided ideal of R.

(2) Define the *annihilator* of M to be

$$\operatorname{Ann}_R(M) = \{ r \in R \mid rM = 0 \} = \{ r \in R \mid \forall m \in M \colon rm = 0 \}$$

Prove that $\operatorname{Ann}(M)$ is a two sided ideal of R.

(3) Let $\phi : S \to R$ be a surjective homomorphism of rings and M a module over S. Show that we can endow an R-module structure given by $r \cdot m = s \cdot m$ for any $s \in \phi^{-1}(r)$ and $m \in M$ if and only if $\ker \phi \subseteq \mathrm{Ann}(M)$.

(4) For example, let $S = k[x]$ and $M = k[x]$ (with the standard action). Then M/f^2M is a $k[x]/(f^2)$-module for any $0 \neq f \in k[x]$. In addition, if f is not invertible, then M/f^2M is not a $k[x]/(f)$-module.

Proof. (1) We need to consider a non-commutative ring R to create an example, since left and right ideals coincide in commutative rings. The first example of a non-commutative ring R that comes to mind will suffice. That is, let R be the ring of 2×2 matrices over some field k. To keep things as simple as possible we consider R as a left R-module by left multiplication. Let $0 \neq a \in k$, we will calculate the annihilator of $m_a = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$. Hence we are interested in solving the matrix equation

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

The solutions are exactly the matrices with $b_{11} = b_{21} = 0$, and thus $\mathrm{Ann}(m_a) = \left\{ \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \mid b, c \in k \right\}$. This is not a right ideal of R because multiplying such an element from the right with an arbitrary matrix in R does in general not give a matrix of this form. For example multiplication from the right with $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ gives b in the top left corner of the matrix, so this top left entry is non-zero whenever b is.

(2) Let $r, s \in \mathrm{Ann}(M)$ and $l \in R$. Then $l(r+s)m = l(rm+sm) = 0$ and $(r+s)lm = r(lm) + s(lm) = 0$.

(3) Assume first $\ker(\phi) \subseteq \mathrm{Ann}(M)$, and let $r \in R$, $m \in M$ and s, $s' \in \phi^{-1}(r)$. Then $s - s' \in \ker(\phi)$, so by assumption

$$0 = (s - s')m = sm - s'm$$

so that $sm = s'm$. Thus, at least the map $R \times M \to M$ sending $(r, m) \to r \cdot m$ is well-defined. The module axioms are then straight-forward to see.

Now assume that the action is well defined. Then in particular for any $s \in \ker(\phi) = \phi^{-1}(0)$ and $m \in M$,

$$sm = 0$$

In other words $\ker(\phi) \subseteq \mathrm{Ann}(M)$.

(4) Clearly, $f^2 \in \mathrm{Ann}(M/f^2M)$, so by the previous point we get that M/f^2M is an $k[x]/(f^2)$-module via the above procedure.

Assume now that $f \neq 0$ is not invertible, and assume by contradiction that M/f^2M in an $R/(f)$-module via the above procedure. Then by the previous point, $f \in \mathrm{Ann}(M/f^2M)$, so in particular

$$f = f \cdot 1 \in f^2M = f^2k[x]$$

so there exists $c \in k[x]$ such that $cf^2 = f$. Since R is a domain, we get

$$cf = 1$$

which contradicts the fact that f is not invertible.

□

Exercise 3. Answer the following questions. Provide an explanation by a proof or a counterexample.

(1) Suppose that R is a Noetherian ring. Let $S \subset R$ be a subring. Is it true that S is Noetherian?
(2) Let R be a commutative Artinian ring. Is every prime ideal of R maximal?

Proof. (1) It is not necessarily true that S is Noetherian. A counterexample is given by an inclusion of any non-Noetherian integral domain (e.g., $k[x_1, x_2, \dots]$) into its fraction field (clearly Noetherian).
(2) Let $\mathfrak{p}$ be a prime ideal of R. Since there exists a correspondence between ideals in $R/\mathfrak{p}$ and ideals in R containing $\mathfrak{p}$, we know that $R/\mathfrak{p}$ is an Artinian integral domain. Let $x \in R/\mathfrak{p}$ be a non-zero element. The sequence of ideals $((x^n))_{n\geq 0}$ is decreasing and hence by Artinianity it stabilizes, which means that $x^n = ux^{n+1}$ for some $u \in R/\mathfrak{p}$ and $n \in \mathbb{N}$. Since $R/\mathfrak{p}$ is a domain, and we have $x^n(1-ux) = 0$ and thus $ux = 1$, which proves that x is invertible. So every non-zero element of $R/\mathfrak{p}$ is invertible, and thus $R/\mathfrak{p}$ is a field. Therefore $\mathfrak{p}$ is maximal inside R.

