EPFL - Fall 2025	Zsolt Patakfalvi
Rings and modules	**Exercises**
Sheet 10 - Solutions	

Exercise 1. Let G be a finite group, R an integrally closed domain, K the fraction field of R and let G act on K by (ring) automorphisms such that R is stable under this action, i.e. $g \cdot r \in R$ for all $g \in G$ and $r \in R$. Let $L := K^G$ be the fixed field of the action and set $S := L \cap R$. In this exercise we show that S is also integrally closed.

(1) Show that each element of K can be written in the form $\frac{a}{b}$, where $a \in R$ and $b \in S$.
(2) Show that L is the fraction field of S.
(3) Show that S is integrally closed.
(4) Show that $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n] \subseteq \mathbb{C}[x, y]$ is integrally closed.
[*Hint:* Show that there is automorphism of $\mathbb{C}(x, y)$ that sends x to $e^{2\pi i/n}x$ and y to $e^{2\pi i/n}y$.]

Proof. We denote by $\cdot$ the action of G; the ring multiplication is denoted by the empty symbol.

(1) Let $\frac{c}{d} \in K$ be an arbitrary element, where $c, d \in R$. Set $x = \prod_{g \neq e_G} g \cdot d$ and $a = cx$, $b = dx$. Note that $b \neq 0$ as all the factors are non-zero (as G acts by automorphisms). Then $b = \prod_{g \in G} g \cdot d$ and thus $h \cdot b = \prod_{g \in G}(hg) \cdot d = b$ for all $h \in G$. Therefore $b \in S$ and $\frac{c}{d} = \frac{a}{b}$.
(2) As L is a field containing S, we have to show that every element of L is a fraction of elements in S. Let $x \in L$ be arbitrary; by the previous point we can write $x = \frac{a}{b}$ with $b \in S$. Now as x is fixed by the action of G, we obtain
$$\frac{a}{b} = g \cdot \frac{a}{b} = \frac{g \cdot a}{g \cdot b} = \frac{g \cdot a}{b}$$
for all $g \in G$, where in the last step we used $b \in S$. But then we obtain $a = g \cdot a$ for all $g \in G$, and thus $a \in S$. Hence x is a fraction of elements in S, which proves $\mathrm{Frac}(S) = L$.
(3) Let $x \in L$ be integral over S. Then in particular, $x \in K$ it is integral over R, and thus as R is integrally closed we have $x \in R$. Hence $x \in L \cap R = S$, and thus S is integrally closed.
(4) Denote $R = \mathbb{C}[x, y]$, $K = \mathbb{C}(x, y)$ and $\zeta := e^{2\pi i/n}$. By the universal property of $\mathbb{C}[x, y]$ there exists a $\mathbb{C}$-algebra endomorphism ϕ of R mapping x to ζx and y to ζy. This is easily seen to be bijective, and thus it induces an automorphism Φ of K such that $\Phi|_R = \phi$. But then $\Phi^{\circ n}|_R = \phi^{\circ n} = \mathrm{Id}_R$, and thus $\Phi^{\circ n} = \mathrm{Id}_K$. So let $G = \langle \Phi \rangle$ be the finite subgroup of automorphisms of K generated by Φ. If we are able to show that $S := K^G \cap R$ is equal to $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n] \subseteq \mathbb{C}[x, y]$ then we are done by the previous point. As every element of $\mathbb{C}$ and every monomial among $x^n, x^{n-1}y, \dots, xy^{n-1}, y^n$ is fixed by ϕ, we may conclude already that $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n] \subseteq S$. Now let $f \in R$ be an element fixed by ϕ, and write $f = \sum_{i,j} f_{ij} x^i y^j$. Then $f_{ij} = \zeta^{i+j} f_{ij}$ for all i, j and hence $f_{ij} = 0$ unless $i + j$ is divisible by n. If $i + j$ is divisible by n then (i, j) can be expressed as an $\mathbb{Z}_{\geq 0}$-linear combination of $(n, 0), (n-1, 1) \dots, (1, n-1), (0, n)$; simply write $i = an + b$ and $j = cn + d$ with $0 \leq b, d < n$, then $b + d \in \{0, n\}$ and

thus either $b = d = 0$ in which case $(i,j) = a(n,0) + c(0,n)$, or $b + d = n$ in which case $(i,j) = a(n,0) + c(0,n) + (b,d)$. Hence every monomial appearing in f with non-zero coefficient is inside $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n]$, and thus also f itself. Therefore $S = \mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n]$, so we are done.

□

Exercise 2. Let k be a field. For the following finitely generated k-algebras R, find a sub-algebra $S \subseteq R$ such that $S \subseteq R$ is integral and S is isomorphic to a polynomial ring:

(1) $R = k[x,y]/(xy-1)$;
(2) $R = k[x_1,x_2,x_3,y_1,y_2,y_3]/(x_1x_2x_3 + y_1y_2y_3)$;

Proof. The idea is to make a change a variable (hence an automorphism of the polynomial ring) to get an ideal which is much easier to work with (notice this is exactly what we do in the proof of Noether's normalization!).

