November 28, 2017

# Number Theory I (Commutative Algebra)

Hélène Esnault, Exercises: Shane Kelly

## Exercise sheet 5

As in the textbook, all rings are commutative with a unit.

If you submit solutions, please choose only **one** exercise.

**Exercise 1.** *Equivalent definitions of faithful flatness.*
Let $M$ be a flat $R$-module (so $M \otimes -$ sends exact sequences to exact sequences). Show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) For any morphism of modules $\alpha : N \to N'$ we have $M \otimes \alpha = 0 \Rightarrow \alpha = 0$.
(2) For any morphism of modules $\alpha : N \to N'$ we have $M \otimes \alpha$ is an injection $\Rightarrow \alpha$ is an injection.
(3) For any module $N$ we have $M \otimes N = 0 \Rightarrow N = 0$.
(4) For any morphism of modules $\alpha : N \to N'$, we have $M \otimes \alpha$ is an isomorphism $\Rightarrow \alpha$ is an isomorphism.

Hint: Consider kernels, cokernels, and the canonical morphism $N \to 0$.

**Exercise 2.** *Ideal criterion for flatness.*
Let $M$ be an $R$-module for some ring $R$. In this exercise we show that flatness can be checked on (finitely generated) ideals, and deduce a consequence for PIDs. More precisely, show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (1), below. Deduce that for a module $M$ over a PID we have

$$M \text{ is flat } \Leftrightarrow M \text{ is torsion-free}$$

where torsion-free means for any $x \in R, m \in M$ we have $xm{=}0 \Rightarrow x{=}0$ or $m{=}0$.

(1) $M$ is flat. That is, for any injection of $R$-modules $N \to N'$, the morphism $N \otimes M \to N' \otimes M$ is also an injection.
(2) For any finitely generated ideal $I \subset R$ the morphism $I \otimes_R M \to M; x \otimes m \mapsto xm$ is an injection.
(3) For any ideal $I \subset R$ the morphism $I \otimes_R M \to M; x \otimes m \mapsto xm$ is an injection.
(4) For any $n \geq 1$ and any submodule $L \subset R^n$ the canonical induced morphism $L \otimes_R M \to R^n \otimes_R M \cong M^n$ is an injection.
(5) For any finite generated module $N'$ and submodule $N \subset N'$, the morphism $N \otimes_R M \to N' \otimes_R M$ is an injection.
(6) For any module $N'$ and finitely generated submodule $N \subset N'$, the morphism $N \otimes_R M \to N' \otimes_R M$ is an injection.

Hint: for (3) $\Rightarrow$ (4) consider $I = L \cap (R \oplus 0^{n-1}) \subset R^n$, $L'' = L/I \subset R^{n-1} \cong R^n/(R \oplus 0^{n-1})$, the canonical morphism of sequences from $0{\to}I{\to}L{\to}L''{\to}0$ to $0{\to}R{\to}R^n{\to}R^{n-1}{\to}0$ and use induction on $n$.

Hint: for (4) $\Rightarrow$ (5) write $N' = R^n/L$ and $K = L'/L$ for some $L \subset L' \subset R^n$.

Hint: for (5) $\Rightarrow$ (6) and (6) $\Rightarrow$ (1) consider writing a module as the filtered union (i.e., colimit) of its finitely generated submodules.

**Exercise 3.** *Tensor products of fields.*

(1) Let $L/K$ be a finite Galois extension. That is, $L \cong K[x]/\langle f(x)\rangle$ for some irreducible polynomial $f \in K[x]$, and when $f$ is considered as a polynomial in $L$, there are *distinct* elements $\alpha_1, \dots, \alpha_d \in L$ such that we have a decomposition $f(y) = \prod_{i=1}^d (y - \alpha_i)$. Using the canonical morphisms

$$\phi_i : L[y]/\langle f(y)\rangle \to L; \qquad y \mapsto \alpha_i,$$

and the isomorphism $L \cong K[x]/\langle f(x)\rangle$ show that there is an isomorphism

$$L \otimes_K L \cong \prod_{i=1}^n L.$$

In particular, a tensor product of integral rings need not be integral.

(2) Let $L'/K$ be a finite separable extension of fields. That is, $L' \cong K[x]/\langle g(x)\rangle$ for some irreducible polynomial $g(x) \in K[x]$, such that there exists a (potentially bigger) field $L \supset L'$ for which there are *distinct* elements $\alpha_1, \dots, \alpha_d \in L$ such that we have a decomposition $g(x) = \prod_{i=1}^d (x - \alpha_i)$ in $L[x]$. Note if we split $g(x)$ into irreducible factors $g(x) = \prod_{i=1}^m g_i(x)$ in $L'[x]$ (not $L[x]$), the $g_i(x)$ are not necessarily linear, but $g_i \neq g_j$ for $i \neq j$. Describe $L' \otimes_K L'$ as a finite product of fields. Define $\omega = e^{2\pi i/3} \in \mathbb{C}$, so $\omega^2 + \omega + 1 = 0$, and describe $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$ as a sum of subfields of $\mathbb{C}$ using $\sqrt[3]{2}$ and $\omega$.

