D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 1

Radical ideals, Local Rings and Affine Varieties

Let A be a ring, k an algebraically closed field and $n > 0$ an integer.

1. Let $\mathfrak{a} \subset A$ be an ideal. Show that its radical $r(\mathfrak{a})$ is an ideal. Furthermore, prove:

   (a) $r(\mathfrak{a}) \supset \mathfrak{a}$

   (b) $r(r(\mathfrak{a})) = r(\mathfrak{a})$

   (c) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

   (d) $r(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$

   (e) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$

   (f) if $\mathfrak{p} \subset A$ is a prime ideal, then $r(\mathfrak{p}^k) = \mathfrak{p}$ for all $k > 0$

   Solution: First we show that $r(\mathfrak{a})$ is an ideal of A. We will strongly use the commutativity of A. Clearly, $0 \in r(\mathfrak{a})$. Let $a \in r(\mathfrak{a})$ with $n > 0$ such that $a^n \in \mathfrak{a}$. For every $x \in A$ we have $(xa)^n = x^n a^n \in \mathfrak{a}$ and hence $xa \in r(\mathfrak{a})$. This shows that $Ar(\mathfrak{a}) \subset r(\mathfrak{a})$.

   For every $a, b \in r(\mathfrak{a})$ and $n, m > 0$ such that $a^n, b^m \in \mathfrak{a}$ we compute using the binomial formula:
$$(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}$$
   Now for every $0 \leqslant i \leqslant n+m$ either $a^i \in \mathfrak{a}$ or $b^{n+m-i} \in \mathfrak{a}$, so by using that $\mathfrak{a}$ is an ideal, we conclude that $a + b \in r(\mathfrak{a})$. Finally, we see that $(-a)^n = (-1)^n a^n \in \mathfrak{a}$ and thus $-a \in r(\mathfrak{a})$. This proves that $r(\mathfrak{a})$ is an ideal.

   (a) This follows directly from the definition.

   (b) Using (a) we only need to show that $r(r(\mathfrak{a})) \subset r(\mathfrak{a})$. For any $a \in r(r(\mathfrak{a}))$ there is an integer $n > 0$ such that $a^n \in r(\mathfrak{a})$, and thus there is an integer $m > 0$ such that $a^{nm} = (a^n)^m \in \mathfrak{a}$. Hence $a \in r(\mathfrak{a})$.

   (c) Since $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ we conclude $r(\mathfrak{a}\mathfrak{b}) \subset r(\mathfrak{a} \cap \mathfrak{b})$. Let $a \in r(\mathfrak{a} \cap \mathfrak{b})$ with $n > 0$ such that $a^n \in \mathfrak{a} \cap \mathfrak{b}$. Then $a^n \in \mathfrak{a}$ and $a^n \in \mathfrak{b}$, so $a \in r(\mathfrak{a}) \cap r(\mathfrak{b})$. Finally, for every $b \in r(\mathfrak{a}) \cap r(\mathfrak{b})$ with $n > 0, m > 0$ such that $b^n \in \mathfrak{a}$ and $b^m \in \mathfrak{b}$ we have $b^{n+m} \in \mathfrak{a}\mathfrak{b}$ and hence $b \in r(\mathfrak{a}\mathfrak{b})$. We conclude $r(\mathfrak{a}\mathfrak{b}) \subset r(\mathfrak{a} \cap \mathfrak{b}) \subset r(\mathfrak{a}) \cap r(\mathfrak{b}) \subset r(\mathfrak{a}\mathfrak{b})$.

   (d) If $r(\mathfrak{a}) = (1)$, then there is an integer $n > 0$ such that $1^n \in \mathfrak{a}$, hence $\mathfrak{a} = (1)$. The converse follows by (a).

(e) The inclusion $r(\mathfrak{a}+\mathfrak{b}) \subset r(r(\mathfrak{a})+r(\mathfrak{b}))$ follows by using (a) for $\mathfrak{a}+\mathfrak{b} \subset r(\mathfrak{a})+r(\mathfrak{b})$. Conversely, for every element $x \in r(r(\mathfrak{a})+r(\mathfrak{b}))$ with $n>0$ such that $x^n \in r(\mathfrak{a})+r(\mathfrak{b})$, there are $a \in r(\mathfrak{a})$ and $b \in r(\mathfrak{b})$ such that $x^n = a+b$. Let $m, \ell > 0$ such that $a^m \in \mathfrak{a}$, $b^\ell \in \mathfrak{b}$. Then $x^{n(m+\ell)} = (x^n)^{m+\ell} \in \mathfrak{a}+\mathfrak{b}$ by using the binomial formula again. Thus $x \in r(\mathfrak{a}+\mathfrak{b})$.

(f) Since every prime ideal is radical, we conclude using (c) that $r(\mathfrak{p}^k) = r(\mathfrak{p}) = \mathfrak{p}$.

2. Consider the polynomial ring $A[X]$. Let $f = \sum_{i=0}^n a_i X^i \in A[X]$ be a polynomial. Prove:

   (a) f is a unit in $A[X]$ if and only if a_0 is a unit in A and $a_1, \dots, a_n$ are nilpotent.

   (b) f is nilpotent if and only if $a_0, \dots, a_n$ are nilpotent.

   (c) f is a zero-divisor if and only if there exists $a \neq 0$ in A such that $af = 0$.

   Solution:

   (a) Assume that f is a unit in $A[X]$. Then there is a polynomial $g = \sum_{i=0}^m b_i X^i \in A[X]$ such that $fg = 1$. We have

$$fg = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j X^k$$

and thus we conclude that $\sum_{i+j=k} a_i b_j = 0$ for all $k > 0$ and $a_0 b_0 = 1$. This proves, that a_0 is a unit. We show that $a_n^{r+1} b_{m-r} = 0$ for all $0 \leqslant r \leqslant m$ by induction on r. We already know that $a_n b_m = 0$, so we have $r = 0$. For $r > 0$ assume that we know the statement for $r' < r$. We have

$$0 = a_n^r \sum_{i+j=n+m-r} a_i b_j = a_n^{r+1} b_{m-r} + \sum_{i+j=n+m-r,\, j>m-r} a_i a_n^{n-i} a_n^{m-j} b_j = a_n^{r+1} b_{m-r}$$

where we used the induction hypothesis for every term in the sum. We conclude that $a_n^{r+1} b_{m-r} = 0$ for all $0 \leqslant r \leqslant m$ and in particular $a_n^{m+1} b_0 = 0$. Since b_0 is a unit, we conclude that a_n is nilpotent. To conclude the proof we show that $f - a_n X^n$ is still a unit. Then by the above it follows that a_{n-1} is nilpotent, so inductively we conclude that $a_1, \dots, a_n$ are nilpotent. To show that $f - a_n X^n$ is still a unit, we more generally prove that the difference of a unit and a nilpotent element in a ring R is a unit in R. Let $u \in R$ be a unit and $x \in R$ nilpotent with $x^\ell = 0$. Consider the element

$$h := \prod_{k=1}^{\ell} (u^{2^k} + x^{2^k})$$

and note that $(u-x)h = u^{2^\ell} - x^{2^\ell} = u^{2^\ell}$ by using ℓ times the binomial formula $(a-b)(a+b) = a^2 - b^2$ and the fact $2^\ell > \ell$. Since u^{2^ℓ} is a unit, too, we conclude that $(u-x)$ is a unit in R.

Conversely, by the above argument the sum of a unit and a nilpotent element is again a unit. Inductively we conclude that if a_0 is a unit and $a_1, \dots, a_n$ are nilpotent, then f is a unit.

(b) Since the nilradical is an ideal, it follows that sums and differences of nilpotent elements are nilpotent. Inductively, we conclude the equivalence.

(c) Assume that f is a zero-divisor and let $g = \sum_{i=0}^m b_i X^i \in A[X]$ be a non-zero polynomial of lowest degree such that $fg = 0$. We show by induction on r that $a_{n-r}g = 0$ for all $0 \leqslant r \leqslant n$. Let $r = 0$. Then $fg = 0$, so $a_n b_m = 0$. Hence $a_n g$ has strictly smaller degree than g and still anihilates f. We conclude that $a_n g = 0$. Let $r > 0$ and assume we know the statement for all smaller r. Note that $0 = fg = \sum_{i=0}^n a_i g X^i = \sum_{i=0}^{n-r} a_i g X^i$ by induction hypothesis. The highest term is thus $0 = a_{n-r} b_m X^{m+n-r}$. Hence, $a_{n-r}g$ has strictly smaller degree than g and still anihilates f. Thus $a_{n-r}g = 0$. We conclude that in particular $a_i b_0 = 0$ for all $0 \leqslant i \leqslant n$ and thus $b_0 f = 0$. The converse is trivial.

3. Fix an element $x_0 \in \mathbb{R}^n$. Denote by $\mathfrak{U} := \{U \subset \mathbb{R}^n \text{ open} \mid x_0 \in U\}$ the set of open neighbourhoods of x_0 and define the set

$$S := \{(U, f) \mid U \in \mathfrak{U},\ f : U \to \mathbb{R} \text{ continuous}\}.$$

We define an equivalence relation on S as follows: two elements $(U, f), (V, g) \in S$ are equivalent if and only if there is an open neighbourhood $W \subset U \cap V$ of x_0 such that $f|_W = g|_W$. We denote the set of equivalence classes of S by R. It is called *ring of germs* of continuous functions. Prove that R is a local ring.

Solution: We need first to define the two operations on R. For $(U, f), (V, g) \in S$ we define $(U, f) \cdot (V, g) := (U \cap V, fg)$ and $(U, f) + (V, g) := (U \cap V, f + g)$. The element $(\mathbb{R}^n, 1)$ is the multiplicative identity and $(\mathbb{R}^n, 0)$ is the additive identity. That this descends to a well-defined ring structure on R follows from direct calculations and the fact that the set of continuous functions on an open neighbourhood of x_0 forms a ring. We will show that it is local. Denote $\mathfrak{m} := \{[(U, f)] \in R \mid f(x_0) = 0\}$. This is a well-defined set and as a short calculation shows, it is an ideal. Also, $1 \notin \mathfrak{m}$. We show that every element $x \notin \mathfrak{m}$ is a unit. Let $[(U, f)] \notin \mathfrak{m}$. Then $f(x_0) \neq 0$. By continuity of f we conclude that there is an open neighbourhood $V \subset U$ such that $\forall x \in V : f(x) \neq 0$. Hence $[(V, \frac{1}{f})] \in R$ is an inverse of $[(U, f)]$. By the proposition from the lecture, we conclude that R is a local ring with maximal ideal $\mathfrak{m}$.

4. Show that the Zariski topology on $\mathbb{C}^n$ is coarser than the usual topology.

Solution: Let $X \subset \mathbb{C}^n$ be a Zariski-closed subset. Then there is some subset $S \subset \mathbb{C}[X_1, \ldots, X_n]$ such that $V(S) = X$. We have

$$X = V(S) = \{x \in \mathbb{C}^n \mid \forall f \in S: f(x) = 0\} = \bigcap_{f \in S} f^{-1}(0)$$

Because every polynomial $f \in S$ is continuous for the usual topology of $\mathbb{C}^n$ we conclude that $f^{-1}(0)$ is closed in the usual topology for all $f \in S$. Since an intersection of closed sets is closed we conclude that X is closed in the usual topology. To show that it is strictly coarser consider the set $\mathbb{Z} \times \{0\}^{n-1} \subset \mathbb{C}^n$. It is closed in the usual topology, but not in the Zariski-topology: Let $f \in \mathbb{C}[X_1, \ldots, X_n]$ be a polynomial that vanishes on $\mathbb{Z} \times \{0\}^{n-1}$. Thus $[f] \in \mathbb{C}[X_1, \ldots, X_n]/(X_2, \ldots, X_n) \cong \mathbb{C}[X_1]$ needs to be a polynomial that vanishes at all points in $\mathbb{Z}$ implying $[f] = 0$. This shows that f vanishes on $\mathbb{C} \times \{0\}^{n-1}$. This shows that the Zariski closure of $\mathbb{Z} \times \{0\}^{n-1}$ in $\mathbb{C}^n$ is $\mathbb{C} \times \{0\}^{n-1}$.