(1) Let $z = x - y$. Then $xy - 1 = (z+y)y - 1 = y^2 + yz - 1$. Thus, $\overline{y}$ satisfies a monic equation with coefficients in $k[\overline{z}]$ which is isomorphic to a polynomial ring, so $S = k[\overline{z}] = k[\overline{x} - \overline{y}] \subseteq R$ does the job.
   Before doing the other points, let us rephrase what we have just done in a more precise way. Let x, y, z denote variables, and let $\theta : k[x,y] \to k[z,y]$ be the automorphism sending x to $z + y$. This automorphism induces
   $$k[x,y]/(xy-1) \cong k[z,y]/(z+y)y-1) = k[z,y]/(y^2+zy-1)$$
   Since $\overline{y}$ satisfies a monic equation over $k[\overline{z}]$, we know by Proposition 8.1.4 in the notes that $k[\overline{z}] \subseteq k[z,y]/(y^2+zy-1)$ is an integral extension. Therefore $k[\overline{x}-\overline{y}] \subseteq k[x,y]/(xy-1)$ is also an integral extension. Finally, $k[\overline{x}-\overline{y}] \cong k[\overline{z}]$ is isomorphic to a polynomial ring, because of the following lemma (apply it to $R = k[z]$, $f = y^2+zy+1$):

   Lemma 0.1. *Let R be a commutative ring, $f \in R[y]$ be a monic polynomial of degree at least 1. Then $R \to R[y]/(f)$ is injective.*

   Proof. If not, there exists $r \neq 0$ such that f divides r. Since f is monic and of degree at least 1, this is impossible. □

(2) Apply $x_1' = x_1 - x_3$, $x_2' = x_2 - x_3$ so that the equation becomes
   $$(x_1' + x_3)(x_2' + x_3)x_3 + y_1y_2y_3 = x_3^3 + x_3^2(x_1' + x_2') + x_3)x_1'x_2' + y_1y_2y_3$$
   which is monic as a polynomial in $k[x_1', x_2', y_1, y_2, y_3][x_3]$. Thus, as before,
   $$S = k\left[\overline{x_1} - \overline{x_3}, \overline{x_2} - \overline{x_3}, \overline{y_1}, \overline{y_2}, \overline{y_3}\right] \subseteq k[x_1,x_2,x_3,y_1,y_2,y_3]/(x_1x_2x_3 + y_1y_2y_3)$$
   works.

□

Exercise 3. Show that the ring
$$k[x,y,z]/(y^3 + y^2x^2 + yx^2 + x^3z)$$
is a domain, and compute its integral closure.

Proof. The polynomial $y^3 + y^2x^2 + yx^2 + x^3z$ is irreducible by Eisenstein's criterion for z, so this ring is indeed a domain.

For this solution, let R denote the ring we are working with, S its integral closure (which we want to find) and K its field of fractions.

Let us first show the following general statement:

Lemma 0.2. *Let R be a UFD, and let p an irreducible primitive polynomial in $R[t]$. Then*

$$\mathrm{Frac}(R[t]/(p)) \cong \mathrm{Frac}(R)[t]/(p)$$

Proof. We know by Gauss lemma that $p(t)$ is irreducible in $\mathrm{Frac}(R)[t]$, so since this ring is a PID, the quotient $\mathrm{Frac}(R)[t]/(p)$ is a field. But for any element in $\mathrm{Frac}(R)[t]/(p)$, so multiple by an element in R lands in $R[t]/p(t)$, so we win. □

By definition, we have

$$\left(\frac{\overline{y}}{\overline{x}}\right)^3 + \overline{y}\left(\frac{\overline{y}}{\overline{x}}\right)^2 + \frac{\overline{y}}{\overline{x}} + \overline{z} = 0 \tag{0.2.a}$$

so $\frac{\overline{y}}{\overline{x}}$ is integral over R. Let $\phi : k[u, v] \to R[\frac{\overline{y}}{\overline{x}}]$ be the map sending u to $\overline{x}$ and v to $\frac{\overline{y}}{\overline{x}}$.

This map is surjective, because in the image we have $\overline{x}$, $\frac{\overline{y}}{\overline{x}}$, and hence also $\overline{y}$. Finally, we have $\overline{z}$ because of equation 0.2.a.