(3) Let $K$ be a field of characteristic $p > 0$. Recall that in such a field we have $(a+b)^p = a^p + b^p$ for every $a, b \in K$. Let $a \in K$ be an element for which $x^p - a$ has no solution[1] in $K$, and let $L = K[x]/\langle x^p - a\rangle$. Show that $L$ is a field, and that there is an isomorphism

$$L \otimes_K L \cong L[s]/\langle s^p\rangle.$$

In particular, a tensor product of reduced rings need not be reduced.

(4) Let $k$ be a field. Recall that $k(x) = \operatorname{Frac} k[x]$ and $k(x,y) = \operatorname{Frac} k[x,y]$. In other words, $k(x) = S^{-1}k[x]$ if $S = k[x] \setminus \{0\}$, and $k(x,y) = S^{-1}k[x,y]$ if $S = k[x,y] \setminus \{0\}$.
   (a) Show $k[x,y] \cong k[x] \otimes_k k[y]$.
   (b) Show that $k(x,y) \otimes_{k[x]} k(x) \cong k(x,y)$.
   (c) Using the first two parts, the fact that $k(x)$ (resp. $k(y)$) is a flat $k[x]$ (resp. $k[y]$) module, and the inclusion $k[x,y] \subset k(x,y)$, show that the canonical morphism

$$k(x) \otimes_k k(y) \to k(x,y)$$

   is an injection. Deduce that $k(x) \otimes_k k(y)$ is a domain. Show furthermore, by considering the universal mapping property of the fraction field, that the above morphism presents $k(x,y)$ as the fraction field of $k(x) \otimes_k k(y)$, and therefore induces a canonical isomorphism $\operatorname{Frac} k[x,y] \cong \operatorname{Frac}\Big(k(x) \otimes_k k(y)\Big)$.
   (d) Describe the elements of $k[x,y]$ which become units in $k(x) \otimes_k k(y)$ (considered as a subring of $k(x,y)$).

---

[1]For example, we might have $K = \mathbb{F}_p(t)$ and $a = t$.

* Let $k$ be an algebraically closed field. Recall that the prime ideals of $k[x,y]$ are of three kinds: $\langle f\rangle$ for some $f \in k[x,y]$ nonzero and irreducible, $\langle x-a, y-b\rangle$ for some $a,b \in k$, and the zero ideal $\langle 0\rangle$.
* Recall also that if $R \subset S$ is an inclusion of domains (such as the inclusion $k[x,y] \subset k(x) \otimes_k k(y)$) which induces an isomorphism of fraction fields $\mathrm{Frac}(R) \cong \mathrm{Frac}(S)$, then the induced map $\mathfrak{p} \mapsto \mathfrak{p} \cap R$ identifies the prime ideals of $S$ with those prime ideals of $R$ which do not contain any units of $S$.

(e) Describe the prime ideals of $k(x), k(y)$ and $k(x,y)$. Using the inclusions $k[x,y] \subset k(x) \otimes_k k(y) \subset k(x,y)$ describe the prime ideals of the ring $k(x) \otimes_k k(y)$.

**Exercise 4.** *Tensor products over PID's.*

(1) Let $R$ be a ring, $I$ an ideal, and $M$ an $R$-module. Show that there is a canonical isomorphism

$$M \otimes_R (R/I) \cong M/IM.$$

(2) Let $R$ be a principal ideal domain, $\mathfrak{p}, \mathfrak{p}' \subset R$ prime ideals, and $m', m > 0$ integers. Show that there is a prime ideal $\mathfrak{q}$ and an integer $n$ such that

$$(R/\mathfrak{p}^m) \otimes_R (R/\mathfrak{p}'^{(m')}) \cong R/\mathfrak{q}^n$$

and say what $\mathfrak{q}$ and $n$ are.

* Recall that if $M$ is a finitely generated module over a principal ideal domain, there is an isomorphism

$$M \cong \left(R^{\oplus N}\right) \oplus \left( \bigoplus_{n>0} \bigoplus_{\substack{0\neq\mathfrak{p}\subset R \\ \mathfrak{p}\text{ prime}}} (R/\mathfrak{p}^n)^{\oplus m_{\mathfrak{p},n}} \right)$$

where $N, m_{\mathfrak{p},n}$ are uniquely defined, and only finitely many $m_{\mathfrak{p},n}$ are nonzero.

(3) If $M$ and $M'$ are finitely generated modules over a ring $R$ which is a PID, describe the above decomposition of $M \otimes_R M'$ in terms of the decompositions of $M$ and $M'$.