5. Let $X \subset k^n$ be a subset. Show that $I(X)$ is an ideal in $k[X_1, \ldots, X_n]$ and it is radical.

   Solution: Clearly $0 \in I(X)$ and for $f \in I(X)$ we have $-f \in I(X)$. Let $f, g \in I(X)$. Then $\forall x \in X: (f+g)(x) = f(x)+g(x) = 0$, hence $f+g \in I(X)$. Let $f \in I(X)$ and $h \in k[X_1, \ldots, X_n]$. Then $\forall x \in X: (hf)(x) = h(x)f(x) = 0$ and thus $hf \in I(X)$. This shows that $I(X)$ is an ideal in $k[X_1, \ldots, X_n]$. Now take $f \in k[X_1, \ldots, X_n]$ and $n > 0$ such that $f^n \in I(X)$. Thus for all $x \in X$ we have $f^n(x) = f(x)^n = 0$. Since k is an integral domain, we conclude that $f(x) = 0$ and thus $f \in I(X)$. This proves that $I(X)$ is radical.

6. Let $X, X' \subset k^n$ and $S, S' \subset k[X_1, \ldots, X_n]$ be subsets. Show:

   (a) $X \subset V(S) \iff S \subset I(X)$

   (b) $V(S \cup S') = V(S) \cap V(S')$

   (c) $I(X \cup X') = I(X) \cap I(X')$

   (d) $S \subset S' \Rightarrow V(S) \supset V(S')$

   (e) $X \subset X' \Rightarrow I(X) \supset I(X')$

   (f) $S \subset I(V(S))$

   (g) $X \subset V(I(X))$

   (h) $V(S) = V(I(V(S)))$

   (i) $I(X) = I(V(I(X)))$

   Solution: It all follows directly from the definitions.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 2

Extensions and Contractions, Modules, Spectrum of a Ring

1. Consider rings A, B and a ring homomorphism $\varphi : A \to B$. As in the lecture, denote:

$$C := \{\varphi^*(\mathfrak{b}) \mid \mathfrak{b} \subset B\} \subset A$$
$$E := \{\varphi_*(\mathfrak{a}) \mid \mathfrak{a} \subset A\} \subset B$$

for the set of contracted ideals and extended ideals, respectively. Show that C is closed under intersections, taking radicals and ideal quotients of ideals and E is closed under sums and products of ideals. More precisely, show that:

(a) for all $\mathfrak{a}, \mathfrak{b} \in C$ we have $\mathfrak{a} \cap \mathfrak{b} \in C$, $r(\mathfrak{a}) \in C$ and $(\mathfrak{a} : \mathfrak{b}) \in C$.

(b) for all $\mathfrak{a}, \mathfrak{b} \in E$ we have $\mathfrak{a} + \mathfrak{b} \in E$ and $\mathfrak{a}\mathfrak{b} \in E$.

Solution:

(a) Let $\mathfrak{c}, \mathfrak{d} \subset B$ be two ideals. The identity $\varphi^*(\mathfrak{c} \cap \mathfrak{d}) = \varphi^*(\mathfrak{c}) \cap \varphi^*(\mathfrak{d})$ follows by set theory and implies that the intersection of two contracted ideals is again contracted.

Next, we show that $\varphi^*(r(\mathfrak{c})) = r(\varphi^*(\mathfrak{c}))$. An element $f \in A$ is in $\varphi^*(r(\mathfrak{c}))$ if and only if there is an integer $n > 0$ such that $\varphi(f)^n = \varphi(f^n) \in \mathfrak{c}$. This is the case if and only if $f^n \in \varphi^*(\mathfrak{c})$ for some $n > 0$ which is equivalent to $f \in r(\varphi^*(\mathfrak{c}))$. This proves that the radical of a contracted ideal is again a contracted ideal.

Finally, we show that $\varphi^*((\mathfrak{c} : \varphi_*\varphi^*(\mathfrak{d}))) = (\varphi^*(\mathfrak{c}) : \varphi^*(\mathfrak{d}))$. Let $f \in \varphi^*((\mathfrak{c} : \varphi_*\varphi^*(\mathfrak{d})))$. Then $\varphi(f)\varphi_*\varphi^*(\mathfrak{d}) \subset \mathfrak{c}$, so by the property $\varphi^*\varphi_*\varphi^*(\mathfrak{d}) = \varphi^*(\mathfrak{d})$ we conclude $f\varphi^*(\mathfrak{d}) \subset \varphi^*(\mathfrak{c})$ and thus $f \in (\varphi^*(\mathfrak{c}) : \varphi^*(\mathfrak{d}))$. Conversely let $f \in (\varphi^*(\mathfrak{c}) : \varphi^*(\mathfrak{d}))$. Then $f\varphi^*(\mathfrak{d}) \subset \varphi^*(\mathfrak{c})$, which implies that $\varphi(f)\varphi(\varphi^*(\mathfrak{d})) \subset \mathfrak{c}$. Since $\mathfrak{c}$ is an ideal we conclude $\varphi(f)\varphi_*(\varphi^*(\mathfrak{d})) \subset \mathfrak{c}$. Hence $f \in \varphi^*((\mathfrak{c} : \varphi_*\varphi^*(\mathfrak{d})))$. This proves that the ideal quotient of contracted ideals is a contracted ideal.

(b) Let $\mathfrak{c}, \mathfrak{d} \subset A$ be ideals. We show that $\varphi_*(\mathfrak{c} + \mathfrak{d}) = \varphi_*(\mathfrak{c}) + \varphi_*(\mathfrak{d})$. We have the inclusion $\varphi(\mathfrak{c} + \mathfrak{d}) \subset \varphi_*(\mathfrak{c}) + \varphi_*(\mathfrak{d})$. Since the right hand side is an ideal we conclude that $\varphi_*(\mathfrak{c} + \mathfrak{d}) \subset \varphi_*(\mathfrak{c}) + \varphi_*(\mathfrak{d})$. Conversely we note that $\varphi_*(\mathfrak{c} + \mathfrak{d}) \supset \varphi(\mathfrak{c} + \mathfrak{d}) \supset \varphi(\mathfrak{c})$ and since the left hand side is an ideal also $\varphi_*(\mathfrak{c} + \mathfrak{d}) \supset \varphi_*(\mathfrak{c})$ and similarly $\varphi_*(\mathfrak{c} + \mathfrak{d}) \supset \varphi_*(\mathfrak{d})$. Since the sum of two ideals is the smallest ideal containing both ideals, we conclude that

$\varphi_*(\mathfrak{c}+\mathfrak{d}) \supset \varphi_*(\mathfrak{c}) + \varphi_*(\mathfrak{d})$. This shows that the sum of two extended ideals is again an extended ideal.

We show that $\varphi_*(\mathfrak{c}\mathfrak{d}) = \varphi_*(\mathfrak{c})\varphi_*(\mathfrak{d})$. By definition of the product of ideals we have $\varphi(\mathfrak{c}\mathfrak{d}) \subset \varphi_*(\mathfrak{c})\varphi_*(\mathfrak{d})$ and thus $\varphi_*(\mathfrak{c}\mathfrak{d}) \subset \varphi_*(\mathfrak{c})\varphi_*(\mathfrak{d})$. Conversely every element in $\varphi_*(\mathfrak{c})\varphi_*(\mathfrak{d})$ can be written as a finite sum of products ab with $a \in \varphi_*(\mathfrak{c})$ and $b \in \varphi_*(\mathfrak{d})$. These elements can again be expressed as finite linear combinations of elements in $\varphi(\mathfrak{c})$ and $\varphi(\mathfrak{d})$, respectively. Multiplying all out and using that φ is a homomorphism we get a finite linear combination of elements $\varphi(cd)$ with $c \in \mathfrak{c}$ and $d \in \mathfrak{d}$. Hence it is contained in $\varphi_*(\mathfrak{c}\mathfrak{d})$. This proves that the product of extended ideals is an extended ideal.

2. Let A be a ring and $\mathfrak{a} \subset A$ be an ideal that is contained in the Jacobson radical of A. Let M, N be A-modules, where N is finitely generated, and let $\varphi : M \to N$ be an A-module homomorphism. Consider the induced homomorphism

$$\varphi_{\mathfrak{a}} : M/\mathfrak{a}M \to N/\mathfrak{a}N$$

Prove that if $\varphi_{\mathfrak{a}}$ is surjective, then φ is surjective.

Solution: We first show that $\mathfrak{a}\left(N/\varphi(M)\right) = N/\varphi(M)$. Clearly, the left hand side is contained in the right hand side. Conversely, let $n \in N$. Because $\varphi_{\mathfrak{a}}$ is surjective, there is an element $m \in M$ such that $\varphi(m) - n \in \mathfrak{a}N$. Choose $a \in \mathfrak{a}$ and $n' \in N$ such that $\varphi(m) - n = an'$. Hence $n + an' \in \varphi(M)$. We conclude that $[n] = [an'] = a[n']$ in $N/\varphi(M)$ and thus the equality $\mathfrak{a}\left(N/\varphi(M)\right) = N/\varphi(M)$. By the fact that a quotient module of a finitely generated module is still finitely generated we can use Nakayama's lemma to conclude that $N/\varphi(M) = 0$ and hence φ is surjective.

3. Let k be a field and $0 \to M_0 \to \cdots \to M_n \to 0$ be an exact sequence of finite dimensional k-vector spaces and k-linear maps. Prove that

$$\sum_{i=0}^{n} (-1)^i \dim_k(M_i) = 0$$

Solution: Denote d_i for the map $d_i : M_i \to M_{i+1}$, where we denote $M_k = 0$ for $k > n$. The long exact sequence splits into short exact sequences $0 \to \ker(d_i) \to M_i \to \operatorname{im}(d_i) \to 0$. By using the dimension formula for linear maps of finite dimensional vector spaces and the fact $\ker(d_{i+1}) = \operatorname{im}(d_i)$ we conclude that $\dim_k(\ker(d_i)) + \dim_k(\ker(d_{i+1})) = \dim_k(M_i)$. Thus

$$\sum_{i=0}^{n} (-1)^i \dim_k(M_i) = \dim_k(\ker(d_0)) + (-1)^n \dim_k(\ker(d_{n+1})) = 0.$$

4. Prove the 4-Lemma by diagram chasing: If the rows of the commutative diagram of A-modules and A-module homomorphisms

$$\begin{tikzcd}
M_1 \arrow[r] \arrow[d, "\alpha"] & M_2 \arrow[r] \arrow[d, "\beta"] & M_3 \arrow[r] \arrow[d, "\gamma"] & M_4 \arrow[d, "\delta"] \\
M_1' \arrow[r] & M_2' \arrow[r] & M_3' \arrow[r] & M_4'
\end{tikzcd}$$

are exact, then the following holds:

(a) If α is surjective, and β and δ are injective, then γ is injective;

(b) if δ is injective, and α and γ are surjective, then β is surjective.

Solution: We will denote $d_i : M_i \to M_{i+1}$ and $d_i' : M_i' \to M_{i+1}'$.

(a) Let $m_3 \in M_3$ with $\gamma(m_3) = 0$. By commutativity of the right square and injectivity of δ we conclude that $d_3(m_3) = 0$. Thus there is an element $m_2 \in M_2$ such that $d_2(m_2) = m_3$. Consider the element $\beta(m_2)$. We have $d_2'(\beta(m_2)) = \gamma(m_3) = 0$. We conclude that there is an element $m_1' \in M_1'$ such that $d_1'(m_1') = \beta(m_2)$. Since α is surjective, there is an element $m_1 \in M_1$ such that $\alpha(m_1) = m_1'$. By injectivity of β and using $\beta(d_1(m_1)) = d_1'(\alpha(m_1)) = \beta(m_2)$ we conclude that $d_1(m_1) = m_2$. Hence $m_3 = d_2(m_2) = d_2(d_1(m_1)) = 0$. This proves that γ is injective.

(b) Let $m_2' \in M_2'$ and look at $d_2'(m_2')$. Since γ is surjective there is an element $m_3 \in M_3$ such that $\gamma(m_3) = d_2'(m_2')$. We have $\delta(d_3(m_3)) = d_3'(\gamma(m_3)) = d_3'(d_2'(m_2')) = 0$. Since δ is injective this implies that $d_3(m_3) = 0$. Thus there is an element $m_2 \in M_2$ such that $d_2(m_2) = m_3$. By commutativity of the middle square we conclude that $d_2'(\beta(m_2) - m_2') = 0$. Hence there is an element $a' \in M_1'$ such that $d_1'(a') = \beta(m_2) - m_2'$. Since α is surjective we can lift this to an element $a \in M_1$ such that $\alpha(a) = a'$. Finally we conclude that $\beta(m_2 - d_1(a)) = d_1'(a') + m_2' - d_1'(\alpha(a)) = m_2'$, which proves that β is surjective.