□

Exercise 4. Let $I \subseteq R$ be an ideal.

(1) Show that
$$IM = \left\{ \sum_{i=1}^{d} r_i m_i \;\middle|\; 1 \leq d \in \mathbb{Z},\ r_i \in I,\ m_i \in M \right\}$$
is an R-submodule of M.
(2) Show that M/IM is an R/I-module with scalar multiplication given by
$$(x+I)(y+IM) = xy + IM.$$

From now, let $R = k[x,y]$, let M be the R-submodule generated by the element $(x,y) \in R \oplus R = N$, and let I be the maximal ideal $I = Rx + Ry$ of R. Note that $R/I \cong k$ via the homomorphism $R \to k$ that evaluates x and y to 0.

(3) Show that $M \subseteq IN$ and hence $I\left(N/M\right) = IN/M$ as R-submodules of N/M.
(4) Show that L/IL is a two dimensional vector-space over k, where $L = N/M$
[Hint: use point (3) and the third isomorphism theorem]

Now, we change a little bit our setup, and we redefine M:

(5) Let M be the submodule generated by the two elements $(x,0)$ and $(0,y)$ of $R \oplus R = N$. Is $N/M \cong R$?
[Hint: look at $\mathrm{Ann}\left(N/M\right)$.]

Proof. (1) We need to prove that IM is an additive subgroup and that it is stable under multiplication by elements of R. By comparing definitions (i.e. that of IM above and that of a subgroup generated by a subset), IM is in fact the subgroup of M generated by the set $\{rm \mid r \in I,\ m \in M\}$, so IM is an additive subgroup of M. On the other hand, we have for all $r \in R$ that

$$r \cdot (IM) = \left\{ \sum_{i=1}^{d} \underbrace{rr_i}_{\in I} m_i \;\middle|\; 1 \le d \in \mathbb{Z},\ r_i \in I,\ m_i \in M \right\} \subseteq IM$$

as I is a left ideal. Thus $IM \le_R M$.

(2) One can prove this by simple (but tedious) verification of well-definedness and of all the axioms. But let us give a more conceptual proof. An abelian group M has a left R-module structure if and only if we have a ring morphism $\lambda : R \to \mathrm{End}_{\mathrm{Ab}}(M)$ (where the multiplication law on the latter is given by composition): if M is an R-module then we can define $\lambda(r) \in \mathrm{End}_{\mathrm{Ab}}(M)$ to be left multiplication by r, and conversely if $\lambda : R \to \mathrm{End}_{\mathrm{Ab}}(M)$ is a ring morphism then $r.m := \lambda(r)(m)$ endows M with the structure of an R-module.
Now let $\lambda : R \to \mathrm{End}_{\mathrm{Ab}}\left(M/IM\right)$ be the ring morphism corresponding to the R-module structure on M/IM. If $r \in I$, then multiplication by r on M/IM is the zero map, and thus $r \in \ker(\lambda)$. As thus $I \subseteq \ker(\lambda)$, we obtain an induced ring morphism $\overline{\lambda} : R/I \to \mathrm{End}_{\mathrm{Ab}}\left(M/IM\right)$, given by $\overline{\lambda}(r + I) = \lambda(r)$ for all $r \in R$. Hence, $\overline{\lambda}$ endows M/IM with the structure of an R/I-module, given explicitly by

$$(x + I)(y + IM) = \overline{\lambda}(x + I)(y + IM) = \lambda(x)(y + IM) = xy + IM.$$

