EPFL - Fall 2024 | Domenico Valloni
Rings and modules | **Exercises**
Sheet 8 - Solutions

Exercise 1. Let R be a ring and let M, K, L and N be R-modules. Assume that $\operatorname{Ext}^i_R(M,N)$, $\operatorname{Ext}^i_R(K,N)$ and $\operatorname{Ext}^i_R(L,N)$ have finite length for all $i \geq 0$, and that there exist integers s such that they are all zero for all $i > s$. Show that if

$$0 \longrightarrow K \longrightarrow M \longrightarrow L \longrightarrow 0$$

is a short exact sequence, then

$$\sum_{i=0}^{s} (-1)^i \operatorname{length} \operatorname{Ext}^i_R(M,N) = \sum_{i=0}^{s} (-1)^i \operatorname{length} \operatorname{Ext}^i_R(K,N) + \sum_{i=0}^{s} (-1)^i \operatorname{length} \operatorname{Ext}^i_R(L,N)$$

Proof. There is an induced long exact sequence on Ext^i's, since this sequence eventually terminates with all terms equal to zero this follows directly from Exercise 6.1 on Sheet 4. *Note:* Exercise 6.1 on Sheet 4 was stated for finitely generated modules M_i over an Artinian and Noetherian ring, however we only used that the M_i's where of finite length in the solution. □

Exercise 2 (Nullstellensatz for $\operatorname{Spec} R$)**.** Let R be a commutative ring. Given a closed subset $Z \subseteq \operatorname{Spec} R$, define $I(Z) := \{f \in R,\ Z \subseteq V(f)\}$. Show that $I(Z)$ is an ideal, and that for all ideals $I \subseteq \operatorname{Spec} R$,

$$I(V(I)) = \sqrt{I}$$

In particular, show that for all ideals I, J of R,

$$V(I) = V(J) \iff \sqrt{I} = \sqrt{J}$$

Proof. Throughout, the letter $\mathfrak{p}$ always denotes a prime ideal.

We will show that $I(Z)$ is an ideal by showing that if $Z = V(I)$, then $I(Z) = \sqrt{I}$, which we know to be an ideal.

Therefore, let us first prove that $I(V(I)) \subseteq \sqrt{I}$, so let $f \in I(V(I))$. By definition, $V(I) \subseteq V(f)$, hence by definition

$$f \in \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \sqrt{I}$$

where the equality is Proposition 6.4.5 in the notes.

On the other hand, if $f \in \sqrt{I}$, then $f^n \in I$ for some n. Hence, $V(I) \subseteq V(f^n)$, so to conclude that $f \in I(V(I))$, we are left to show that $V(f) = V(f^n)$. Since $(f^n) \subseteq (f)$, $V(f) \subseteq V(f^n)$. Conversely, if $\mathfrak{p} \ni f^n$, then also $\mathfrak{p} \ni f$ since $\mathfrak{p}$ is prime, so $V(f^n) \subseteq V(f)$ and we are done.

In the second statement, the "left to right" implication is immediate with what we just did, and the "right to left" follows from the general fact that for any ideal I, $V(I) = V(\sqrt{I})$. This is a restatement that for all primes $\mathfrak{p}$,

$$\mathfrak{p} \supseteq I \iff \mathfrak{p} \supseteq \sqrt{I}$$

□

Exercise 3. Let R be a commutative ring and $I \subseteq R$ be a radical ideal. Show that I is prime if and only if $V(I)$ is an irreducible topological space.

Proof. We will use exercise 2 of this sheet and exercise 3 of sheet 7 without further mention.

Suppose first that I is prime, and assume that $V(I) = V(J) \cup V(K)$ with J, K radical. Then

$$I = \sqrt{I} = I(V(I)) = I(V(J) \cup V(K)) = I(V(J \cap K)) = \sqrt{J \cap K} = J \cap K$$

(the intersection of two radical ideals is radical). If by contradiction $V(J) \neq V(I)$ (or in other words $I \subsetneq J$) and $V(J) \neq V(I)$ (i.e. $I \subsetneq K$), then there exist $a \in J \setminus I$, $b \in K \setminus I$. However, $ab \in J \cap K = I$, which contradicts the fact that I is prime.