5. Prove the 3×3-lemma: If

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M_1' \arrow[r] \arrow[d] & M_2' \arrow[r] \arrow[d] & M_3' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_1 \arrow[r] \arrow[d] & M_2 \arrow[r] \arrow[d] & M_3 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_1'' \arrow[r] \arrow[d] & M_2'' \arrow[r] \arrow[d] & M_3'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

is a commutative diagram of A-modules and A-module homomorphisms, and all columns and the middle row are exact, then the top row is exact if and only if the bottom row is exact.

Solution: This follows directly from the snake lemma: if the bottom row is exact, look at the morphisms $M_i \to M_i''$ and use the snake lemma. If the top row is exact, use the snake lemma for the morphisms $M_i' \to M_i$.

6. In this exercise, we generalize the notion of an affine variety introduced in the lecture. Let A be a ring. We denote by $\mathrm{spec}(A)$ the set of all prime ideals of A. For a subset $S \subset A$ define

$$V(S) := \{\mathfrak{p} \in \mathrm{spec}(A) \mid S \subset \mathfrak{p}\}$$

Show that:

(a) If $\mathfrak{a} \subset A$ is the ideal generated by S, then $V(S) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

(b) $V(0) = \mathrm{spec}(A)$ and $V(1) = \varnothing$.

(c) For a family of subsets $(S_i)_{i \in I} \subset A$ we have $V(\bigcup_{i \in I} S_i) = \bigcap_{i \in I} V(S_i)$.

(d) For finitely many ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset A$ we have $V(\bigcap_{i=1}^n \mathfrak{a}_i) = \bigcup_{i=1}^n V(\mathfrak{a}_i)$.

This shows that the subsets $(V(S))_{S \subset A}$ form the closed sets of a topology on $\mathrm{spec}(A)$, called *Zariski* topology. We call the topological space $\mathrm{spec}(A)$ the *(prime) spectrum* of A.

Solution:

(a) Every prime ideal that containes S also contains $\mathfrak{a}$ and vice versa. Thus $V(S) = V(\mathfrak{a})$. The radical of $\mathfrak{a}$ is the intersection of all prime ideals containing $\mathfrak{a}$. Thus every prime ideal that contains $\mathfrak{a}$ contains $r(\mathfrak{a})$ and the converse is clear. Hence $V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

(b) Every prime ideal contains the zero ideal and no prime ideal contains the unit ideal, hence $V(0) = \operatorname{spec}(A)$ and $V(1) = \varnothing$.

(c) This follows by set theory.

(d) We use a proposition from the lecture. If a prime ideal $\mathfrak{p}$ contains $\bigcap_{i=1}^{n} \mathfrak{a}_i$, then it contains one of the $\mathfrak{a}_i$ by the proposition. Thus $V(\bigcap_{i=1}^{n} \mathfrak{a}_i) \subset \bigcup_{i=1}^{n} V(\mathfrak{a}_i)$. The converse is true by set theory.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 3

Tensor Product, Modules, Spectrum of a Ring

1. Let A be a local ring and M, N two finitely generated A-modules. Prove that $M \otimes_A N = 0$ implies $M = 0$ or $N = 0$. Give an example of modules over a non-local ring which do not have this property.

   Solution: Denote by $\mathfrak{m}$ the maximal ideal of A and by $k := A/\mathfrak{m}A$ the residue field. Assume that $M \otimes_A N = 0$. Naturally $M/\mathfrak{m}M$ and $N/\mathfrak{m}N$ are not only A-modules but also k-vector spaces. First we prove that $(M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N) = 0$. Look at the surjective map $M \twoheadrightarrow M/\mathfrak{m}M$. By right exactness of the tensor product we conclude that $M \otimes_A N \twoheadrightarrow M/\mathfrak{m}M \otimes_A N$ is surjective. Similarly we find that $(M/\mathfrak{m}M) \otimes_A N \twoheadrightarrow (M/\mathfrak{m}M) \otimes_A (N/\mathfrak{m}N)$ is surjective. Hence the composite map is surjective, which proves that $(M/\mathfrak{m}M) \otimes_A (N/\mathfrak{m}N) = 0$. We note that the tensor map $(M/\mathfrak{m}M) \times (N/\mathfrak{m}N) \to (M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N)$ is k-bilinear and thus in particular A-bilinear. Hence it factors through $(M/\mathfrak{m}M) \otimes_A (N/\mathfrak{m}N)$ by the universal property. We conclude that the tensor map is zero and thus $(M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N) = 0$. Now by the dimension formula of tensor products of vector spaces (or by considering an explicit basis) we conclude that $M/\mathfrak{m}M = 0$ or $N/\mathfrak{m}N = 0$ and thus $M = \mathfrak{m}M$ or $N = \mathfrak{m}N$. By Nakayama's Lemma it follows that $M = 0$ or $N = 0$.

   An example where this is not true over a non-local ring is $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$. This is zero because for every elementary tensor $a \otimes b$ we have $a \otimes b = (3a) \otimes b = a \otimes (3b) = a \otimes 0 = 0$.

2. Let A be a ring. Prove the following:

   (a) If M and N are flat A-modules, then so is $M \otimes_A N$.

   (b) If B is a flat A-algebra and M a flat B-module, then M is flat as an A-module.

   Solution:

   (a) Let $L \hookrightarrow L'$ be an injective homomorphism of A-modules. Since M and N are flat and using a proposition from the lecture we conclude that the induced homomorphism $L \otimes_A M \to L' \otimes_A M$ is injective. Using this proposition again we conclude that $(L \otimes_A M) \otimes_A N \to (L' \otimes_A M) \otimes_A N$ is injective. By associativity of the tensor product we conclude that $L \otimes_A (M \otimes_A N) \to L' \otimes_A (M \otimes_A N)$ is injective and hence $M \otimes_A N$ is flat, by using the proposition again.

(b) Let $L \hookrightarrow L'$ be an injective homomorphism of A-modules. We use the A-isomorphism $(L \otimes_A B) \otimes_B M \cong L \otimes_A M$ given by $\ell \otimes b \otimes m \mapsto \ell \otimes (bm)$ and the analogue for L'. That this is indeed well-defined can be checked using the universal property of the tensor product in the following way: for every element $m \in M$ we have an A-bilinear map $L \times B \to L \otimes_A M$ given by $(l, b) \mapsto l \otimes (bm)$. Hence it factors through the tensor product $L \otimes_A B$. Varying $m \in M$ we get a homomorphism $(L \otimes_A B) \times M \to L \otimes_A M$ which is not only A-bilinear, but also B-bilinear. It thus factors through the tensor product $(L \otimes_A B) \otimes_B M$. Conversely the map $L \times M \to (L \otimes_A B) \otimes_B M$ given by $(l, m) \mapsto (l \otimes 1) \otimes m$ is A-bilinear and thus factors through the tensor product $L \otimes_A M$. It is not hard to see that this provides an inverse for the mentioned map and thus we have an isomorphism.

We get a commutative diagram

$$\begin{tikzcd}
L \otimes_A M \arrow[r] \arrow[d, "\cong"] & L' \otimes_A M \arrow[d, "\cong"] \\
(L \otimes_A B) \otimes_B M \arrow[r] & (L' \otimes_A B) \otimes_B M
\end{tikzcd}$$

The A-homomorphism at the bottom is injective because of the flatness of B as an A-module and the flatness of M as a B-module. Hence the upper A-homomorphism is injective. By the proposition from the lecture this implies that M is flat as an A-module.

3. Let A be a ring. Consider a short exact sequence of A-modules and homomorphisms $0 \to M' \to M \to M'' \to 0$. Prove that if M' and M'' are finitely generated, then so is M.

   Solution: Let $m'_1, \ldots, m'_r \in M'$ and $n''_1, \ldots, n''_s \in M''$ be generators of the respective A-modules. Denote by $m_1, \ldots, m_r \in M$ the images of $m'_1, \ldots, m'_r$ in M and by $n_1, \ldots, n_s \in M$ lifts of $n''_1, \ldots, n''_s$ in M. We claim that $m_1, \ldots, m_r, n_1, \ldots, n_s$ generate M. Let $a \in M$. By assumption its image $a'' \in M''$ can be written as $\sum_{i=1}^s \alpha_i n''_i$ for some coefficients $\alpha_1, \ldots, \alpha_s \in A$. But then $a - \sum_{i=1}^s \alpha_i n_i$ is in the kernel of the map $M \to M''$ and thus is the image of an element $b \in M'$. By assumption $b = \sum_{j=1}^r \beta_j m'_j$ for some coefficients $\beta_1, \ldots, \beta_r \in A$. We conclude that $a = \sum_{i=1}^s \alpha_i n_i + \sum_{j=1}^r \beta_j m_j$. This proves the claim.

4. Let A be a ring. Prove that for any three A-modules M_1, M_2, M and homomorphisms $M_1 \xrightarrow{f} M \xleftarrow{g} M_2$ there exists an A-module P and homomorphisms $M_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} M_2$ such that the diagram

$$\begin{tikzcd}
P \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & M_2 \arrow[d, "g"] \\
M_1 \arrow[r, "f"] & M
\end{tikzcd}$$

commutes and with the following universal property: for any A-module N and homomorphisms $M_1 \xleftarrow{u} N \xrightarrow{v} M_2$ such that $f \circ u = g \circ v$ there exists a unique homomorphism $h : N \to P$ making the whole diagram commute:

$$\begin{tikzcd}
N \arrow[dr, dotted, "h"] \arrow[drr, bend left, "v"] \arrow[ddr, bend right, "u"'] & & \\
& P \arrow[r, "\pi_2"'] \arrow[d, "\pi_1"] & M_2 \arrow[d, "g"'] \\
& M_1 \arrow[r, "f"] & M
\end{tikzcd}$$

Finally, show that P is unique up to a unique isomorphism.

[Hint: Look at a submodule of $M_1 \times M_2$.]

Solution: We define $P := \{(m_1, m_2) \in M_1 \oplus M_2 \mid f(m_1) = g(m_2)\}$. Since it is the kernel of the homomorphism $M_1 \oplus M_2 \to M$ given by $(m_1, m_2) \mapsto f(m_1) - g(m_2)$ it is an A-module. We define $\pi_1 : P \to M_1$ and $\pi_2 : P \to M_2$ to be the respective projections of $M_1 \oplus M_2$ restricted to P. By the very definition of P the diagram

$$\begin{tikzcd}
P \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & M_2 \arrow[d, "g"] \\
M_1 \arrow[r, "f"] & M
\end{tikzcd}$$

commutes. We show that (P, π_1, π_2) satisfies the required universal property. Let N be an A-module and let $u : N \to M_1$ and $v : N \to M_2$ be homomorphisms such that $f \circ u = g \circ v$. We construct a homomorphism $h : N \to P$ by $h(n) := (u(n), v(n))$. By the requirement $f \circ u = g \circ v$ this is indeed well-defined. And it is a homomorphism, since u and v are homomorphisms. Furthermore, we see that the diagram

$$\begin{tikzcd}
N \arrow[dr, dotted, "h"] \arrow[drr, bend left, "v"] \arrow[ddr, bend right, "u"'] & & \\
& P \arrow[r, "\pi_2"'] \arrow[d, "\pi_1"] & M_2 \arrow[d, "g"'] \\
& M_1 \arrow[r, "f"] & M
\end{tikzcd}$$

commutes. The uniqueness of h follows directly from the construction. Now let (P', π_1', π_2') be another module with the same universal property. Then by the universal property of P we have a unique homomorphism $h : P' \to P$ such that the diagram

$$
\begin{tikzcd}
P' \arrow[dr, dotted, "h"] \arrow[drr, bend left, "\pi_2'"] \arrow[ddr, bend right, "\pi_1'"'] & & \\
& P \arrow[r, "\pi_2"'] \arrow[d, "\pi_1"] & M_2 \arrow[d, "g"'] \\
& M_1 \arrow[r, "f"] & M
\end{tikzcd}
$$

commutes. Using the universal property for P' we analogously get a homomorphism $h' : P \to P'$. Composing those homomorphisms we get a homomorphism $h' \circ h : P \to P$ such that the diagram

$$
\begin{tikzcd}
P \arrow[dr, dotted, "h' \circ h"] \arrow[drr, bend left, "\pi_2"] \arrow[ddr, bend right, "\pi_1"'] & & \\
& P \arrow[r, "\pi_2"'] \arrow[d, "\pi_1"] & M_2 \arrow[d, "g"'] \\
& M_1 \arrow[r, "f"] & M
\end{tikzcd}
$$

commutes. By the uniqueness statement of the universal property of P we conclude that $h' \circ h$ is the identity. Hence h is a unique isomorphism.