(3) Let $m \in M$ be arbitrary, then there exists a polynomial $f \in R$ such that $m = (xf, yf)$. Thus $m = x \cdot (f, 0) + y \cdot (0, f) \in IN$, and so we obtain $M \subseteq IN$. In particular, IN/M is a well-defined R-submodule of N/M. To conclude, notice that

$$\begin{aligned} I\left(N/M\right) &= \left\{ \sum_{i=1}^{d} r_i(n_i + M) \;\middle|\; 1 \le d \in \mathbb{Z},\ r_i \in I,\ n_i \in N \right\} \\ &= \left\{ \underbrace{\left(\sum_{i=1}^{d} r_i n_i\right)}_{\in IN} + M \;\middle|\; 1 \le d \in \mathbb{Z},\ r_i \in I,\ n_i \in N \right\} \\ &= \left\{ \textstyle\sum_{i=1}^{d} r_i n_i \;\middle|\; 1 \le d \in \mathbb{Z},\ r_i \in I,\ n_i \in N \right\} \Big/ M = IN/M. \end{aligned}$$

(4) By (3) we have

$$L/IL \overset{(3)}{=} \left(N/M\right) \Big/ \left(IN/M\right) \cong N/IN$$

by the third isomorphism theorem. Now observe that the map

$$\begin{aligned} N &\to R/I \oplus R/I \\ (f, g) &\mapsto (f + I, g + I) \end{aligned}$$

is surjective and has kernel IN (verify it!). Thus, as by the remark above (3) we have $R/I \cong k$ (can you describe the R-module structure on k given by this isomorphism?), we obtain by the first isomorphism theorem that $N/IN \cong k \oplus k$.

(5) Let $(f, g) \in N$ be arbitrary. Then $xy(f, g) = fy(x, 0) + gx(0, y) \in M$, and thus $xy((f, g) + M) = 0$ inside N/M. As $(f, g) \in N$ was arbitrary, we obtain $xy \in$

$\mathrm{Ann}(N/M)$. On the other hand, as R is a domain, we have $\mathrm{Ann}({}_R R) = (0)$. As the annihilator is preserved under R-module isomorphisms, we thus have $N/M \ncong R$.

□

Exercise 5. Let

$$0 \to M \to N \to N/M \to 0$$

be a short exact sequence of R-modules. For each of the following assertions either prove that the assertion holds or provide a counterexample.

(1) If M and N/M are finitely generated, then N is too.
(2) Conversely, if N is finitely generated, then N/M is finitely generated too.
(3) If N is finitely generated, then M is finitely generated too.

Proof. (1) As M is finitely generated, we can find a subset $\{m_1, \ldots, m_k\} \subseteq M$ generating M as an R-module, and as N/M is finitely generated we can find a subset $\{n_1 + M, \ldots, n_l + M\} \subseteq N/M$ generating N/M as an R-module.
We claim that N is generated by $\{m_1, \ldots, m_k, n_1, \ldots, n_l\}$. Given $n \in N$, we can write $n + M = \sum_{j=1}^{l} s_j(n_j + M)$ for some $s_j \in R$, and so $n - \sum_{j=1}^{l} s_j n_j \in M$. But then there exist $r_i \in R$ such that $n - \sum_{j=1}^{l} s_j n_j = \sum_{i=1}^{k} r_i m_i$. This exhibits n as an R-linear combination of the m_i's and n_j's and so N is generated by these elements.

(2) The statement is true. Suppose $\{n_1, \ldots n_k\}$ generate N, then in fact $\{n_1 + M, \ldots, n_k + M\}$ generates N/M. Indeed any $n + M \in N/M$ can be written as

$$n + M = \left(\sum_{i=1}^{k} r_i n_i\right) + M = \sum_{i=1}^{k} r_i(n_i + M)$$

and thus $n + M$ is an R-linear combination of the $n_i + M$'s.

(3) This statement is not true. Take $R = \mathbb{C}[x_1, x_2, ...]$, the polynomial ring in infinitely many variables. (An element of R is by definition a polynomial in finitely many of the variables $x_1, x_2, ...$, and addition and multiplication are then exactly what one would think it is).

Let N be R viewed as a module over itself, and take the submodule M to be generated by $\{x_1, x_2, ...\}$. This is a proper submodule, as it does not contain the constants $\mathbb{C} \subset N$. Any element of M is a polynomial $f(x_1, ..., x_i)$ with no constant term. Given a finite set of such polynomials $\{f_i\} \subset M$, there is an integer I such that any element contained in $\langle\{f_i\}\rangle$ can be written as a linear combination of monomials, each of which has positive degree in some x_i with $i < I$. So this span cannot be equal to all of M, as it does not contain x_n for $n \gg 0$.

Note: the statement in (3) is true for modules over an important class of rings called Noetherian rings. These include many common rings such as fields k, $\mathbb{Z}$, and $k[x_1, ..., x_n]$. So $\mathbb{C}[x_1, x_2, ...]$ is an example of a non-Noetherian ring.