This map is also injective, because otherwise we would obtain an isomorphism

$$T := k[u, v]/\mathfrak{p} \cong R[\frac{\overline{y}}{\overline{x}}]$$

for some non-zero prime ideal $\mathfrak{p}$. But then any element in $\mathfrak{p}$ gives an algebraic relation between $\overline{u}$ and $\overline{v}$, so

$$\mathrm{trdeg}_k(\mathrm{Frac}(T)) < 2$$

On the other hand, we have by the lemma that

$$\mathrm{Frac}(S) = \mathrm{Frac}(R) = k(x, z)[y]/(y^3 + y^2x^2 + yx^2 + x^3z)$$

which is algebraic over $k(x, z)$. Hence it transcendence degree is 2, contradiction.

Thus, $R[\frac{\overline{y}}{\overline{x}}] \cong k[u, v]$, so it is integrall closed, and hence $S = R[\frac{\overline{y}}{\overline{x}}]$. □

Exercise 4. Let R be a ring. Let M, N be R-modules and I an ideal of R. Prove that there are isomorphisms of R-modules $M \otimes_R N \cong N \otimes_R M$ and $M \otimes_R (R/I) \cong M/IM$.

Proof. The solution consists of the following steps.

(1) We first prove that $M \otimes_R N \cong N \otimes_R M$. For this purpose, we construct mutually inverse maps from one side to the other. To construct, $M \otimes_R N \to N \otimes_R N$ we just observe that the map $M \times N \to N \otimes_R M$ given by $(m, n) \mapsto n \otimes m$ is bilinear. Hence we obtain a map $M \otimes_R N \to N \otimes_R N$ given on simple tensors by $m \otimes n \mapsto n \otimes m$. By swapping the roles of M and N we obtain also a map in the reverse direction, and the two maps are mutually inverse as their composition is the the identity on simple tensors (and simple tensors generate the tensor product).

(2) Let us give two proofs:

Proof 1: The bilinear map $M \times {}^{R}\!/_{I} \to {}^{M}\!/_{IM}$ sending $(m, \bar{r})$ to rm (it is straightforward to see it is well-defined) induces

$$M \otimes_R {}^{R}\!/_{I} \to {}^{M}\!/_{IM}$$

On the other hand, we have a map $M \to M \otimes_R {}^{R}\!/_{I}$ sending m to $m \otimes 1$. Furthermore, any element of the form rm with $r \in I$, $m \in M$ in sent to $rm \otimes 1 = m \otimes \bar{r} = 0$, so since these elements generate IM, we deduce a map

$${}^{M}\!/_{IM} \to M \otimes_R {}^{R}\!/_{I}$$

These two maps are inverses of each other, so we win.

Proof 2: We consider the exact sequence $0 \to I \to R \to {}^{R}\!/_{I} \to 0$. Taking its tensor product with a module M and using right exactness we obtain an exact sequence

$$I \otimes_R M \to R \otimes_R M \to ({}^{R}\!/_{I}) \otimes_R M \to 0.$$

The middle group $R \otimes_R M$ can be identified with M using the map $r \otimes m \mapsto rm$. Under this identification the image of the homomorphism $I \otimes_R M \to R \otimes_R M$ is equal to IM. This implies that $({}^{R}\!/_{I}) \otimes_R M$ is isomorphic to ${}^{M}\!/_{IM}$.

□

Exercise 5. Let R be a ring, and M, N and P be R-modules. Show that there exists a natural bijection

$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Use this to prove that

$$- \otimes_R N : \{R\text{-modules}\} \to \{R\text{-modules}\}, \quad A \mapsto A \otimes_R N$$

is a right exact covariant functor.

Proof. We start by proving that $- \otimes_R N$ is a covariant functor. For this we need to assign to an R-module homomorphism $f : M \to M'$ an R-module homomorphism $M \otimes_R N \to M' \otimes_R N$, which for conceptual reasons we will denote by $f \otimes_R \mathrm{id}_N$ (but you may also denote it $f \otimes_R N$ if you like). To construct $f \otimes_R \mathrm{id}_N$, let $\iota : M \oplus N \to M \otimes_R N$ and $\iota' : M' \oplus N \to M' \otimes_R N$ be the unique R-bilinear maps in the definition of the tensor product. Let $f \oplus \mathrm{id}_N : M \oplus N \to M' \oplus N$ be defined by $(f \oplus \mathrm{id}_N)(n, m) = (f(n), m)$, then $f \oplus \mathrm{id}_N$ is obviously R-linear. The composition $\iota' \circ F$ defines an R-bilinear map $M \oplus N \to M' \otimes_R N$. By the universal property of $M \otimes_R N$ there exists a unique morphism $f \otimes_R \mathrm{id}_N : M \otimes_R N \to M' \otimes_R N$ such that $\iota' \circ (f \oplus \mathrm{id}_N) = (f \otimes_R \mathrm{id}_N) \circ \iota$. Notice that on simple tensors, $f \otimes_R \mathrm{id}_N$ is given by $m \otimes n \mapsto f(m) \otimes n$. We now have to verify points (1) and (2) in the definition of a covariant functor given on the Sheet. It is a very useful thing to note that as simple tensors generate the tensor product, two maps with domain a tensor product agree if and only if they agree on simple tensors.