5. Let A be a ring. Recall the definition of the prime spectrum of a ring from exercise sheet 2. For every element $f \in A$ denote $D(f)$ for the open complement of $V((f))$ in $\mathrm{spec}(A)$. Show that these sets form a basis of open sets for the Zariski topology on $\mathrm{spec}(A)$. Furthermore, prove:

   (a) $\forall f, g \in A$ we have $D(f) \cap D(g) = D(fg)$

   (b) $D(f) = \varnothing$ if and only if f is nilpotent

   (c) $D(f) = \mathrm{spec}(A)$ if and only if f is a unit

   (d) $\mathrm{spec}(A)$ is quasicompact

   These open sets are called *basic open sets* of $\mathrm{spec}(A)$.

   Solution: By definition we can write $D(f) = \{\mathfrak{p} \in \mathrm{spec}(A) \mid f \notin \mathfrak{p}\}$ for $f \in A$. We need to show that the basic open sets cover $\mathrm{spec}(A)$ and that for every two basic open sets B_1, B_2 and every point $x \in B_1 \cap B_2$ there is a basic open set B_3 such that $x \in B_3 \subset B_1 \cap B_2$. The first property is true because of $D(1) = \mathrm{spec}(A)$. For the second one let $D(f), D(g)$ with $f, g \in A$ be basic open sets. By (a) below we have $D(f) \cap D(g) = D(fg)$ and thus the second property of being a basis for the topology is also satisfied. Hence the basic open sets form indeed a basis for the topology.

(a) For every prime ideal $\mathfrak{p} \subset A$ we have $fg \notin \mathfrak{p}$ if and only if $f \notin \mathfrak{p}$ and $g \notin \mathfrak{p}$. Thus the equality.

(b) Since the nilradical is the intersection of all prime ideals, every prime ideal contains all nilpotent elements. Thus $D(f) = \varnothing$ for all nilpotent elements $f \in A$.

(c) By definition a prime ideal cannot contain a unit, hence $D(f) = \operatorname{spec}(A)$ for every unit $f \in A$.

(d) Since the basic open sets form a basis of the topology it is enough to consider covers by basic open sets. Let $(f_i)_{i \in I} \in A$ be elements such that $\bigcup_{i \in I} D(f_i) = \operatorname{spec}(A)$. By taking the complement and using de Morgans law we get $\bigcap_{i \in I} V((f_i)) = \varnothing$. By exercise sheet 2, exercise 6(c) and 6(a) we conclude that $V(\sum_{i \in I}(f_i)) = \varnothing$. Hence the ideal $\sum_{i \in I}(f_i)$ must contain 1. Thus there is a finite subset $J \subset I$ such that $\sum_{j \in J}(f_j)$ contains 1. But then by the above argument in reverse, we have $\bigcup_{j \in J} D(f_j) = \operatorname{spec}(A)$. Hence the finite subcover already covers $\operatorname{spec}(A)$.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 4

Localisation, Splitting Lemma, Irreducible Variety

1. Let A be a ring ~~reduced ring (i.e. without any nonzero nilpotent elements)~~. Let M be a finitely generated A-module and let $f : M \to M$ be a surjective module homomorphism. Then f is also injective.

   Remark: The intended proof did not work, so we give a general proof which does not need A to be reduced. Many apologies for this inconvenience!

   Solution:

   One variant of Nakayama says that if N is a finitely generated A-module and $\mathfrak{a} \subset A$ an ideal such that $\mathfrak{a}N = N$, then there is an element $x \in 1 + \mathfrak{a}$ such that $xN = 0$. We use this as follows: We consider M as $A[X]$-module, where X acts as f on M, i.e. for any $p(X) \in A[X]$ and $m \in M$ we have $p(X) \cdot m = p(f)(m)$. Since f is surjective, for the ideal $\mathfrak{a} := (X)$ we have $\mathfrak{a}M = M$. Hence there is an element $a \in 1 + \mathfrak{a}$ such that $aM = 0$, which implies that there is a polynomial $q(X) \in A[X]$ such that $1 + q(X)X = a$. We conclude that for every element $b \in \ker(f)$ we have $b = (1 + q(X)X)b = ab = 0$. Hence f is injective.

2. Let A be a ring such that every localisation $A_\mathfrak{p}$ of A with respect to a prime ideal $\mathfrak{p} \subset A$ has no nonzero nilpotent elements. Prove that A has no nonzero nilpotent elements. Is the same true for zero-divisors?

   Solution: We have $0 = \mathfrak{nil}(A_\mathfrak{p}) = \mathfrak{nil}(A)_\mathfrak{p}$ for all prime ideals $\mathfrak{p} \subset A$. Since being zero is a local property of an A-module, we conclude that $\mathfrak{nil}(A) = 0$. For zero-divisors this is not true as the following example shows: consider $\mathbb{Q} \times \mathbb{Q}$ as ring. It certainly has zero-divisors and the only prime ideals are $\{0\} \times \mathbb{Q}$ and $\mathbb{Q} \times \{0\}$. Denote by R the localisation at $\{0\} \times \mathbb{Q}$. Assume that $[(a, b) : (0, c)]$ is a zero-divisor in R. Then there is an element $[(d, e) : (0, f)]$ in R such that their product $[(ad, eb) : (0, cf)]$ is zero, so by definition of the localisation there is an element $(g, h) \notin \{0\} \times \mathbb{Q}$ such that $(adg, ebh) = (ad, eb)(g, h) = 0$. Since g is non-zero, either a or d is zero. But then $(a, b)(1, 0) = 0$ or $(d, e)(1, 0) = 0$ and so one of the elements $[(a, b) : (0, c)]$ or $[(d, e) : (0, f)]$ must be zero in R already and thus is no non-zero zero-divisor.

3. Let A be a ring. Let T, S be two multiplicatively closed subsets and let U be the image of T in $S^{-1}A$. Prove that $(ST)^{-1}A$ is isomorphic to $U^{-1}S^{-1}A$.

   Solution: Consider the canonical map $f : A \to (ST)^{-1}A$. Since $S \subset ST$, the elements of the subset $f(S) \subset (ST)^{-1}A$ are invertible and thus f factors through a unique homomorphism $g : S^{-1}A \to (ST)^{-1}A$ by the universal property. But as $T \subset ST$, we see that the elements of $g(U) = f(T) \subset (ST)^{-1}A$ are invertible and by the universal property g factors through a unique homomorphism $h : U^{-1}S^{-1}A \to (ST)^{-1}A$. Conversely consider the map $f' : A \to U^{-1}S^{-1}A$. We see that the elements of $f'(ST)$ are invertible and thus f' factors through a unique homomorphism $h' : (ST)^{-1}A \to U^{-1}S^{-1}A$. By using the uniqueness we conclude that $h \circ h'$ and $h' \circ h$ are both the respective identity homomorphisms. Thus h is an isomorphism with inverse h'.

4. Let A be an integral domain and M an A-module. Prove that the following are equivalent:

   (a) M is torsion-free.

   (b) $M_{\mathfrak{p}}$ is torsion-free for all prime ideals $\mathfrak{p} \subset A$.

   (c) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals $\mathfrak{m} \subset A$.

   Solution: "(a)$\Rightarrow$(b)": Assume that there is a prime ideal $\mathfrak{p} \subset A$ such that $M_{\mathfrak{p}}$ has a torsion element $[m, s] \in M_{\mathfrak{p}}$, where $m \in M$ is non-zero and $s \notin \mathfrak{p}$. Thus there is a non-zero element $a \in A$ such that $a[m, s] = [am, s] = 0$. By definition of localisation there is an element $r \notin \mathfrak{p}$ such that $ram = 0$. Since A is an integral domain we conclude that $am = 0$ and hence M has torsion.

   "(b)$\Rightarrow$(c)": Immediate.

   "(c)$\Rightarrow$(a)": Let $m \in M$ be a non-zero torsion element. Consider the annihilator $\mathrm{Ann}(m) := \{a \in A \mid am = 0\}$ of m. It is an ideal which clearly does not contain 1. Hence there is a maximal ideal $\mathfrak{m} \subset A$ containing $\mathrm{Ann}(m)$. The element $[m, 1]$ is non-zero in $M_{\mathfrak{m}}$ because there is no element $s \notin \mathfrak{m}$ such that $sm = 0$. But $[m, 1]$ is still annihilated by a non-zero element of A and hence $M_{\mathfrak{m}}$ has torsion.

5. (Splitting Lemma) Let A be a ring and $0 \to M' \to M \to M'' \to 0$ a short exact sequence of A-modules. The sequence is called *split* if there is an isomorphism $M \to M' \oplus M''$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, equal] & M \arrow[r, "v"] \arrow[d, "\cong"] & M'' \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & M' \arrow[r] & M' \oplus M'' \arrow[r] & M'' \arrow[r] & 0 \end{tikzcd}$$

   commutes, where the homomorphisms in the lower row are the inclusion and projection respectively.

   Prove the splitting lemma, i.e. that the following are equivalent:

   (a) The short exact sequence splits.

   (b) There is a homomorphism $i : M'' \to M$ such that $v \circ i = \mathrm{id}_{M''}$.

(c) There is a homomorphism $s : M \to M'$ such that $s \circ u = \mathrm{id}_{M'}$.

Solution: Denote $\pi_1 : M' \oplus M'' \to M'$ and $\pi_2 : M' \oplus M'' \to M''$ for the respective projections, and $\varphi_1 : M' \to M' \oplus M''$ and $\varphi_2 : M'' \to M' \oplus M''$ for the respective inclusions.

"(a)⇒(b)": Denote $f : M \to M' \oplus M''$ for the given isomorphism. We define the homomorphism $i : M'' \to M$ to be $i := f^{-1} \circ \varphi_2$. Then $v \circ i = \pi_2 \circ f \circ f^{-1} \circ \varphi_2 = \mathrm{id}_{M''}$.

"(a)⇒(c)": Denote $f : M \to M' \oplus M''$ for the given isomorphism. We define the homomorphism $s : M \to M'$ to be $s := \pi_1 \circ f$. Then $s \circ u = \pi_1 \circ f \circ f^{-1} \varphi_1 = \mathrm{id}_{M'}$.

"(b)⇒(a)": We define a homomorphism $g : M' \oplus M'' \to M$ as $g := u + i$. Note that $(0 \oplus v) \circ g = 0 \oplus \mathrm{id}_{M''}$. Thus for any element $(m', m'') \in M' \oplus M''$ with $g(m', m'') = 0$ we conclude that $m'' = 0$. Hence $u(m') = 0$. Since u is injective we conclude that $m' = 0$. This shows that g is injective. On the other hand, let $m \in M$ and consider the element $n := m - i \circ v(m)$. This element is in the kernel of v and thus lifts to an element $n' \in M'$. We conclude that $g(n', v(m)) = u(n') + i \circ v(m) = m$ and hence g is surjective and therefore an isomorphism. The commutativity of the diagram holds by design.

"(c)⇒(a)": Define a homomorphism $f : M \to M' \oplus M''$ by $f := s \oplus v$. Note that $f \circ u = (\mathrm{id}_{M'} \oplus 0)$. Hence any non-zero element $m \in M$ with $f(m) = 0$ cannot lie in the image of u. But then $v(m) \neq 0$ and so f is injective. On the other hand, for every element $(m', m'') \in M' \oplus M''$ we can choose a lift $n \in M$ of $m'' \in M''$ and so we have $f(u(m') + n) = (m', m'')$. Hence f is surjective and therefore an isomorphism.