**Exercise 5.** *The Picard group.*

(1) Let $R$ be a domain with fraction field $K$ and $M$ a module such that $M \otimes_R K = 0$. Show that for for every element $m \in M$ there exists some $x \in R$ such that $xm = 0$ in $M$ (for example using [AK2017, Lemma 8.16]). By considering the multiplication by $x$ module map $R \to R; y \mapsto xy$ show that this implies $m = 0$ if $M$ is flat. Deduce that if $M$ is a flat $R$-module such that $M \otimes_R K = 0$ then $M = 0$. Since projective modules are flat, deduce that this is also true of projective modules.

(2) If $R \to S$ is a morphism of rings, show that for any $R$-module $M$, we have

$$\otimes^i_S(M \otimes_R S) \cong (\otimes^i_R M) \otimes_R S.$$

(3) Deduce that we have

$$\wedge^i_S(M \otimes_R S) \cong (\wedge^i_R M) \otimes_R S.$$

* Recall that for any $R$-modules $M, M'$ and $n \geq 0$ there is a canonical isomorphism
$$\bigoplus_{\substack{i,j\geq 0\\ i+j=n}} \left(\wedge^i M) \otimes_R (\wedge^j M')\right) \xrightarrow{\sim} \wedge^n (M \oplus M');$$
(by definition $\wedge^0 M = R$ for any module $M$).
* Recall also that there is an isomorphism $\wedge^i_R(R^n) \cong R^{\binom{n}{i}}$ where $\binom{n}{i}$ is $n$ choose $i$.

(4) If $P$ is a projective $R$ module (so $P \oplus Q \cong R^n$ for some module $Q$ and $n \geq 0$) show that $\wedge^i P$ is also projective for all $i$.

(5) Let $R$ be a domain with fraction field $K$. Define the *rank* of a projective module $P$ to be the dimension of the $K$-vector space $P \otimes_R K$. Recall that a finite dimensional vector space $V$ is of dimension $d$ if and only if
$$\wedge^i V \neq 0 \text{ for } 1 \leq i \leq d \text{ and } \wedge^i V = 0 \text{ for } i > d.$$
Using parts (1), (3), and (4) show that a finitely generated projective module $P$ is of rank $d$ if and only if
$$\wedge^i P \neq 0 \text{ for } 1 \leq i \leq d \text{ and } \wedge^i P = 0 \text{ for } i > d.$$

(6) Let $P$ be a finitely generated projective module over a domain $R$ (so $P \oplus Q \cong R^n$ for some module $Q$ and $n \geq 0$). Suppose furthermore that $P$ is of rank one. By considering the operation $\wedge^n_R$ and the previous parts, show that there exists a second finitely generated rank one projective module $P'$ such that $P \otimes_R P' \cong R$.

(7) Continuing to assume that $R$ is a domain, deduce that the set of isomorphism classes of finitely generated rank one projective modules, equipped with the operation $\otimes_R$ is a commutative group. This group is called the *Picard group* of $R$.

**Exercise 6.** *Lazard's theorem [AK2017, Theorem 9.13].*
Let $M$ be an $R$-module for some ring $R$.

* Recall that in class we considered the system
$$\Phi = \{M_i, \phi_n \mid i \in I, n \in N\}$$
where $I$ is the set of morphisms $\alpha_i : R^{m_i} \to M$ (all $m_i \geq 0$ are allowed), $N$ is the set of morphisms $\phi_n : R^{n_i} \to R^{n_j}$ such that $\alpha_{j_n}\phi_n = \alpha_{i_n}$, and $M_i = R^{m_i}$. Its proven in [AK2017, Proposition 9.12] that $M = \varinjlim \Phi$.
* Recall that we also showed in class that any filtered colimit of flat modules is flat, [AK2017, Proposition 9.9].

Show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (8) $\Rightarrow$ (1).

(1) $M$ is flat.

(2) For any exact sequence $R^i \to R^j \to P \to 0$ (with $i, j$ integers), the morphism
$$\hom_R(P, R) \otimes_R M \to \hom_R(P, M)$$
$$\phi \otimes m \mapsto (p \mapsto \phi(p)m)$$
is surjective.

(3) For any exact sequence $R^i \to R^j \to P \to 0$ (with $i, j$ integers) and morphism $\beta : P \to M$ there exists a factorisation $\beta : P \xrightarrow{\gamma} R^n \xrightarrow{\alpha} M$.

(4) Given any $\alpha : R^m \to M$ and $k \in Ker(\alpha)$, there is a factorisation $\alpha : R^m \xrightarrow{\phi} R^n \to M$ such that $\phi(k) = 0$.
(5) Given any $\alpha : R^m \to M$ and $k_1, \ldots, k_r \in Ker(\alpha)$, there is a factorisation $\alpha : R^m \xrightarrow{\phi} R^n \to M$ such that $\phi(k_i) = 0$ for all $i$.
(6) Given $R^r \xrightarrow{\rho} R^m \xrightarrow{\alpha} M$ such that $\alpha\rho = 0$, there exists a factorisation $\alpha : R^m \xrightarrow{\phi} R^n \to M$ such that $\phi\rho = 0$.
(7) The system $\Phi$ above is filtered.
(8) $M$ is a filtered colimit of free modules of finite rank.