(1) By the above description, $\mathrm{id}_M \otimes_R \mathrm{id}_N$ maps any simple tensor $m \otimes n$ to $m \otimes n$, and thus $\mathrm{id}_M \otimes_R \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}$

(2) Let $f : M \to M'$ and $f' : M' \to M''$ be R-module homomorphisms. Both the map $(f' \otimes_R \mathrm{id}_N) \circ (f \otimes_R \mathrm{id}_N)$ and the map $(f' \circ f) \otimes_R \mathrm{id}_N$ send any simple tensor $m \otimes n$ to $f'(f(m)) \otimes n$. As simple tensors generate $M \otimes_R N$ we hence have $(f' \otimes_R \mathrm{id}_N) \circ (f \otimes_R \mathrm{id}_N) = (f' \circ f) \otimes_R \mathrm{id}_N$.

We now construct the bijection in question. Let $\iota : M \oplus N \to M \otimes_R N$ be the R-bilinear map from the definition of the tensor product. Let $f : M \otimes_R N \to P$ be an R-module homomorphism. Then $f \circ \iota : M \oplus N \to P$ is R-bilinear. Define the map $\eta(f) = \eta_{M,N,P}(f) : M \to \mathrm{Hom}_R(N, P)$ by

$$\begin{aligned} \eta(f) : M &\to \mathrm{Hom}_R(N,P) \\ m &\mapsto (n \in N \mapsto (f \circ \iota)(m,n) \in P) \,. \end{aligned}$$

Using R-bilinearity of $f \circ \iota$ it is straightforward to verify that this is well-defined, i.e. that $\eta(f)(m) \in \mathrm{Hom}_R(N, P)$ an that η is an R-linear map.
To show that η is bijective, we also perform a construction in the reverse direction. Let $F : M \to \mathrm{Hom}_R(N, P)$ be R-linear, then it is straightforward to verify that the map $\widetilde{F} : M \oplus N \to P$ defined by $\widetilde{F}(m, n) = F(m)(n)$ is R-bilinear. Hence the universal property of the tensor product gives an R-module homomorphism $\theta(F) = \theta_{M,N,P}(F) : M \otimes_R N \to P$ such that $\theta(F) \circ \iota = \widetilde{F}$. We hence obtain a map $\theta : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(M \otimes_R N, P)$.
We now verify that the above two constructions are mutually inverse. Let $f : M \otimes_R N \to P$ be R-linear, then

$$(\theta(\eta(f)))(m \otimes n) = \widetilde{\eta(f)}(m,n) = \eta(f)(m)(n) = (f \circ \iota)(m,n) = f(m \otimes n)$$

for all simple tensors $m \otimes n$. As simple tensors generate $M \otimes_R N$ we conclude $\theta(\eta(f)) = f$.
On the other hand, let $F : M \to \mathrm{Hom}_R(N, P)$ be R-linear. Then we have for all $m \in M$ and $n \in N$ that

$$[(\eta(\theta(F)))(m)](n) = (\theta(F) \circ \iota)(m,n) = \widetilde{F}(m,n) = F(m)(n).$$

Hence we obtain $\eta(\theta(F)) = F$.
We conclude that η and θ are mutually inverse (and in particular also θ is R-linear, as η is). In fact, $\eta_{M,N,P}$ is a natural bijection, which means that it is functorial in M, N, P (i.e. it makes the appropriate commutative diagram commute). We will need only functoriality in M, so we only show this part: let $g : M \to M'$ be an R-module homomorphism. To show that for fixed N, P, the map $\eta_M := \eta_{M,N,P}$ is natural in M, means by definition that we need to verify that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(M \otimes_R N, P) & \xrightarrow{\eta_M} & \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P)) \\ {\scriptstyle \mathrm{Hom}_R(g \otimes_R \mathrm{id}_N, P)} \uparrow & & \uparrow {\scriptstyle \mathrm{Hom}_R(g, \mathrm{Hom}_R(N,P))} \\ \mathrm{Hom}_R(M' \otimes_R N, P) & \xrightarrow{\eta_{M'}} & \mathrm{Hom}_R(M', \mathrm{Hom}_R(N,P)) \end{array}$$

commutes. To do so, let $f' : M' \otimes_R N \to P$ be arbitrary. Then for any $m \in M$ and $n \in N$ we have

$$\begin{aligned} [\eta_M \circ \mathrm{Hom}_R(g \otimes_R \mathrm{id}_N, P)(f')](m)(n) &= [\eta_M(f' \circ (g \otimes_R \mathrm{id}_N))](m)(n) = \\ &= f' \circ (g \otimes_R \mathrm{id}_N) \circ \iota(m,n) = f'(g(m) \otimes n). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} [\mathrm{Hom}_R(g, \mathrm{Hom}_R(N,P)) \circ \eta_{M'}(f')](m)(n) &= [\eta_{M'}(f') \circ g](m)(n) = \eta_{M'}(f')(g(m))(n) = \\ &= f' \circ \iota'(g(m), n) = f'(g(m) \otimes n). \end{aligned}$$