6. A topological space is called *irreducible* if it is non-empty and every two non-empty open subsets have a non-empty intersection. Prove that for $\mathrm{spec}(A)$ the following are equivalent:

   (a) $\mathrm{spec}(A)$ is irreducible.

   (b) The nilradical of A is a prime ideal.

   (c) There is a dense point $x \in \mathrm{spec}(A)$, i.e. the closure of $\{x\}$ is $\overline{\{x\}} = \mathrm{spec}(A)$.

   Remark: We call such a point as in (c) a *generic point.*

   Solution: "(a)⇒(b)": If the nilradical is not a prime ideal, then there are elements a, b which are not in the nilradical but such that ab is in the nilradical. Hence $D(a) \cap D(b) = D(ab) = \varnothing$ by using exercise 5 on exercise sheet 3. But a and b are both not in the nilradical and thus there are prime ideals which do not contain a or b, respectively. Thus $D(a)$ and $D(b)$ are both non-empty. Hence $\mathrm{spec}(A)$ is reducible.

   "(b)⇒(c)": By assumption, the nilradical is itself a point in $\mathrm{spec}(A)$. Let $V(S)$ be a closed set that contains the nilradical $\mathfrak{nil}(A)$. Thus $S \subset \mathfrak{nil}(A)$. Since $\mathfrak{nil}(A)$

is the intersection of all prime ideals, we conclude that $S \subset \mathfrak{p}$ for all prime ideals $\mathfrak{p} \subset A$ and thus $V(S) = \mathrm{spec}(A)$.

"(c)$\Rightarrow$(a)": If there exists a dense point, then every non-empty open subset has to contain it. In particular $\mathrm{spec}(A)$ is non-empty. Then the intersection of every two non-empty open subsets is non-empty because it contains the dense point.

Solutions Sheet 5

Noetherian Rings, Modules and Topological Spaces

1. Let A be a ring. If $A[X]$ is Noetherian, is A necessarily Noetherian?

   Solution: Yes, because $A \cong A[X]/(X)$ and a quotient of a Noetherian ring is Noetherian.

2. Let A be a ring such that every localisation $A_\mathfrak{p}$ at a prime ideal $\mathfrak{p} \subset A$ is Noetherian. Is A necessarily Noetherian?

   Solution: No. A counterexample is $R := \prod_{i \in \mathbb{N}} \mathbb{Z}/2\mathbb{Z}$, an infinite product of copies of $\mathbb{Z}/2\mathbb{Z}$. The ring R is not Noetherian, since $\left(\prod_{0 \leqslant i \leqslant n} \mathbb{Z}/2\mathbb{Z}\right)_{n \in \mathbb{N}}$ is a strictly increasing chain of ideals. It is not hard to see that every element in R is idempotent, i.e. for every $a \in R$ we have $a^2 = a$. Pick a prime ideal $\mathfrak{p} \subset R$. Let $a \in \mathfrak{p}$. Then clearly $1 - a \notin \mathfrak{p}$ and we have $a(1-a) = a - a^2 = 0$. Thus $a = 0$ in the localisation $R_\mathfrak{p}$. But every element $b \notin \mathfrak{p}$ becomes a unit in $R_\mathfrak{p}$. We conclude that $R_\mathfrak{p}$ is a field and in particular Noetherian. This provides a counter example.

3. Which of the following rings over $\mathbb{C}$ are Noetherian?

   (a) The ring of rational functions of z having no pole on the circle $|z| = 1$.

   (b) The ring of power series in z with a positive radius of convergence.

   (c) The ring of power series in z with an infinite radius of convergence.

   (d) The ring of polynomials in z whose first k derivatives vanish at the origin, where k is a fixed non-negative integer.

   (e) The ring of polynomials in z, w whose partial derivatives with respect to w vanish for $z = 0$.

   Solution: (Thanks to JJ for these solutions)

   (a) It is Noetherian: Define

   $$S := \mathbb{C}[z] \smallsetminus \bigcup_{\substack{a \in \mathbb{C} \\ |a|=1}} (z - a)$$

   Then S is a multiplicative subset of $\mathbb{C}[z]$ and $S^{-1}\mathbb{C}[z]$ is the ring of rational functions having no pole on the unit circle. Since $\mathbb{C}$ is a field and thus Noetherian, the Hilbert Basis Theorem states that $\mathbb{C}[z]$ is Noetherian. Further, the Noetherian property is preserved by localization, hence this ring is Noetherian.

(b) It is Noetherian: We can identify the ring of power series with positive radius of convergence with the ring of germs of holomorphic functions at $z = 0$. The elements of the latter are defined as equivalence classes of tuples (U, f) consisting of an open set U containing 0 and a holomorphic function $f : U \to \mathbb{C}$. Two such tuples (U, f) and (V, g) are equivalent whenever f and g agree on some subset of $U \cap V$ containing 0. Denote this ring by R. If a non-zero element in R represented by (U, f) satisfies $f(0) \neq 0$, then this element is a unit. On the other hand, if $f(0) = 0$, then there exist an integer $k \geqslant 1$ and unit (V, h) such that $f = z^k h$. From this follows that every non-zero ideal is of the form (z^k) for some k. Moreover $(z^k) \subset (z^\ell)$ precisely when $\ell \leqslant k$. Since every decreasing sequence of positive integers becomes constant, we see that R is Noetherian.

(c) It is not Noetherian: Let R denote the ring in question. This can be identified with the ring of holomorphic functions on $\mathbb{C}$. For each $n \in \mathbb{Z}_{>0}$ define

$$I_n = \{f \in R \mid f(k) = 0 \text{ for all } k \in \mathbb{Z} \text{ with } |k| \geqslant n\}$$

Then each I_n is an ideal, and properly contained in I_{n+1} (take for example (the continuation of) $\frac{\sin(\pi z)}{\prod_{k=-n}^{n}(z-k)}$). Thus $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$ is a strictly increasing sequence of ideals. Hence R is not Noetherian.

(d) It is Noetherian: Let $S = \mathbb{C} + z^{k+1}\mathbb{C}[z] \subset \mathbb{C}[z]$ be the ring of polynomials whose first k derivatives vanish at the origin. Consider the subring $R = \mathbb{C}[z^{k+1}]$. Then S is generated as an R-module by the elements $1, z^{k+2}, \ldots, z^{2k+1}$. Hence S is Noetherian as an R-module (a quotient of a free R-module). But if a ring is Noetherian over a subring then it is already Noetherian.

(e) It is not Noetherian: Let $R = \mathbb{C}[z, zw, zw^2, zw^3, \ldots] \subset \mathbb{C}[z, w]$. Then R is the ring of polynomials p such that $\frac{\partial p}{\partial w}(0, w) = 0$. Let $I_n := (z, zw, \ldots, zw^n)$. We claim that $zw^{n+1} \notin I_n$, which implies that the I_n form a strictly increasing sequence of ideals. Consider a general element $f = \sum_{k=0}^{n} b_k zw^k$ in I_n, where $b_k \in R$. Any monomial of b_k which is divided by w is also divided by z. Thus we find that all the monomials of f are either a scalar multiple of $z^m w^n$ for some $m \geqslant 2$ or of zw^k for some $0 \leqslant k \leqslant n$. Hence indeed $zw^{n+1} \notin I_n$.

4. Let k be a field which is finitely generated as $\mathbb{Z}$-module. Prove that k is a finite field.

Solution: Assume by contradiction that $\mathrm{char}(k) = 0$. Since k is finitely generated as $\mathbb{Z}$-module and $\mathbb{Z}$ is Noetherian, we know that k is Noetherian as module over $\mathbb{Z}$. But $\mathbb{Q} \subset k$ is a submodule and thus $\mathbb{Q}$ is finitely generated as $\mathbb{Z}$-module which we know is not true. A contradiction. Now assume that $\mathrm{char}(k) = p > 0$. Then $\mathbb{F}_p \subset k$. Since k is finitely generated as $\mathbb{Z}$-module, it is finitely generated as $\mathbb{F}_p$-module. Thus k is finite.

5. Let X be a topological space. We say that X is *Noetherian*, if the open subsets of X satisfy the ascending chain condition, i.e. for every chain $U_i \subset U_{i+1}$ for $i \geqslant 0$ of open subsets, there is an integer $n \geqslant 0$ such that $U_i = U_{i+1}$ for all $i \geqslant n$. Prove:

   (a) A Noetherian space is quasi-compact.

   (b) If A is a Noetherian ring, then $\operatorname{spec}(A)$ is Noetherian. Is the converse also true?

   Solution:

   (a) Let $\bigcup_{i \in I} V_i = X$ be an open covering of X. Without loss of generality we can assume $I = \mathbb{N}$. For $n \in \mathbb{N}$ define
   $$U_n := \bigcup_{i \leqslant n} V_i.$$
   We see that $U_n \subset U_{n+1}$ for all $n \in \mathbb{N}$. Since X is Noetherian, we conclude that there is an integer $N \geqslant 0$ such that $U_i = U_{i+1}$ for all $i \geqslant N$, which implies that $U_N = \bigcup_{i \leqslant N} V_i = \bigcup_{i \in \mathbb{N}} V_i = X$. Hence there is a finite subcover and this proves that X is quasi-compact.

   (b) We will use exercise 6 from exercise sheet 1. Let $(U_i)_{i \in \mathbb{N}}$ be an ascending chain of open subsets of $\operatorname{spec}(R)$. For every $i \in \mathbb{N}$ let $I_i \subset R$ be an ideal such that $\operatorname{spec}(R) \smallsetminus V(I_i) = U_i$. We conclude that $V(I_i) \supset V(I_{i+1})$ for all $i \in \mathbb{N}$. Therefore $I(V(I_i)) \subset I(V(I_{i+1}))$ for all $i \in \mathbb{N}$. Since R is Noetherian we conclude that the chain of ideals $I(V(I_i))$ becomes stationary and thus the chain $V(I(V(I_i))) = V(I_i)$ becomes stationary. This implies that the chain U_i becomes stationary.

   The converse is not true. Consider the ring $A := k[X_1, X_2, \dots]/(X_1^2, X_2^2, \dots)$ for a field k, i.e. the quotient of the polynomial ring in infinitely many variables modulo the ideal generated by all squares of variables. Let $\mathfrak{p} \subset A$ be prime ideal. Then the ideal $(X_1, X_2, \dots)$ is contained in $\mathfrak{p}$. But the ideal $(X_1, X_2, \dots)$ is already maximal. Hence $\operatorname{spec}(A)$ is only one point and trivially Noetherian as topological space. On the other hand, the ideals $I_n := (X_1, \dots, X_n)$ for $n \in \mathbb{N}$ form a strictly ascending chain in A, which proves that A is not Noetherian.

Solutions Sheet 6

Primary Decomposition & k-Algebras

Definition: Let A be a ring and $\mathfrak{a} \subset A$ an ideal which admits a primary decomposition. Let P be the set of associated prime ideals of $\mathfrak{a}$. The minimal elements of P with respect to inclusion are called *isolated prime ideals* of $\mathfrak{a}$, the others are called *embedded prime ideals*.

1. The power of a maximal ideal is a primary ideal. Show that the converse is not true: find an example of a ring A and a primary ideal $\mathfrak{a} \subset A$ such that its radical $r(\mathfrak{a})$ is a maximal ideal, but $\mathfrak{a}$ is not a power of $r(\mathfrak{a})$.

   Solution: Consider the ring $A := \mathbb{Z}[X]$. We have the maximal ideal $\mathfrak{m} := (2, X)$ and the ideal $\mathfrak{a} := (4, X)$. Since $r(\mathfrak{a}) = \mathfrak{m}$ we know that $\mathfrak{a}$ is $\mathfrak{m}$-primary. However $\mathfrak{a} \not\subset \mathfrak{m}^2 = (4, X^2, 2X)$, so $\mathfrak{a}$ cannot be a power of $\mathfrak{m}$.

2. Let k be a field. Consider the polynomial ring $A := k[X, Y, Z]$ and the ideal $\mathfrak{a} := (X^2, XY, YZ, XZ) \subset A$. Find a minimal primary decomposition of $\mathfrak{a}$ and the associated prime ideals. Which components are isolated and which are embedded?