Conversely, assume $V(I)$ is an irreducible topological space, and assume by contradiction that I is not prime. Then there exist a, $b \notin I$ such that $ab \in I$. But then, $V(I) \nsubseteq V(a)$, $V(I) \nsubseteq V(b)$ and $V(I) \subseteq V(ab) = V(a) \cap V(b)$. But then, setting $Z_1 = V(a) \cap V(I)$ and $Z_2 = V(b) \cap V(I)$ gives $V(I) = Z_1 \cup Z_2$, with none of the Z_i being $V(I)$. This contradicts that $V(I)$ is irreducible. □

Exercise 4. Let $R = \mathbb{C}[x, y, z]$ and $I = (xy - z^2, x^2 - y^2) \subseteq R$. Identify $V(I) \subset \mathbb{C}^3$. Notice that this naturally breaks into smaller algebraic sets. What are the ideals of each piece?

Proof. A point $(p, q, r) \in \mathbb{C}^3$ is in $V(I)$ if and only if $pq - r^2 = 0$ and $p^2 - q^2 = (p-q)(p+q) = 0$. So either $p = q$ or $p = -q$. In the first case, the first equation becomes $0 = p^2 - r^2 = (p - r)(p + r)$ and so either $p = r$ or $p = -r$. In the second case, the first equation becomes $0 = -p^2 - r^2 = (p - ir)(p + ir)$ and so $r = ip$ or $r = -ip$. Therefore

$$V(I) = \underbrace{\{(p, p, p) : p \in \mathbb{C}\}}_{:=V_1} \cup \underbrace{\{(p, p, -p) : p \in \mathbb{C}\}}_{:=V_2} \cup \underbrace{\{(p, -p, ip) : p \in \mathbb{C}\}}_{:=V_3} \cup \underbrace{\{(p, -p, -ip) : p \in \mathbb{C}\}}_{V_4}$$

The ideals of these four pieces are $\mathfrak{p}_1 := (x-y, x-z)$, $\mathfrak{p}_2 := (x-y, x+z)$, $\mathfrak{p}_3 := (x+y, x+iz)$ and $\mathfrak{p}_4 := (x + y, x - iz)$ respectively. Notice that they are all prime (because up to a linear change of variables they are all just (x, y)), and thus V_i is irreducible for all i. Hence $V(I)$ doesn't split up further. □

Exercise 5. Let F be an algebraically closed field. Let X and Y be algebraic sets in F^n.

(1) Prove that $I(X \cup Y) = I(X) \cap I(Y)$
(2) By considering $X = V(x^2 - y)$ and $Y = V(y)$ for the ideals $(x^2 - y)$ and (y) in $F[x, y]$, show that it need not be true that $I(X \cap Y) = I(X) + I(Y)$.
(3) Prove that in general $\sqrt{I(X) + I(Y)} = I(X \cap Y)$.

Proof. (1) Suppose $f \in I(X \cup Y)$. Then $f(P) = 0$ for all $P \in X$ and all $p \in Y$. So $f \in I(X)$ and $f \in I(Y)$. Conversely, suppose $f \in I(X) \cap I(Y)$. Then $f(P) = 0$ for all $P \in X$ and all $P \in Y$. Therefore $f \in I(X \cup Y)$.

(2) $I(X) = (x^2 - y)$, $I(Y) = (y)$ and $I(X \cap Y) = I(\{(0, 0)\}) = (x, y)$. But $I(X) + I(Y) = (x^2, y)$.

(3) This follows from a question on the previous exercise sheet and the Nulstellensatz. Let $I = I(X)$ and $J = I(Y)$, so $V(I) = X$ and $V(J) = Y$. By Exercise 2 on Exercise sheet 7 we have $I(X \cap Y) = I(V(I + J))$. But by the Nulstellensatz, $I(V(I + J)) = \sqrt{I + J}$.

□

Review exercises for material from "Anneaux et corps"

Exercise 6. Show that $x^3 + y^7 \in k[x, y]$ is irreducible.
[*Hint:* Use the consequence of Gauss's theorem saying that for a unique factorisation domain R and a primitive polynomial $f \in R[t]$, we have that f is irreducible in $\mathrm{Frac}(R)[t]$ if and only if it is irreducible in $R[t]$.]