As both results agree, the above diagram indeed commutes, and thus the bijection is natural in M. If you want to verify that it is natural in all components the you need to take simultaneously R-module homomorphisms $M \to M'$, $N \to N'$ and $P \to P'$ and show that the appropriate diagram commutes, but this is more of a language verification and messy so we omit it here.
We now proceed to show right exactness. Let

$$0 \to K \to L \to M \to 0$$

be an exact sequence of R-modules. We want to show that the sequence

$$K \otimes_R N \to L \otimes_R N \to M \otimes_R N \to 0$$

is exact. As we want to use the natural bijection constructed above, we want to apply $\mathrm{Hom}_R(-, P)$ to this sequence and see what happens. To keep track of exactness, this suggests proving the following lemma.

Lemma 1. *Consider R-module homomorphisms $\alpha : A \to B$ and $\beta : B \to C$. If $0 \to \mathrm{Hom}_R(C, P) \to \mathrm{Hom}_R(B, P) \to \mathrm{Hom}_R(A, P)$ is exact for all R-modules P, then $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is exact. (This is in fact an 'if and only if' but we don't need it for this exercise.)*

Proof. We start by verifying exactness at C, i.e. that β is surjective. To do so, take $P = \mathrm{coker}(\beta)$, and let $q : C \to P$ be the natural surjection. Note that $\mathrm{Hom}_R(\beta, P)(q) = q \circ \beta = 0$, and thus by injectivity of $\mathrm{Hom}_R(\beta, P)$ we conclude $q = 0$. Hence $\mathrm{coker}(\beta) = 0$ which implies that β is surjective.
Now we verify exactness at B. Take $P = C$ and $\mathrm{id}_C \in \mathrm{Hom}_R(C, C)$. Then

$$0 = \mathrm{Hom}_R(\alpha, C) \circ \mathrm{Hom}_R(\beta, C)(\mathrm{id}_C) = \beta \circ \alpha.$$

Thus $\mathrm{im}(\alpha) \subseteq \ker(\beta)$. To verify the reverse inclusion, take $P = \mathrm{coker}(\alpha)$ and let $p : B \to P$ be the natural surjection. Then $\mathrm{Hom}_R(\alpha, P)(p) = p \circ \alpha = 0$, and thus by the exactness assumption we obtain that there exists $\phi \in \mathrm{Hom}_R(C, P)$ such that $\mathrm{Hom}_R(\beta, P)(\phi) = p$. That is, $\phi \circ \beta = p$ and in particular $\ker(\beta) \subseteq \ker(p) = \mathrm{im}(\alpha)$. Hence we have exactness at B. ☐

We are now ready to prove right exactness. As $\mathrm{Hom}_R(-, \mathrm{Hom}_R(N, P))$ is left exact, the sequence

$$0 \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(L, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(K, \mathrm{Hom}_R(N, P))$$

is exact. By naturality of η we have a commutative diagram

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) & \longrightarrow & \mathrm{Hom}_R(L, \mathrm{Hom}_R(N, P)) & \longrightarrow & \mathrm{Hom}_R(K, \mathrm{Hom}_R(N, P)) \\
& \eta_M \uparrow & & \eta_L \uparrow & & \eta_K \uparrow \\
0 \longrightarrow & \mathrm{Hom}_R(M \otimes_R N, P) & \longrightarrow & \mathrm{Hom}_R(L \otimes_R N, P) & \longrightarrow & \mathrm{Hom}_R(K \otimes_R N, P).
\end{array}$$

As the vertical arrows are bijective R-module homomorphisms, it is straightforward to verify that exactness of the top row implies exactness of the bottom row. As hence the bottom row is exact for any R-module P, the Lemma 1 allows us to conclude that $K \otimes_R N \to L \otimes_R N \to M \otimes_R N \to 0$ is exact. Hence $- \otimes_R N$ is a right exact covariant functor. ☐

Exercise 6. Let A be a ring, with A-algebras B and C and an A-module M. Show that:

(1) $B \otimes_A M$ naturally has the structure of a B-module,

(2) $B \otimes_A C$ naturally has the structure of an A-algebra,
(3) $B \otimes_A B$ naturally has a ring morphism to B.