   Solution: We claim that $\mathfrak{a} = (X, Y) \cap (X, Z) \cap (X^2, Y^2, Z^2, XY, XZ, YZ) =: \mathfrak{b}$. Clearly $\mathfrak{a} \subset \mathfrak{b}$. On the other hand, let $f \in \mathfrak{b}$. Then we can write

$$f = a_1X^2 + a_2Y^2 + a_3Z^2 + a_4XY + a_5XZ + a_6YZ$$

   for some $a_1, \ldots, a_6 \in A$. We see that $f \in \mathfrak{a}$ if and only if $a_2Y^2 + a_3Z^2 \in \mathfrak{a}$. Since $f \in (X, Z)$ we conclude that $a_2Y^2 \in (X, Z)$, so $a_2Y^2 \in (XY, ZY) \subset \mathfrak{a}$. Similarly we know that $f \in (X, Y)$ and thus $a_3Z^2 \in (XZ, YZ) \subset \mathfrak{a}$. Therefore $f \in \mathfrak{a}$ and hence $\mathfrak{a} = \mathfrak{b}$. Note that (X, Y) and (X, Z) are prime ideals and thus in particular primary. Furthermore, the ideal $(X^2, Y^2, Z^2, XY, XZ, YZ)$ is equal to $(X, Y, Z)^2$ and as power of a maximal ideal it is also primary. Thus we have found a primary decomposition of $\mathfrak{a}$ and we see that it is a minimal one:

$$\begin{aligned} X &\in (X, Y) \cap (X, Z), \text{ but } X \notin \mathfrak{a} \\ Y^2 &\in (X, Y) \cap (X, Y, Z)^2, \text{ but } Y^2 \notin \mathfrak{a} \\ Z^2 &\in (X, Z) \cap (X, Y, Z)^2, \text{ but } Z^2 \notin \mathfrak{a} \end{aligned}$$

   The associated prime ideals are $(X, Y), (X, Z), (X, Y, Z)$. The ideals $(X, Y), (X, Z)$ are isolated primes and (X, Y, Z) is embedded.

3. Let k be a field and A a finitely generated k-algebra. Prove the following statement: An ideal $\mathfrak{a} \subset A$ is a maximal ideal if and only if $\mathfrak{a}$ is prime and the quotient $A/\mathfrak{a}$ is a finite dimensional k-vector space.

   Solution: Assume that $\mathfrak{a}$ is maximal. Then in particular it is a prime ideal. Furthermore, using the weak version of Hilbert's Nullstellensatz we conclude that $A/\mathfrak{m}$ is a finite field extension of k and thus finite dimensional over k. Conversely assume that $\mathfrak{a}$ is prime and $A/\mathfrak{a}$ is a finite dimensional k-vector space. Thus $A/\mathfrak{a}$ is an integral domain. Take a non-zero element $f \in A/\mathfrak{a}$. The multiplication by f gives a k-linear map

$$\begin{aligned} A/\mathfrak{a} &\to A/\mathfrak{a} \\ g &\mapsto fg \end{aligned}$$

   Since $A/\mathfrak{a}$ is an integral domain, this map is injective. Because of the finite dimensionality as k-vector space it is thus also surjective. We conclude that there is an element $g \in A/\mathfrak{a}$ such that $fg = 1$, hence $A/\mathfrak{a}$ is a field which proves that $\mathfrak{a}$ is a maximal ideal.

4. Let k be a field and A a finitely generated k-algebra. Let $\mathfrak{a} \subset A$ be a radical ideal. Using the previous exercise, prove that the associated prime ideals of $\mathfrak{a}$ are all maximal if and only if $A/\mathfrak{a}$ is a finite dimensional k-vector space.

   Solution: Since k is a field and A a finitely generated k-algebra we know that A is Noetherian, so primary decomposition exists.

   Assume that $A/\mathfrak{a}$ is finite dimensional as k-vector space. Using the previous exercise we conclude that every prime ideal in $A/\mathfrak{a}$ is maximal. Using the 1-to-1 correspondence of ideals in $A/\mathfrak{a}$ and ideals in A containing $\mathfrak{a}$ we conclude that every associated prime ideal of $\mathfrak{a}$ is maximal.

   Conversely assume that every associated prime ideal of $\mathfrak{a}$ is maximal. Since $\mathfrak{a}$ is radical we have $r(\mathfrak{a}) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ for distinct maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n \subset A$. For all $1 \leqslant k \leqslant n$ consider the short exact sequence of k-vector spaces:

$$\mathfrak{m}_k/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k) \hookrightarrow A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k) \twoheadrightarrow A/\mathfrak{m}_k$$

   Using the isomorphism theorem from algebra, we deduce that

$$\mathfrak{m}_k/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k) \cong (\mathfrak{m}_k + \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{k-1})/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{k-1}) = A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{k-1})$$

   where the last equality follows from the fact that the maximal ideals are distinct and the proposition from the lecture stating that if a prime ideal contains an intersection of ideals, it contains at least one of the ideals. We know from the previous exercise that $A/\mathfrak{m}_1$ is a finite dimensional k-vector space. Using induction, the above short exact sequence and the fact that if the left hand side and the right hand side of the short exact sequence are both finite dimensional, then so is the middle term, we deduce that $A/\mathfrak{a}$ is a finite dimensional k-vector space.

5. For $k := \mathbb{C}$, explain the geometry behind exercise 2.

   Solution: We look at $V(\mathfrak{a}) \subset \mathbb{C}^3$. By definition, this is the set of $x \in \mathbb{C}^3$ such that $\forall f \in \mathfrak{a}$ we have $f(x) = 0$. It is enough to check that condition on the generators. Hence $x \in V(\mathfrak{a})$ if and only if $X = 0$ and $YZ = 0$. We conclude that $V(\mathfrak{a})$ is in fact the union of the Y-axis (when $X, Z = 0$) and the Z-axis (when $X, Y = 0$). Those are two irreducible components of $V(\mathfrak{a})$. The Y-axis corresponds to the prime ideal (X, Z) and the Z-axis corresponds to the ideal (X, Y). Thus we recovered the isolated prime ideals of $\mathfrak{a}$.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 7

Primary Decomposition, Artinian Rings and Modules

Definition: Let A be a ring and $\mathfrak{p} \subset A$ a prime ideal of A. Denote $\varphi : A \to A_{\mathfrak{p}}$ for the localisation map. For an integer $n > 0$ we define the *n-th symbolic power of* $\mathfrak{p}$ to be the ideal $\mathfrak{p}^{(n)} := \varphi^* \varphi_*(\mathfrak{p}^n)$.

1. Let A be a ring and $\mathfrak{p} \subset A$ a prime ideal. Let $n > 0$ be an integer. Consider the n-th symbolic power $\mathfrak{p}^{(n)}$. Prove:

   (a) $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal.

   (b) If $\mathfrak{p}^n$ has a primary decomposition, then $\mathfrak{p}^{(n)}$ is its $\mathfrak{p}$-primary component.

   (c) $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ if and only if $\mathfrak{p}^n$ is a primary ideal.

   Solution:

   (a) Since $\varphi_*(\mathfrak{p})$ is a maximal ideal in $A_{\mathfrak{p}}$ we know that $\varphi_*(\mathfrak{p})^n$ is a $\varphi_*(\mathfrak{p})$-primary ideal. But $\varphi_*(\mathfrak{p})^n = \varphi_*(\mathfrak{p}^n)$ (see solutions of exercise 1, sheet 2) and since the contraction of a primary ideal is primary, we conclude that $\mathfrak{p}^{(n)}$ is a primary ideal.

   (b) Let $\mathfrak{p}^n = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition and set $\mathfrak{p}_i := r(\mathfrak{q}_i)$ for all $1 \leqslant i \leqslant n$. Since $r(\mathfrak{p}^n) = \mathfrak{p}$ we conclude that $\mathfrak{p}$ is a minimal prime ideal associated to $\mathfrak{p}^n$, and it is in fact the only one. Without loss of generality assume that $\mathfrak{q}_1$ is the $\mathfrak{p}$-primary component of the decomposition. Since $\mathfrak{p}^n \subset \mathfrak{p}^{(n)}$ we see that we can exchange $\mathfrak{q}_1$ in the decomposition by $\mathfrak{q}_1 \cap \mathfrak{p}^{(n)}$, which is still a $\mathfrak{p}$-primary ideal by a Lemma from the lecture. By the second uniqueness theorem we thus conclude that $\mathfrak{q}_1 = \mathfrak{q}_1 \cap \mathfrak{p}^{(n)}$ and so $\mathfrak{q}_1 \subset \mathfrak{p}^{(n)}$. On the other hand $\mathfrak{p}^n \subset \mathfrak{q}_1$ and so $\mathfrak{p}^{(n)} \subset \varphi^*\varphi_*(\mathfrak{q}_1)$. But by a Proposition we have the equality $\varphi^*\varphi_*(\mathfrak{q}_1) = \mathfrak{q}_1$. This concludes the proof.

   (c) If $\mathfrak{p}^{(n)} = \mathfrak{p}^n$, then by (a) the ideal $\mathfrak{p}^n$ is primary. Conversely, if $\mathfrak{p}^n$ is primary, then it has itself as trivial primary decomposition. Using (b) we conclude that $\mathfrak{p}^{(n)} = \mathfrak{p}^n$.

2. Let k be a field and consider the ring $A := k[X, Y, Z]$. Compute the ideal of A given by

$$\mathfrak{a} := (Y^2 + XY - XZ - YZ, (X + Y)^2 + 2X) \cap ((X + Y)^2, X, Y^3 - Y^2 Z)$$

   and find a minimal primary decomposition of $\mathfrak{a}$.

   (*Hint:* Substitutions might be helpful.)

Solution: We substitute $U := X + Y$ and $V := Y - Z$ and use the fact that we can change one generator by a multiple of another one, thus finding:

$$\begin{aligned}\mathfrak{a} &= (UV, U^2 + 2X) \cap (U^2, X, Y^2V) \\ &= (UV, U^2 + 2X) \cap (U^2, X, U^2V - X^2V - 2XYV) \\ &= (UV, U^2 + 2X) \cap (U^2, X)\end{aligned}$$

Substituting $W := U^2 + 2X$ we get:

$$\mathfrak{a} = (UV, W) \cap (U^2, W)$$

Now we see that $\mathfrak{a} = (U^2V, W)$. We have the decomposition

$$\mathfrak{a} = (U^2, W) \cap (V, W)$$

which is in fact a minimal primary decomposition, as both (U^2, W) and (V, W) are primary ideals with different radicals. Substituting back and doing a bit of cosmetics, we get the primary decomposition:

$$\mathfrak{a} = (Y^2, X) \cap (Y - Z, (X + Y)^2 + 2X).$$

3. Let A be a ring and $\mathfrak{a} \subset A$ an ideal which admits a primary decomposition. Let $\mathfrak{p}$ be a maximal element of the set $\{(\mathfrak{a} : x) \mid x \in A \smallsetminus \mathfrak{a}\}$. Prove that $\mathfrak{p}$ is an associated prime ideal of $\mathfrak{a}$.

   Solution: By the first uniqueness theorem, we know that every prime ideal of the form $(\mathfrak{a} : x)$ for some $x \in A$ is an associated prime ideal. Thus we only need to proof that $\mathfrak{p}$ is indeed a prime ideal. Let $x \in A \smallsetminus \mathfrak{a}$ such that $\mathfrak{p} = (\mathfrak{a} : x)$. Let $f, g \in A$ such that $fg \in \mathfrak{p}$. Then $fgx \in \mathfrak{a}$ and we see that $\mathfrak{p} \subset (\mathfrak{a} : gx)$. If $\mathfrak{p} = (\mathfrak{a} : gx)$, then $f \in \mathfrak{p}$. If not, then by maximality of $\mathfrak{p}$ we conclude that $gx \in \mathfrak{a}$. But this implies that $g \in \mathfrak{p}$. Hence $\mathfrak{p}$ is a prime ideal.

4. Let A be a ring and M an Artinian A-module. Let $f : M \to M$ be an injective module homomorphism. Prove that f is an isomorphism.

   Solution: Consider the descending chain of submodules $I_n := \mathrm{im}(f^n)$ for $n > 0$. Since M is Artinian, we conclude that there exists an integer $N > 0$ such that for all $n \geqslant N$ we have $I_n = I_{n+1}$. Let $a \in M$. We conclude that there is an element $b \in M$ such that $f^{n+1}(b) = f^n(a)$. Hence we have $f^n(f(b) - a) = 0$. Since f is injective, so is f^n and thus $f(b) = a$, proving that f is surjective. We conclude that f is an isomorphism.