□

Exercise 6. (1) Let

$$0 \to M \to N \to N/M \to 0$$

be a short exact sequence of R-modules. For each of the following assertions either prove that the assertion holds or provide a counterexample.

- If N is free, then ${}^{N}\!/_{M}$ is free.
- If N is free, then M is free.
- If M and ${}^{N}\!/_{M}$ are free, then N is free.

(2) Let $R = \mathbb{Z}$. Is $\mathbb{Z}[x]\big/(x^2+1)\mathbb{Z}[x]$ a free R-module? How about $\mathbb{Z}[x]\big/(2x^2)\mathbb{Z}[x]$? Is $\mathbb{Q}$ a free R-module? Is it finitely generated?

Proof. A module is free if it is isomorphic to $\bigoplus_I R$ for some (possibly infinite) indexing set I.

Digression:

Definition 1. A subset $\{m_i\} \subset M$ is a basis for M if:

- It spans M: every $m \in M$ can be written as $m = \sum r_i m_i$ for some $r_i \in R$.
- It is linearly independent: if $\sum r_i m_i = 0$ for $r_i \in R$ then $r_i = 0$ for each i.

Lemma 1. *The module M is free if and only if it has a basis.*

Proof. Assume M is free, so $M \cong \bigoplus_I R$. We can define a basis $\{e_i\}_I$ for M where e_i is 1 in its i^{th} position and zero elsewhere. It is straightforward that these span and are linearly independent. Conversely suppose we have a module M which has a basis $\{e_i\}_{i\in I}$. Define $\phi : \oplus_I R \to M$ by extending linearly from $\phi((\delta_{i,j})_{j\in I}) = e_i$ for each $i \in I$. This is surjective, because any $m \in M$ can be written as a linear combination of the e_i and each of these is in the image. It is injective, because if not there is some non-zero element of $\oplus_I R$ killed by ϕ. But this gives a non-trivial linear dependence among the e_i in M. □

Now we return to the solution.

(1)
- This is false: a counterexample is given by $R = \mathbb{Z}$, $N = \mathbb{Z}$, $M = 2\cdot\mathbb{Z}$, for then $N/M \cong \mathbb{Z}/2\mathbb{Z}$.
- This is also false: a counterexample is $R = \mathbb{Z}/4\mathbb{Z}$, $N = \mathbb{Z}/4\mathbb{Z}$ and $M = 2\cdot\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. This has too few elements to be a free $\mathbb{Z}/4\mathbb{Z}$-module.
- This is true. Suppose M has basis $\{m_1,\dots,m_k\}$ and N/M has basis $\{n_1 + M,\dots,n_l + M\}$. We claim that $\{m_1,\dots,m_k,n_1,\dots,n_l\}$ is a basis for N. They span by the argument in Exercise 4.1. For linear independence: suppose $\sum s_j n_j + \sum r_i m_i = 0$. This implies $\sum s_j(n_j + M) = 0$ in N/M and so the s_j's are all zero by the linear independence of the $n_j + M$'s. But then $\sum r_i m_i = 0$ is a linear dependence for a basis of M, forcing also the r_i's to be zero as well.

(2)
- $\mathbb{Z}[x]/(x^2+1)\mathbb{Z}[x]$ is a free $\mathbb{Z}$-module, with basis $\{1, x\}$ (it is isomorphic to $\mathbb{Z}[i]$).
- $\mathbb{Z}[x]/(2x^2)\mathbb{Z}[x]$ is not free since x^n is a torsion element for all $n \geq 2$ (as $x^n \notin (2x^2)$ but $2x^n \in (2x^2)$).
- $\mathbb{Q}$ is not a free $\mathbb{Z}$ module. Indeed, any two elements of $\mathbb{Q}$ are $\mathbb{Z}$-linearily dependet: if $a/b, c/d \in \mathbb{Q}$ then either both are equal to zero, or $cb(a/b) - ad(c/d) = 0$ is a non-trivial $\mathbb{Z}$-linear relation. Thus if $\mathbb{Q}$ was a free $\mathbb{Z}$-module, then it must be generated by a single element, which is impossible. For example, this can be seen by the second part of the question:
  $\mathbb{Q}$ is not finitely generated over $\mathbb{Z}$ since if $\{\frac{p_1}{q_1},\dots,\frac{p_n}{q_n}\}$ is a generating set, let $q = q_1\cdots q_n$. Then $\frac{1}{q+1}$ does not lie in the $\mathbb{Z}$-span of $\{\frac{p_1}{q_1},\dots,\frac{p_n}{q_n}\}$.