Proof. (1) Giving a B-module structure on $B \otimes_A M$ is equivalent to giving a ring map $\lambda : B \to \mathrm{End}_{\mathbb{Z}}(B \otimes_A M)$. To define $\lambda(b)$, note that the map $B \oplus M \to B \otimes_A M$ given by $(b', m) \mapsto (bb') \otimes m$ is A-bilinear. Hence we obtain a map of A-modules $\lambda(b) : B \otimes_A M \to B \otimes_A M$ given on simple tensors by $\lambda(b)(b' \otimes m) = (bb') \otimes m$. In particular, $\lambda(b)$ is a $\mathbb{Z}$-endomorphism of $B \otimes_A M$. It is then straightforward to verify that $\lambda(1) = \mathrm{id}_{B \otimes M}$, $\lambda(b + b') = \lambda(b) + \lambda(b')$ and $\lambda(bb') = \lambda(b) \circ \lambda(b')$ for all $b, b' \in B$; simply check these identities on simple tensors where they easily follow.

(2) First we need to construct a ring structure on $B \otimes_A C$. On simple tensors, it would be natural to suspect $(b \otimes c) \cdot (b' \otimes c') = (bb') \otimes (cc')$ to work, but of course one needs to verify that this is well defined. A clean way is to do the following: For $b \in B$ and $c \in C$, the map

$$B \oplus C \to B \otimes_A C$$
$$(b', c') \mapsto (bb') \otimes (cc')$$

is easily verified to be A-bilinear, and hence induces an A-linear map $\lambda_{(b,c)}$ given on simple tensors by $\lambda_{(b,c)}(b' \otimes c') = (bb') \otimes (cc')$. Next, one may verify that the map $\lambda_{\bullet} : B \oplus C \to \mathrm{End}_A(B \otimes_A C)$ given by $(b, c) \mapsto \lambda_{(b,c)}$ is A-bilinear, and hence induces an A-linear map $\Lambda : B \otimes_A C \to \mathrm{End}_A(B \otimes_A C)$, given on simple tensors by $\Lambda(b \otimes c) = \lambda_{b,c}$. Now for $\tau, \tau' \in B \otimes_A C$ we define their product by $\tau \cdot \tau' := \Lambda(\tau)(\tau')$. On simple tensors this indeed gives $(b \otimes c) \cdot (b' \otimes c') = (bb') \otimes (cc')$, and it is straightforward to verify the axioms of (commutative) ring multiplication. As Λ is a morphism of A-modules, it is also straightforward that the map $A \to B \otimes_A C$ given by $a \mapsto a \otimes 1 = 1 \otimes a$ gives $B \otimes_A C$ the structure of an A-algebra.

(3) The map $B \oplus B \to B$ given by $(b, b') \mapsto bb'$ is A-bilinear and hence induces an A-linear map $\Delta : B \otimes_A B \to B$, given on simple tensors by $\Delta(b \otimes b') = bb'$. As simple tensors generate $B \otimes_A B$ as an A-module, and hence also as an A-algebra, it suffices to verify multiplicativity on simple tensors. This is easily checked.

□

Exercise 7. Prove the following assertions:

(1) Let R be a commutative ring, and let M_1 and M_2 be free R-modules with bases $\{e_1, ..., e_m\}$ and $\{f_1, ..., f_n\}$ respectively. Show that a basis of $M_1 \otimes_R M_2$ is given by $\{e_i \otimes f_j\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$.
(2) Hence show that the element $e_1 \otimes f_2 + e_2 \otimes f_1$ cannot be written as $u \otimes v$ for any $u \in M_1$ and $v \in M_2$.

Proof. (1) As we have already seen, tensor products are distributive with respect to direct sums and for any R-module N, we have $N \otimes_R R \cong N$. Thus, we have

$$M_1 \otimes_R M_2 \xrightarrow{\cong}_{(1)} R^{\oplus m} \otimes_R R^{\oplus n} \xrightarrow{\cong}_{(2)} (R^{\oplus m} \otimes_R R)^{\oplus n} \xrightarrow{\cong}_{(3)} R^{\oplus mn}.$$

Hence, $M \otimes_R N$ is free of the right rank. Let us find an explicit basis by precisely remembering what our isomorphisms do. Let w_i denote the standard i'th coordinate vector (which we see both in $R^{\oplus m}$ and $R^{\oplus n}$). Then by definition, our choice of isomorphism (1) sends $e_i \otimes f_j$ to $w_i \otimes w_j$.

Recall that the isomorphism $M \otimes_R (S \oplus T) \to (M \otimes_R S) \oplus (M \otimes_R T)$ is given by

$$m \otimes (s,t) \mapsto (m \otimes s, m \otimes t).$$

Hence, isomorphism (2) sends $w_i \otimes w_j$ to

$$(w_i \otimes 0, \dots, w_i \otimes 1, \dots, w_i \otimes 0)$$

where the only $w_i \otimes 1$ term is the j'th one. Finally, in general, the isomorphism $M \otimes_R R \to M$ is given by $m \otimes r \mapsto rm$, so we conclude that the image of the elements $e_i \otimes f_j$ through this whole string os isomorphism is

$$w_{ij} := (0, \dots, w_i, \dots, 0).$$

Since these elements form a basis of $R^{\oplus mn}$, we win.