5. Let A be a ring and M a Noetherian A-module. Let $\mathfrak{a} \subset A$ be the annihilator of M, i.e. $\mathfrak{a} = \{x \in A \mid xM = 0\}$. Prove that the ring $A/\mathfrak{a}$ is Noetherian.

   Is the same true if we replaced Noetherian with Artinian?

Solution: Since M is Noetherian, it is finitely generated by, say, the elements $m_1 \dots, m_n$. Consider the homomorphism

$$\begin{aligned} \varphi : A &\to M^n \\ a &\mapsto (am_1, \dots, am_n) \end{aligned}$$

The kernel of φ is precisely the annihilator $\mathfrak{a}$. Thus $A/\mathfrak{a}$ can be identified with a submodule of M^n. But since M is Noetherian, so is M^n and so is every submodule of M^n. We conclude that $A/\mathfrak{a}$ is Noetherian as an A-module. Hence it is Noetherian as a ring.

If we replaced Noetherian with Artinian, the statement becomes wrong. Consider $M := \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ as a $\mathbb{Z}$-module by multiplication. Clearly the annihilator $\mathfrak{a}$ is zero, as no integer is divisible by every power of p. On the other hand M is Artinian: Let $\frac{a}{p^n} \in M$ with a and p^n coprime. By the Lemma of Bézout we conclude that there are $u, v \in \mathbb{Z}$ such that $ua - vp^n = 1$. But then $\frac{ua}{p^n} = \frac{1}{p^n} + v$, which shows that $\frac{ua}{p^n} \equiv \frac{1}{p^n}$ in M. Hence every descending chain of submodules is of the form $\left\langle \frac{1}{p^n} \right\rangle \supset \left\langle \frac{1}{p^k} \right\rangle \supset \dots$ with $k \leqslant n$. We conclude that M is Artinian. This provides a counter example, as $\mathbb{Z} = \mathbb{Z}/\mathfrak{a}$ is not Artinian.

Solutions Sheet 8

Artinian Rings and Modules, Krull Intersection Theorem

1. Let k be a field and A a finitely generated k-algebra. Prove that the following are equivalent:

   (a) A is an Artinian ring.

   (b) A is a finite dimensional k-vector space.

   Solution: "(a)$\Rightarrow$(b)": If A is Artinian, then it is isomorphic to a product $A \cong \prod_{i=1}^{n} A_i$ of local Artinian rings A_i by the classification theorem. So without loss of generality we assume that A is a local Artinian ring with maximal ideal $\mathfrak{m} \subset A$. By Hilbert's Nullstellensatz we know that $L := A/\mathfrak{m}$ is a finite field extension of k. From one Proposition we know that $\mathfrak{m}^n = 0$ for some integer $n > 0$. For every $1 \leqslant i \leqslant n$ we have $L \otimes_A \mathfrak{m}^i \cong \mathfrak{m}^i/\mathfrak{m}^{i+1}$. Since A is also Noetherian, $\mathfrak{m}^i$ is finitely generated as A-module and thus $L \otimes_A \mathfrak{m}$ is finitely generated as L-vector space and hence also as k-vector space. For $1 \leqslant i \leqslant n$ we have the exact sequences

   $$\mathfrak{m}^i/\mathfrak{m}^{i+1} \to A/\mathfrak{m}^{i+1} \to A/\mathfrak{m}^i$$

   where the left term is a finite dimensional k-vector space. For $i = 1$, the right hand side is L and thus also finite dimensional as k-vector space, so the middle term $A/\mathfrak{m}^2$ is finite dimensional as k-vector space. By induction and the fact that $\mathfrak{m}^n = 0$ we conclude that $A/\mathfrak{m}^n = A$ is finite dimension as k-vector space.

   "(b)$\Rightarrow$(a)": If A is a finite dimensional k-vector space, then it is Artinian as k-vector space. But every ideal of A is a k-vector space and thus they satisfy the descending chain condition, which proves that A is Artinian as ring.

2. Let A be a Noetherian ring. Prove the equivalence of the following statements:

   (a) A is an Artinian ring.

   (b) $\operatorname{spec}(A)$ is discrete and finite.

   (c) $\operatorname{spec}(A)$ is discrete.

   Solution: "(a)$\Rightarrow$(b)": If A is Artinian, we know that every prime ideal is maximal. Hence every point of $\operatorname{spec}(A)$ is closed. We also know, that there are only finitely many distinct maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ of A. Hence $\operatorname{spec}(A)$ is finite. Furthermore $\operatorname{spec}(A) \smallsetminus V(\bigcap_{i \neq k} \mathfrak{m}_i) = \mathfrak{m}_k$ and thus every point is also closed. We conclude that $\operatorname{spec}(A)$ is a discrete finite space.

"(b)⇒(c)": Immediate.

"(c)⇒(a)": We show that $\dim(A) = 0$. Assume otherwise. Then there are two prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subset A$ such that $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq A$. But then $\mathfrak{p}_1 \in \operatorname{spec}(A)$ is not a closed point, since its closure contains $\mathfrak{p}_2$. A contradiction to $\operatorname{spec}(A)$ being discrete. Since A is Noetherian of dimension 0 we conclude that A is Artinian.

3. Let R be the ring of germs at 0 of C^∞-functions on $\mathbb{R}$ and let $\mathfrak{m} = (x)$ denote the ideal generated by the coordinate function x. It is the unique maximal ideal of R. Show by elementary calculus that if f is a C^∞-function such that all its derivatives vanish at the origin, then f/x is also such a function. Conclude that $\mathfrak{m}\left(\bigcap_{j\geqslant 1} \mathfrak{m}^j\right) = \bigcap_{j\geqslant 1} \mathfrak{m}^j$. Moreover, recall that the intersection $\bigcap_{j\geqslant 1} \mathfrak{m}^j$ is non-zero. It contains for instance the function $e^{-\frac{1}{x^2}}$. This example therefore shows that the finiteness conditions are necessary in both Nakayama's Lemma and Krull's Intersection Theorem.

   Solution (sketch): We only sketch the proof, which is purely analytic. Firstly, one can show by induction on k and using Bernoulli de l'Hopital that for any such f and any $k \geqslant 0$ the first derivative of f/x^k at 0 exists and equals 0. Secondly, one can show that the same is true for any j-th derivative, where $j \geqslant 1$, which can be done by induction on j using the first part. This implies $f/x \in \mathfrak{m}^j$ for any $j \geqslant 1$ and consequently $f \in \mathfrak{m}(\bigcap\limits_{j\geqslant 1} \mathfrak{m}^j)$. As all of the derivatives at 0 of any $f \in \bigcap\limits_{j\geqslant 1} \mathfrak{m}^j$ vanish, we deduce $\bigcap\limits_{j\geqslant 1} \mathfrak{m}^j \subset \mathfrak{m}(\bigcap\limits_{j\geqslant 1} \mathfrak{m}^j)$.

4. Consider the monoid ring $R := K[\mathbb{Q}^{\geqslant 0}] = K[\{X^\alpha \mid \alpha \in \mathbb{Q}^{\geqslant 0}\}]$ over a field K.

   (a) Find a maximal ideal $\mathfrak{m} \neq 0$ of R such that $\mathfrak{m}^n = \mathfrak{m}$ for all $n \geqslant 1$.

   (b) Use R to construct a ring $\bar{R}$ with $r(0)^n \neq 0$ for all $n \geqslant 1$.

   Solution: (a) Let $\mathfrak{m}$ be the ideal generated by the elements X^α for all $\alpha \in \mathbb{Q}^{>0}$. It is maximal, because the factor ring is isomorphic to K. Since $X^\alpha = (X^{\alpha/n})^n \in \mathfrak{m}^n$ for each $n \geqslant 1$, we have $\mathfrak{m}^n = \mathfrak{m}$.

   (c) For any rational number $\alpha > 0$ with denominator n we have $(X^\alpha)^n \in (X)$. Thus for $\bar{R} := R/(X)$ we have $r(0) = \mathfrak{m}/(X)$. From (a) it follows that $r(0)^n = r(0) \neq 0$ for all $n \geqslant 1$.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 9

Dimension and Height

1. Let A be a ring. Prove the following statements:

   (a) For every prime ideal $\mathfrak{p} \subset A$ we have $\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \leqslant \dim(A)$.

   (b) For every ideal $\mathfrak{a} \subset A$ we have $\mathrm{ht}(\mathfrak{a}) + \mathrm{coht}(\mathfrak{a}) \leqslant \dim(A)$.
   (Recall that $\mathrm{ht}(\mathfrak{a}) = \inf\limits_{\mathfrak{p} \supset \mathfrak{a} \text{ prime}} \mathrm{ht}(\mathfrak{p})$)

   Solution:

   (a) Let $\varphi : A \to A_{\mathfrak{p}}$ and $\psi : A \to A/\mathfrak{p}$ be the canonical homomorphisms. By definition we have $\mathrm{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$ and $\mathrm{coht}(\mathfrak{p}) = \dim(A/\mathfrak{p})$. For all chains of prime ideals $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ in $A_{\mathfrak{p}}$ and $\mathfrak{p} = \mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_r$ in $A/\mathfrak{p}$ we have the chain $\varphi^*(\mathfrak{p}_0) \subsetneq \cdots \subsetneq \varphi^*(\mathfrak{p}_n) = \psi^*(\mathfrak{q}_0) \subsetneq \cdots \subsetneq \psi^*(\mathfrak{q}_r)$ of prime ideals of A. The length of this chain is thus $n + r \leqslant \dim(A)$. Taking the supremum over all such pairs of chains yields the result.

   (b) Let $\mathfrak{p} \subset A$ be a prime ideal. Then by definition of $\mathrm{ht}(\mathfrak{a})$ and (a) above we have
   $$\mathrm{ht}(\mathfrak{a}) + \mathrm{coht}(\mathfrak{p}) \leqslant \mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \leqslant \dim(A)$$
   Taking the supremum of the left hand side over all prime ideals $\mathfrak{p}$ which contain $\mathfrak{a}$ yields the result:
   $$\mathrm{ht}(\mathfrak{a}) + \mathrm{coht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{a}) + \sup_{\mathfrak{p} \supset \mathfrak{a} \text{ prime}} \mathrm{coht}(\mathfrak{p}) \leqslant \dim(A)$$

2. Give an example of a

   (a) non-Noetherian local ring A with maximal ideal $\mathfrak{m}$ and $\dim A > \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

   (b) Noetherian non-local ring A with a maximal ideal $\mathfrak{m}$ such that $\dim A > \mathrm{ht}(\mathfrak{m})$.

   Solution: Let k be a field.

   (a) The localisation A of the ring $k[X^\alpha|_{\alpha \in \mathbb{Q}^{>0}}]$ at the prime ideal $(X^\alpha|_{\alpha \in \mathbb{Q}^{>0}})$ satisfies $\dim(A) = 1 > 0 = \dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

   (b) Since the dimension of a ring is the supremum of the heights of maximal ideals it is enough to find a ring with two maximal ideals of different heights. Exercise 4 gives an example.

3. Let A be a ring and consider the polynomial ring in one variable $A[X]$. Let $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subset A[X]$ be two prime ideals such that their contraction to A is equal $\mathfrak{p} := \mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A$. Prove that $\mathfrak{p}_1 = \mathfrak{p}A[X]$. Deduce that for any three subsequent prime ideals $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3 \subset A[X]$ their contractions $\mathfrak{p}_1 \cap A, \mathfrak{p}_2 \cap A, \mathfrak{p}_3 \cap A$ cannot all be equal.