□

Optional exercise. Not on the exam. Suggested if you are seriously interested in algebra.

Exercise 7. Let k be a field. In this exercise, we want to understand *differential operators* on $k[x]$. To this end, define the operator $\frac{\partial}{\partial x}\,\mathrm{End}_k(k[x])$ by the usual rule

$$\frac{\partial}{\partial x}(x^n) := nx^{n-1}.$$

Define also $x \in \mathrm{End}_k(k[x])$ defined by multiplication by x. Finally, define the subring $\mathcal{D} \subseteq \mathrm{End}_k(k[x])$ to be the sub-k-algebra generated by x and $\frac{\partial}{\partial x}$.

We will show that this non-commutative rung behaves very differently, whether we work in characteristic zero or in positive characteristic.

(1) Show that a basis of $\mathcal{D}$ as a k-vector space is given by the elements $x^i\left(\frac{\partial}{\partial x}\right)^j$, where $(i,j) \in \mathbb{N}^2$ if $\operatorname{char} k = 0$, and $i \in \mathbb{N}$ and $j \in \{0,1,\dots,p-1\}$ if $\operatorname{char} k = p > 0$.

(2) Now we change the perspective and consider a quotient of the free k-algebra on two generators $\mathcal{D}^{form} = k\langle u,v\rangle/(uv - vu - 1)$. Prove that in $\mathcal{D}^{form}$ we have the identity

$$uP(v) = \frac{\partial}{\partial v}P(v) + P(v)u$$

for all polynomials $P(v) \in k[v]$. Use this to prove that $\mathcal{D}^{form}$ is generated as a k-vector space by $\{v^j u^i \mid (i,j) \in \mathbb{N}^2\}$.

(3) Show that there are well defined ring homomorphisms ϕ and ψ from $\mathcal{D}^{form}$ to $\mathrm{End}_k(k[x])$, such that $\phi(u) = \frac{\partial}{\partial x}$ and $\phi(v) = x$, as well as $\psi(u) = x$ and $\psi(v) = -\frac{\partial}{\partial x}$. Show that ϕ and ψ are surjective onto $\mathcal{D}$, and define an isomorphism betwenn $\mathcal{D}$ and $\mathcal{D}^{form}$ if and only if $\mathrm{char}(k) = 0$.

(4) Determine the submodules of $k[x]$ as a left $\mathcal{D}$-module (with left $\mathcal{D}$-module structure given by the inclusion $\mathcal{D} \subset \mathrm{End}_k(k[x])$) in the case when $\operatorname{char} k = 0$.

(5) Determine the left submodules of $k[x]$ as a $\mathcal{D}$-module when $\operatorname{char} k = 2$.

Proof. (1) Let us first show that $\mathcal{B}_1 := \{x^i\left(\frac{\partial}{\partial x}\right)^j\}_{i,j\geq 0}$ spans $\mathcal{D}$ (in any characteristic). By definition of $\mathcal{D}$ (recall that we work in a non-commutative setup), it enough to show that each $\left(\frac{\partial}{\partial x}\right)^j \circ x^i$ is spanned by $\mathcal{B}_1$. Note that

$$\frac{\partial}{\partial x}x = x\frac{\partial}{\partial x} + 1$$

(this follows from the Leibniz rule) so an induction on i and j shows that $\mathcal{B}_1$ spans $\mathcal{D}$ as a k-vector space.

Now notice that if $\mathrm{char}(k) = p > 0$ then $\left(\frac{\partial}{\partial x}\right)^j = 0$ for all $j \geq p$ (repeatedly taking derivatives more than p times will produce a factor divisible by p in front of every monomial). Thus if we let $\Omega = \mathbb{Z}^2_{\geq 0}$ if $\mathrm{char}(k) = 0$ and $\Omega = \mathbb{Z}_{\geq 0} \times \{0,\dots,p-1\}$ if $\mathrm{char}(k) = p > 0$, we obtain that already $\mathcal{B} = \{x^i\left(\frac{\partial}{\partial x}\right)^j \mid (i,j) \in \Omega\}$ generates $\mathcal{D}$.