(2) Suppose we can write $e_1 \otimes f_2 + e_2 \otimes f_1 = u \otimes v$ for $u \in M_1$ and $v \in M_2$. Then writing $u = \sum_i a_i e_i$ and $v = \sum_j b_j f_j$ we get $e_1 \otimes f_2 + e_2 \otimes f_1 = \sum_{i,j} a_i b_j e_i \otimes f_j$. But this is a linear combination among basis vectors, so we have $a_1 b_2 = a_2 b_1 = 1$ and all other $a_i b_j = 0$. The first implies that all of a_1, b_2, a_2, b_1 are non-zero, which implies that $a_1 b_1$ is also non-zero. But this is a contradiction.

□

Exercise 8. We will define the exterior product of a module. This construction is especially important, for example in differential/algebraic geometry when one considers differential forms.

Let R be a commutative ring, and let M be an R-module. For any $n > 0$, define $T^n(M) := M \otimes_R \cdots \otimes_R M$ (n times). We also set $T^0(M) := R$. For any $n \geq 0$, we define $\bigwedge^n M$ as the quotient of $T^n M$ by the submodule I generated by elements of the form

$$m_1 \otimes \cdots \otimes m_n,$$

with $m_i = m_j$ for some $i \neq j$. The image of $m_1 \otimes \cdots \otimes m_n$ in $\bigwedge^n M$ is denoted $m_1 \wedge \cdots \wedge m_n$.

Note that if $f \colon M \to N$ is a morphism of R-modules, then it naturally induced a morphism $T^n(f) \colon T^n(M) \to T^n(N)$ of R-modules (apply f to each tensor), and passes to the quotient $\bigwedge^n f \colon \bigwedge^n M \to \bigwedge^n N$.

From now on, assume that M is free of finite rank $r \geq 1$, with basis $\mathcal{B} = \{e_1, \dots, e_r\}$.

- Show that $\bigwedge^r M$ is free with basis $e_1 \wedge \cdots \wedge e_r$, and that $\bigwedge^l M = 0$ for any $l > r$.
- Show that for $0 \leq i \leq r$, $\bigwedge^i M$ is free of rank $\binom{r}{i}$.
  Hint: First find a the appropriate number of generators. To show that it is a basis (i.e. the linear independance), wedge it by an appropriate element to get something in $\bigwedge^r M$, where you know an explicit basis.
- Fix the isomorphism $\theta \colon \bigwedge^r M \to R$ corresponding to the basis found in the first point. Let $f \colon M \to M$ be an endomorphism, corresponding to a matrix $A \in M_{r \times r}(R)$ (with respect to $\mathcal{B}$). Show that the diagram

$$\begin{array}{ccc} \bigwedge^r M & \xrightarrow{\bigwedge^r f} & \bigwedge^r M \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ R & \xrightarrow{\cdot \det(A)} & R \end{array}$$

  commutes.

- Use the above to give a new proof that if A and B are two $r \times r$-matrices, then $\det(AB) = \det(A)\det(B)$.
  Hint: $\bigwedge$ is functorial.

Proof. Before anything, let us show the following lemma:

Lemma 0.3. *For any $n > 0$, $m_1, \dots, m_n \in M$ and $\sigma \in S_n \coloneqq \mathrm{Bij}\{1, \dots, n\}$, we have*

$$m_{\sigma(1)} \wedge \cdots \wedge m_{\sigma(n)} = \mathrm{sgn}(\sigma) m_1 \wedge \cdots \wedge m_n.$$

Proof of the lemma. Since the group S_n is generated by transpositions of the form $\sigma_i = (i, i+1)$, it is enough to show the result for these elements. Hence, it is enough to show that

$$m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \wedge m_i \wedge \cdots \wedge m_n = -m_1 \wedge \cdots \wedge m_n.$$

Up to wedging on the left by $m_1 \wedge \cdots \wedge m_{i-1}$ and on the right by $m_{i+2} \wedge \cdots \wedge m_n$, we are left to show that

$$m_{i+1} \wedge m_i = -m_i \wedge m_{i+1}.$$

Since by assumption $(m_i + m_{i+1}) \wedge (m_i + m_{i+1}) = 0$, we obtain that by multilinearity that

$$0 = m_i \wedge m_i + m_i \wedge m_{i+1} + m_{i+1} \wedge m_i + m_{i+1} \wedge m_{i+1}.$$

Since the extremal terms of the right-hand-side are zero by definition, we conclude. □

Now, let us start the proof if the exercise.