Proof. We use the hint for $R = k[y]$. It is therefore sufficient to check that $x^3 + y^7$ is irreducible in $k(y)[x]$. Suppose it is not, since the degree is three it has to have a linear term in any factorisation and hence there exists f, g coprime such that $\frac{f}{g}$ is a root of $x^3 + y^7$. We write: $\frac{f^3}{g^3} + y^7 = 0$, and hence $f^3 = -g^3 y^7$. It then follows that y^3 divides f but then also that y divides g, which contradicts coprimality.

□

Review exercises for material from "Anneaux et corps"

Exercise 7. Let $R = k[x, y, z]$. Show that $(xz^3 + yz^3 - y^2z^2 + xyz - xy)$ is a prime ideal of R.
[*Hint*: Use Eisenstein's Criterion.]

Proof. View $f = xz^3 + yz^3 - y^2z^2 + xyz - xy$ as an element of $k[x, y][z]$, so $f = (x + y)z^3 - y^2z^2 + xyz - xy$. This satisfies the hypotheses of Eisenstein's criterion for $p = y$, and so f is irreducible in R. Thus (f) is a prime ideal.

□

Review exercises for material from "Anneaux et corps"

Exercise 8. Solve the following exercises:

(1) Consider the polynomial $f = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ in $\mathbb{C}[X, Y]$. Write it as an element of $(\mathbb{C}[X])[Y]$, that is collect together terms according to powers of Y, and then use Eisenstein's criterion to show that f is prime in $\mathbb{C}[X, Y]$.
(2) Let F be any field. Show that the polynomial $f = X^2 + Y^2 - 1$ is irreducible in $F[X, Y]$, unless F has characteristic 2. What happens in that case?

Proof. (1) $p = X - 1$ is prime in $\mathbb{C}[X]$ and satisfies the conditions of Eisenstein's criterion for f.
(2) Eisenstein's criterion gives that $X^2 + Y^2 - 1$ is irreducible if $Y - 1 \neq Y + 1$, i.e. it is irreducible if $1 \neq -1$, i.e. unless the characteristic is 2. In characteristic 2 we have $X^2 + Y^2 - 1 = (X + Y + 1)^2$ and hence this polynomial is not irreducible.

□

Exercise 9. Show the following:

(1) Let $F \subseteq L$ be a field extension, and suppose $a_1, \ldots, a_n$ are elements of L which are algebraically independent over F. Prove that $F(a_1, \ldots, a_n)$ is isomorphic to the fraction field of the polynomial ring $F[x_1, \ldots, x_n]$.

(2) Let $F \subseteq L$ be a field extension. Show that a subset of L is a transcendence basis for L over F if and only if it is a maximal algebraically independent set. As a consequence show that a transcendence basis exists for any field extension $F \subseteq L$.

Proof. (1) Define a ring homomorphism $\phi : F[x_1, ..., x_n] \to L$ by $x_i \mapsto a_i$ and $\phi|_F = \mathrm{id}_F$. We claim this is injective. For suppose $\phi(f) = 0$ for some f. This gives a polynomial with coefficients in F satisfied by the a_i, and so by definition of algebraic independence, $f = 0$. This injectivity, along with the existence of inverses in L, means we can extend ϕ to an injective homomorphism $F(x_1, \ldots, x_n) \hookrightarrow L$. Lastly, the image is a field (as $F(x_1, \ldots, x_n)$ is) containing F and $a_1, \ldots, a_n$, and thus contains $F(a_1, \ldots, a_n)$. But as every element of the image is a rational function of the $a_1, \ldots, a_n$ with coefficients in F, we conclude that the image is precisely $F(a_1, \ldots, a_n)$. Hence $F(a_1, \ldots, a_n)$ is isomorphic to $F(x_1, \ldots, x_n)$.

(2) Suppose the set $\{a_i\}_{i \in I}$ is a transcendence basis for $L \supseteq F$, with some (perhaps infinite) indexing set I. It is algebraically independent by definition, so we need to show it is maximal subject to this. Suppose not, so there is some element a of L which such that $\{a\} \cup \{a_i\}_{i \in I}$ is algebraically independet. But by definition of transcendent basis, $L \supseteq F(\{a_i\}_{i \in I})$ is algebraic, so there is a non-zero polynomial $p \in F(\{a_i\}_{i \in I})[X]$ such that $p(a) = 0$. The coefficients of p are rational functions of the a_i's, so by multiplying through to clear denominators, we can view p as a non-zero multivariate polynomial with coefficients in F satisfied by some subset of $\{a_i\}_{i \in I}$ and a. This contradicts the choice of a.