Now we need to prove that the elements of $\mathcal{B}$ are k-linearily independent. Let $\lambda_\bullet : \Omega \to k$ be a set of finitely many non-zero coefficients in k such that $\sum_{(i,j)\in\Omega} \lambda_{i,j} x^i \left(\frac{\partial}{\partial x}\right)^j = 0$. In particular, if we evaluate the expression on the LHS at 1 we obtain $\sum_{(i,0)\in\Omega} \lambda_{i,0} x^i = 0$ as element of $k[x]$, and thus $\lambda_{i,0} = 0$ for all i. Suppose we have proven $\lambda_{i,j} = 0$ for all i and all $j < J$ for some $J > 0$ (satisfying $J \le p-1$ if $\mathrm{char}(k) = p > 0$). Then we have $\sum_{(i,j)\in\Omega,\ j\ge J} \lambda_{i,j} x^i \left(\frac{\partial}{\partial x}\right)^j = 0$, and evaluating the LHS at x^J shows that $\lambda_{i,J} = 0$ for all i. By induction, we conclude that $\lambda_{i,j} = 0$ for all $(i,j) \in \Omega$. Thus $\mathcal{B}$ is a basis of $\mathcal{D}$.

(2) Inside $\mathcal{D}^{form}$, we can use the relation $uv - vu - 1 = 0$ to swap the u's and v's in any given monomial. Let us make this precise. By induction on j, one proves

$$uv^j = \frac{\partial}{\partial v} v^j + v^j u$$

inside $\mathcal{D}^{form}$ (i.e. modulo $uv - vu - 1$). The formula in question then follows by k-linearity. Multiplying the formula by powers of u, it then follows also more generally that

$$u^i P(v) = \sum_{k=0}^{i} \left(\frac{\partial}{\partial v}\right)^k (P(v)) \cdot u^{i-k}.$$

In particular, we have a formula to replace any monomial $u^i v^j$ by an expression where in all monomials v is to the left of u. By using this iteratively, moving all v's to the left, one can express every element of $\mathcal{D}^{form}$ as a sum of monomials of the form $v^j u^i$. That is, $\mathcal{B}^{form} := \{v^j u^i \mid i, j \in \mathbb{Z}_{\ge 0}\}$ is a generating set of $\mathcal{D}^{form}$ as a k-vector space.

(3) By the universal property of the free k-algebra on two generators, there exists a k-algebra morphism $\Phi : k\langle u, v\rangle \to \mathrm{End}_k(k[x])$ mapping $u \mapsto \frac{\partial}{\partial x}$ and $v \mapsto x$. To show that Φ factors through $\mathcal{D}^{form}$, it suffices to prove that $uv - vu - 1$ is in the kernel of Φ. This amounts to proving that for all $f \in k[x]$ we have $\frac{\partial}{\partial x}(xf(x)) = f(x) + x\frac{\partial}{\partial x} f(x)$, which follows from the (algebraic) Leibnitz-rule. Therefore, we obtain the well-defined $\phi : \mathcal{D}^{form} \to \mathrm{End}_k(k[x])$ mapping $u \mapsto \frac{\partial}{\partial x}$ and $v \mapsto x$.

Now as $\mathcal{D}$ contains $\frac{\partial}{\partial x}$ and x, the image of ϕ is contained in $\mathcal{D}$. On the other hand, as every element of $\mathcal{B}$ is attained by ϕ (evaluating at $v^i u^j$), we obtain that the image is exactly $\mathcal{D}$, i.e. ϕ is surjective onto $\mathcal{D}$.

By repeating the same argument for $\Psi : k\langle u, v\rangle \to \mathrm{End}_k(k[x])$ mapping $u \mapsto x$ and $v \mapsto -\frac{\partial}{\partial x}$, we obtain also the desired map $\psi : \mathcal{D}^{form} \to \mathrm{End}_k(k[x])$, surjective onto $\mathcal{D}$.

Now finally we investigate when the surjective morphism $\phi : \mathcal{D}^{form} \to \mathcal{D}$ is also injective. If $\mathrm{char}(k) = p > 0$ then u^p is mapped to $\left(\frac{\partial}{\partial x}\right)^p$, which as we have seen is equal to 0 inside $\mathcal{D}$. To conclude that ϕ isn't injective, it remains to show that u^p isn't equal to 0 inside $\mathcal{D}^{form}$. This can be seen via ψ, because $\psi(u^p)$ is the k-endomorphism of $k[x]$ given by multiplication with x^p, which is not the zero map. So u^p is non-zero inside $\mathcal{D}^{form}$, and hence ϕ is not injective. The same argument, replacing u and v, shows that ψ is not injective either.