- By Exercise 7, we know that for any $n > 0$, a basis of $T^n(M)$ is given by the elements

$$e_{i_1} \otimes \cdots \otimes e_{i_n},$$

with $i_1, \dots, i_n \in \{1, \dots, r\}$. By the lemma we just proved, we obtain that each $\bigwedge^i M$ is generated by the elements

$$e_{i_1} \wedge \cdots \wedge e_{i_r},$$

with $1 \leq i_1 < \cdots < i_r \leq r$. This shows immediately that $\bigwedge^l M = 0$ for $l > r$, and that $\bigwedge^r M$ is generated by $e_1 \wedge \cdots \wedge e_r$.

Our goal is to show that this element is a basis of $\wedge^r M$. Hence, assuming that there exists $s \in R$ such that $s(e_1 \wedge \cdots \wedge e_n) = 0$, we want to show that $s = 0$.

Consider the map $M^{\oplus r} \cong R^{\oplus r \times r} \to R$ given by taking the determinant, where the isomorphism above is induced by the basis $\mathcal{B}$. Since this map is multilinear, it induces an R-linear morphism

$$\det\colon T^r(M) \to R.$$

Furthermore, recall that if a matrix A has two identical colons, then $\det(A) = 0$. Thus, det induces an R-linear morphism at the level of quotients

$$\det\colon \bigwedge^r M \to R.$$

By definition, it sends $e_1 \wedge \cdots \wedge e_n$ to 1, so

$$0 = \det(s(e_1 \wedge \cdots \wedge e_n)) = s \det(e_1 \wedge \cdots \wedge e_n) = s.$$

In particular, $s = 0$ so this point is proven.

- For any $J = \{j_1, \dots, j_i\} \subseteq \mathcal{B}$, set $e_I := e_{j_1} \wedge \dots \wedge e_{j_i}$. By our proof of the previous point, we know that $\bigwedge^i M$ is generated by the elements e_J with $|J| = i$. Note that there are exactly $\binom{r}{i}$ of these elements, so our goal is to show that they form a basis.

  Assume that there exist elements $\lambda_J \in R$ such that
$$\sum_{|J|=i} \lambda_J e_J = 0,$$
  and let $J' \subseteq \mathcal{B}$ with $|J'| = i$. Denote $J'_c := \mathcal{B} \setminus J'$. Then for any $J \neq J'$, $e_J \wedge e_{J'_c} = 0$, so we obtain that
$$0 = e_{J'_c} \wedge \sum_J \lambda_J e_J = \pm \lambda_{J'} e_1 \wedge \dots \wedge e_n.$$
  By the previous point, we deduce that $\lambda_{J'} = 0$. Doing this for all J', we conclude.
- Write $f(e_i) = \sum_j a_{ji} e_j$, so that $A = \{a_{ij}\}_{i,j}$. Then we obtain that
$$\begin{aligned}
\left(\bigwedge^r f\right)(e_1 \wedge \dots \wedge e_r) &= \left(\sum_j a_{j1} e_j\right) \wedge \dots \wedge \left(\sum_j a_{jr} e_j\right) \\
&= \sum_{j_1,\dots,j_r} \left(\prod_i a_{j_i i}\right) e_{j_1} \wedge \dots \wedge e_{j_r} \\
&\underset{\uparrow}{=} \sum_{\sigma \in S_r} \left(\prod_i a_{\sigma(i) i}\right) e_{\sigma(1)} \wedge \dots \wedge e_{\sigma(r)}
\end{aligned}$$
  [we must have $\{j_1, \dots, j_r\} = \{1, \dots, r\}$ (i.e. $i \mapsto j_i$ is a permutation) to have a non-zero term]
$$\begin{aligned}
&\underset{\uparrow}{=} \left(\sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) \prod_i a_{\sigma(i) i}\right) e_1 \wedge \dots \wedge e_r
\end{aligned}$$
  [see the lemma]
$$= \det(A)(e_1 \wedge \dots \wedge e_r).$$
- Let $f_A \colon R^{\oplus r} \to R^{\oplus r}$ denote the morphism corresponding to A (and similarly define f_B). Note that by definition, we have $\bigwedge^r (f_A \circ f_B) = \bigwedge^r f_A \circ \bigwedge^r f_B$. By the previous point, we have
$$\begin{aligned}
\det(AB) e_1 \wedge \dots \wedge e_n &= \left(\bigwedge^r (f_A \circ f_B)\right)(e_1 \wedge \dots \wedge e_n) \\
&= \left(\bigwedge^r f_A\right)\left(\bigwedge^r f_B\right)(e_1 \wedge \dots \wedge e_n) = \left(\bigwedge^r f_A\right)(\det(B) e_1 \wedge \dots \wedge e_n) \\
&= \det(A) \det(B) e_1 \wedge \dots \wedge e_n.
\end{aligned}$$
  In particular,
$$\det(AB) = \det(A)\det(B).$$

□