Conversely, suppose $\{a_i\}_{i \in I}$ is a maximal algebraically independent set. We need to show that $L \supseteq F(\{a_i\}_{i \in I})$ is algebraic. Let $a \in L$ be arbitrary. As $\{a_i\}_{i \in I} \cup \{a\}$ is not algebraically independent there is some multivariate non-zero polynomial f with coefficients in F such that $f(a, a_{i_1}, \ldots, a_{i_n}) = 0$ for some $i_1, \ldots, i_n \in I$. This must have some non-zero a term as otherwise it gives an algebraic dependence among the a_i's. This gives a polynomial satisfied by a with coefficients in $F(\{a_i\}_{i \in I})$ by dividing through by the coefficient of the highest power of a, and thus $L \supseteq F(\{a_i\}_{i \in I})$ is algebraic.

To show that a transcendence basis exists, we use Zorn's lemma on the partially ordered set Σ of algebraically independent sets over F inside L. If Σ is empty then $L \supseteq F$ is algebraic and there is nothing to prove. Hence assume that Σ is non-empty. To apply Zorn's Lemma, we must show that any chain of algebraically independent sets has an upper bound in Σ. Suppose $(A_\alpha)_{\alpha \in \Omega}$ is such a chain, i.e. for all indexes $\alpha, \beta \in \Omega$, either $A_\alpha \subseteq A_\beta$ or $A_\alpha \supseteq A_\beta$ holds. Then $\bigcup_{\alpha \in \Omega} A_\alpha$ defines an algebraically independent set, since any polynomial relation in $\bigcup_{\alpha \in \Omega} A_\alpha$ is a polynomial relation in A_α for A_α sufficiently large. Therefore $\bigcup_{\alpha \in \Omega} A_\alpha$ is an uppe rbound for the chain $(A_\alpha)_{\alpha \in \Omega}$. By Zorn's Lemma there exists a maximal algebraically independent set of elements in L. By what has already been proven such a a maximal algebraically independent set consitutes a transcendence basis for L over F.

□

Exercise 10. Prove that if $F \subseteq K \subseteq L$ are field extensions such that $\mathrm{trdeg}_F L < \infty$, then $\mathrm{trdeg}_F L = \mathrm{trdeg}_F K + \mathrm{trdeg}_K L$

Proof. By previous exercises $\mathrm{trdeg}_F L$ is the cardinality of any maximal algebraically F-independent subset $\{\alpha_1, \ldots, \alpha_{\mathrm{trdeg}_F L}\} \subseteq L$. Let $B = \{\beta_1, \ldots, \beta_{\mathrm{trdeg}_F K}\} \subseteq K$ be a maximal algebraically F-independent subset of K and let $C = \{\gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L}\} \subseteq L$ be a maximal algebraically K-independent subset of L. By construction,

$$B \cup C = \{\beta_1, \ldots, \beta_{\mathrm{trdeg}_F K}, \gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L}\} \subseteq L$$

is an algebraically F-independent subset of L. To conclude, we have to show that $F(B \cup C) \subseteq L$ is an algebraic extension. By elementary field theory, algebraicity is transitive, and so it it sufficient to show that both $F(B \cup C) \subseteq K(C)$ and $K(C) \subseteq L$ are algebraic. The latter is true by definition, so it remains to show that $F(B \cup C) \subseteq K(C)$ is algebraic. But now notice that $K(C) = (F(B \cup C))(K)$ (i.e. the field obtained by adjoining the elements of K to $F(B \cup C)$). So it is enough to show that every element of K is algebraic over $F(B \cup C)$, as then every rational function of the elements of C with coefficients in C is algebraic too. This is now automatic, since $F(B) \subseteq K$ is algebraic. Hence $F(B \cup C) \subseteq K(C)$ is algebraic, and thus also $F(B \cup C) \subseteq L$. So $B \cup C$ is a transcendence basis of L over F, which proves $\mathrm{trdeg}_F L = \mathrm{trdeg}_F K + \mathrm{trdeg}_K L$. □