It remains to consider the case where $\mathrm{char}(k) = 0$. We have seen that $\mathcal{B}^{form} := \{v^j u^i \mid i, j \in \mathbb{Z}_{\ge 0}\}$ generates $\mathcal{D}^{form}$ over k, and in characteristic zero $\mathcal{B} = \{x^i \left(\frac{\partial}{\partial x}\right)^j \mid i, j \in \mathbb{Z}_{\ge 0}\}$ is a k-basis of $\mathcal{D}$. But then ϕ induces a bijection between $\mathcal{B}^{form}$ and $\mathcal{B}$, and thus we obtain that $\mathcal{B}^{form}$ is also linearily independent, and thus a k-basis. Therefore ϕ induces a bijection between two bases, and is thus a vector-space isomorphism. In particular, ϕ is injective, and hence $\mathcal{D}^{form} \cong \mathcal{D}$ in characteristic zero. The argument for ψ is completely analogous.

(4) We claim that $k[x]$ is a simple $\mathcal{D}$-module. First note that $k[x]$ is generated as a $\mathcal{D}$-module by the element $1 \in k[x]$, because for any $f(x) \in k[x]$, the k-endomorphism of $k[x]$ given by multiplcation with $f(x)$ is an element of $\mathcal{D}$, and the image of 1 under this endomorphism is $f(x)$. Hence any element of $k[x]$ can be obtained by letting some element of $\mathcal{D}$ act on 1, i.e. 1 generates $k[x]$ as a $\mathcal{D}$-module. Now suppose N is a non-zero $\mathcal{D}$-submodule of $k[x]$. We will show that $1 \in N$. As N is non-zero, it contains some non-zero element $f(x) = \sum_{i=0}^{n} a_i x^i$ (where $a_n \neq 0$). We need to find a differential operator D such that $D(f) = 1$. In fact, $D = \frac{1}{a_n n!}(\frac{\partial}{\partial x})^n$ will do it (here we use that $\mathrm{char}(k) = 0$).

(5) The first thing to note is that

$$\frac{\partial}{\partial x}(x^2) = 2x = 0.$$

Similarly $\frac{\partial}{\partial x}(x^{2n}) = 0$ any $n \in \mathbb{N}$.

Now let N be a non-zero $\mathcal{D}$-submodule of $k[x]$, and notice that N is generated by a single element. Indeed, the ring $\mathcal{D}$ contains a copy of $k[x]$ as a subring (by viewing an element p of $k[x]$ as the k-endomorphism of $k[x]$ given by left multiplication by p), and the induced $k[x]$-module structure on $k[x]$ is the natural one. Thus N is also a $k[x]$-submodule of $k[x]$, i.e. an ideal. But $k[x]$ is a PID, so N is generated by some f as a $k[x]$-module. In fact, we can take f to be the monic polynomial of minimal degree inside N (there is a unique one). As $N \neq 0$ we have $f \neq 0$, and as the derivative of f is has degree strictly smaller than f and is inside N (as N is a $\mathcal{D}$-module), we must have $\frac{\partial}{\partial x} f(x) = 0$. This means that $f(x) = \sum_{i=1}^{2n} a_i x^{2i}$ for some $a_0, \dots, a_n \in k$ with $a_n = 1$.

Finally, we show that $\mathcal{D} \cdot f = k[x] \cdot f$ as k-subspaces of $k[x]$; it suffices to show that the LHS is included in the RHS. As both sides are k-vector spaces, it suffices to prove that $\mathcal{B} \cdot f \subseteq k[x] \cdot f$. This is true as $\left(x^i \left(\frac{\partial}{\partial x}\right)^j\right) \cdot f(x) = 0$ if $j \geq 1$, and $x^i f(x) \in k[x] \cdot f$ for all $i \geq 0$.

Therefore, we conclude that the $\mathcal{D}$-submodules of $k[x]$ are exactly the subsets of the form $k[x] \cdot f$ with f monic and only having terms of even degree. Notice also that any two distinct such f give distinct submodules.

□