   [Hint: Take a ring of fractions and use that $\dim(K[X]) = 1$ for every field K]

   Solution: Since $\mathfrak{p}_1$ is an ideal we have $\mathfrak{p}A[X] \subset \mathfrak{p}_1$. We localise $A[X]$ at the multiplicative set $S := A \setminus \mathfrak{p}$ and get $S^{-1}A[X] = A_{\mathfrak{p}}[X]$ and the two prime ideals $S^{-1}\mathfrak{p}_1 \subsetneq S^{-1}\mathfrak{p}_2$ with contractions $S^{-1}\mathfrak{p}_1 \cap A_{\mathfrak{p}} = S^{-1}\mathfrak{p}_2 \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Now consider the quotient $R := A_{\mathfrak{p}}[X]/\mathfrak{p}A_{\mathfrak{p}}[X] \cong (A_{\mathfrak{p}}/p)[X]$. Since $A_{\mathfrak{p}}/\mathfrak{p}$ is a field we know that the dimension of R is equal to 1. We conclude that therefore the image of $S^{-1}\mathfrak{p}_1$ in R is the zero ideal (because it cannot be equal to the image of $S^{-1}\mathfrak{p}_2$) and thus $S^{-1}\mathfrak{p}_1 = \mathfrak{p}A_{\mathfrak{p}}[X]$. By the correspondence of ring of fractions we conclude that $\mathfrak{p}_1 = \mathfrak{p}A[X]$.

   Assume we have three subsequent prime ideals $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \mathfrak{p}_3 \subset A[X]$ such that all of their contractions to A are equal to the prime ideal $\mathfrak{p} \subset A$. By using the previous proof twice we conclude that $\mathfrak{p}_2 = \mathfrak{p}A[X] = \mathfrak{p}_1$ which is a contradiction.

4. Consider the ring $R := \mathbb{C}[X, Y, Z]/(XY, XZ)$. Compute the height of the two maximal ideals $\mathfrak{m}_1 := (X - 1, Y, Z) \subset R$ and $\mathfrak{m}_2 := (X, Y - 1, Z) \subset R$. Interpret your result geometrically on the variety $V(XY, XZ) \subset \mathbb{C}^3$.

   Solution: Note that the ideals are maximal by the correspondence of ideals in R and ideals in $\mathbb{C}[X, Y, Z]$ containing (XY, XZ). Furthermore note that $(XY, XZ) = (X) \cap (Y, Z)$ in the ring $\mathbb{C}[X, Y, Z]$ and thus every prime ideal of R corresponds to a prime ideal in $\mathbb{C}[X, Y, Z]$ containing (X) or (Y, Z).

   We have the chain of prime ideals $\mathfrak{m}_1 = (X - 1, Y, Z) \supsetneq (Y, Z)$. Every prime ideal $\mathfrak{p} \subset \mathfrak{m}_1$ must contain (Y, Z) because $X \notin \mathfrak{m}_1$. Furthermore, there is no prime ideal in between $\mathfrak{m}_1$ and (Y, Z), since every $f \in \mathfrak{m}_1 \setminus (Y, Z)$ must be divisible by $(X - 1)$, say $f = a(X - 1)$ for some $a \in R \setminus (Y, Z)$. If $(X - 1)$ is contained in the ideal, then we are done, if not, then $a \in \mathfrak{m}_1$ and we can use induction on the degree. Hence the chain is maximal and we conclude that $\mathrm{ht}(\mathfrak{m}_1) = 1$.

   Consider the chain of prime ideals $\mathfrak{m}_2 = (X, Y - 1, Z) \supsetneq (X, Z) \supsetneq (X)$. We conclude that $\mathrm{ht}(\mathfrak{m}_2) \geqslant 2$. Since $Y \notin \mathfrak{m}_2$ we conclude that every prime ideal of R contained in $\mathfrak{m}_2$ corresponds to a prime ideal in $\mathbb{C}[X, Y, Z]$ which contains X. Thus $\mathrm{ht}(\mathfrak{m}_2) \leqslant \dim(R/(X)) = \dim(\mathbb{C}[Y, Z]) = 2$. Hence $\mathrm{ht}(\mathfrak{m}_2) = 2$.

   For the geometric interpretation note that $V(XZ, YZ)$ is the union of the X-axis and the YZ-plane in $\mathbb{C}^3$. The point which corresponds to $\mathfrak{m}_1$ is a point on the X-axis and thus there is only one irreducible subspace which contains that point, namely the X-axis itself which corresponds to the ideal (Y, Z). On the other hand, the point which corresponds to $\mathfrak{m}_2$ lies on the YZ-plane and more precisely on the Y-axis. Thus there is the irreducible variety of the Y-axis (corresponding to the ideal (X, Z) and the irreducible variety of the YZ-plane (corresponding to the ideal (X)) which contains the Y.axis and thus the point. This also shows geometrically the results $\mathrm{ht}(\mathfrak{m}_1) = 1$ and $\mathrm{ht}(\mathfrak{m}_2) = 2$.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 10

Krull Dimension

1. We have seen that for a Noetherian ring A we have $\dim(A[X]) = \dim(A) + 1$. Let now A be a ring, which is not necessarily Noetherian. Use Exercise 3 of sheet 9 to prove the inequality

$$\dim(A) + 1 \leqslant \dim(A[X]) \leqslant 2\dim(A) + 1.$$

Solution: Let $n := \dim(A)$. For every prime ideal $\mathfrak{p} \subset A$ the ideal $\mathfrak{p}[X] = \mathfrak{p} \cdot A[X]$ is a prime ideal in $A[X]$, since $A[X]/\mathfrak{p}[X] \cong (A/\mathfrak{p})[X]$ is an integral domain. Its contraction to A is again $\mathfrak{p}$, i.e. $\mathfrak{p}[X] \cap A = \mathfrak{p}$. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of prime ideals in A. The previous arguments show that then $\mathfrak{p}_0[X] \subsetneq \cdots \subsetneq \mathfrak{p}_n[X]$ is a chain of prime ideals in $A[X]$. However, we have the strict inclusions $\mathfrak{p}_n[X] \subsetneq \mathfrak{p}_n[X] + (X) \subsetneq A[X]$, so $\mathfrak{p}_n[X]$ is not a maximal ideal. This proves that $\dim(A) + 1 \leqslant \dim(A[X])$.

Conversely let $s := \dim(A[X])$ and let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_s$ be a chain of prime ideals in $A[X]$. By contraction to A we get a chain of prime ideals $\mathfrak{p}_0 \cap A \subseteq \cdots \subseteq \mathfrak{p}_s \cap A$ in A, with not necessarily strict inclusions. Assume that there are m distinct contractions. By exercise 3 of sheet 9 we know that at least two contractions out of three subsequent prime ideals must differ. This shows $s+1 \leqslant 2m \leqslant 2(\dim(A)+1)$ and hence $s \leqslant 2\dim(A) + 1$.

2. Let A be a Noetherian ring. Prove that $\dim(A[X, X^{-1}]) = \dim(A) + 1$.

Solution: Since A is Noetherian, we know that $\dim(A[X]) = \dim(A) + 1$. Prime ideals in $A[X, X^{-1}]$ correspond to prime ideals in $A[X]$ which do not contain X. Hence $\dim(A[X, X^{-1}]) \leqslant \dim(A[X]) = \dim(A) + 1$. Conversely, a prime ideal $\mathfrak{p}$ in A gives rise to a prime ideal $\mathfrak{p}[X, X^{-1}]$ in $A[X, X^{-1}]$ with contraction $\mathfrak{p}[X, X^{-1}] \cap A = \mathfrak{p}$. However, $\mathfrak{p}[X, X^{-1}]$ is not maximal, because $A[X, X^{-1}]/\mathfrak{p}[X, X^{-1}] \cong (A/\mathfrak{p})[X, X^{-1}]$ is not a field. Hence $\dim(A[X, X^{-1}]) \geqslant \dim(A) + 1$.

3. Let k be a field. Consider the ring $A := k[X, Y, W, Z]/(XW - YZ)$ and its quotient ring $B := A/(X, Y) \cong k[W, Z]$. Define the prime ideal $\mathfrak{p} := (W, Z) \subset A$ and denote by $\mathfrak{q} \subset B$ its image in B, which is again a prime ideal. What is $\dim(A)$? Prove that $\mathrm{ht}(\mathfrak{p}) = 1$, but $\mathrm{ht}(\mathfrak{q}) = 2$.

Solution: By Krull's principal ideal theorem, we conclude that $(XW - YZ)$ has height 1 in $k[X, Y, W, Z]$. Since $\dim(A)$ is its coheight, we have $1 + \dim(A) \leqslant \dim(k[X, Y, W, Z]) = 4$. Hence $\dim(A) \leqslant 3$. On the other hand, there is the chain of prime ideals $(XW - YZ) \subsetneq (X,Y) \subsetneq (X,Y,W) \subsetneq (X,Y,W,Z)$. Thus $\dim(A) \geqslant 3$ and we obtain equality.

Note that $A/\mathfrak{p} \cong k[X,Y]$. Hence $\mathrm{ht}(\mathfrak{p}) + 2 \leqslant \dim(A) = 3$, which implies $\mathrm{ht}(\mathfrak{p}) \leqslant 1$. Since A is an integral domain and $\mathfrak{p}$ is non-zero in A we conclude that $\mathrm{ht}(\mathfrak{p}) \geqslant 1$ and thus we obtain equality.

Note that $\mathfrak{q}$ is the maximal ideal (W,Z) in B and $\dim(B) = 2$. Since $(0) \subsetneq (W) \subsetneq \mathfrak{q}$ is a chain of prime ideals in B we conclude that $2 \leqslant \mathrm{ht}(\mathfrak{q}) \leqslant \dim(B) = 2$.

4. Give an example of a zero-dimensional ring, which is not Noetherian.

   Solution: Let k be a field and let $A := \prod_{i\in\mathbb{N}} k$ be an infinite product of k. The ideals $I_n := k^n \times \prod_{i>n}\{0\} \subset A$ are a strictly increasing chain of ideals, so A is not Noetherian. On the other hand, the proof of exercise 2 of sheet 5 shows that every localisation of A at a prime ideal is a field. Thus every prime ideal has height 0, which proves that $\dim(A) = 0$.

5. Let k be a field and $A := k[X_1, X_2, \ldots]$ be the polynomial ring with countably many variables. For $i \geqslant 0$ define the prime ideals $\mathfrak{p}_i := (X_{2^i}, \ldots, X_{2^{i+1}-1})$ in A. Define the multiplicative set $S := A \smallsetminus \bigcup_{i=0}^{\infty} \mathfrak{p}_i$ and the ring $B := S^{-1}A$. Show that B has infinite dimension. Prove that B is Noetherian using the lemma below.

   Lemma: *Let A be a ring such that every localisation $A_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m} \subset A$ is Noetherian, and every non-zero element $x \in A$ is contained in only finitely many maximal ideals. Then A is Noetherian.*

   Solution: Note that $k(X_k, k \notin [2^i, 2^{i+1}-1])[X_{2^i}, \ldots, X_{2^{i+1}-1}]_{\mathfrak{p}_i} \cong A_{\mathfrak{p}_i} \cong B_{S^{-1}\mathfrak{p}_i}$ and so we have $\mathrm{ht}(S^{-1}\mathfrak{p}_i) = 2^i$ and hence $\dim(B) = \infty$.

   We prove that all $S^{-1}\mathfrak{p}_i$ are maximal ideals in B. Let $\alpha \in B \smallsetminus S^{-1}\mathfrak{p}_i$. After clearing denominators we assume that $\alpha \in A \smallsetminus \mathfrak{p}_i$. After removing all monomials of α which contain X_{2^i} we see that $\alpha + X_{2^i} \in S$ and hence is a unit in B. This proves that $S^{-1}\mathfrak{p}_i$ is a maximal ideal in B.

   Next we prove that the $S^{-1}\mathfrak{p}_i$ are the only maximal ideals. Let $\mathfrak{p} \subset B$ be a prime ideal. Thus its contraction to A is contained in $\bigcup_{i=0}^{\infty} \mathfrak{p}_i$. Choose a non-constant element $a \in \mathfrak{p} \cap A$. Consider the set $M := (\mathfrak{p} \cap A) \smallsetminus \bigcup_{i=0}^{n} \mathfrak{p}_i$, where n is large enough, such that a does not contain any variable with index greater or equal to 2^{n+1}. If M is empty, then $\mathfrak{p} \cap A$ is contained in $\bigcup_{i=0}^{n} \mathfrak{p}_i$ and hence contained in one of the $\mathfrak{p}_i$. If M is non-empty then choose $b \in M$. Then b must contain a variable of index greater than 2^{n+1} whose monomial does not contain a variable of index smaller than 2^{n+1}. We conclude that $a + b$ is not contained in any of the $\mathfrak{p}_i$ and is thus a unit in B, which is a contradiction. Hence $\mathfrak{p}$ is contained in one of the prime ideals $S^{-1}\mathfrak{p}_i$.

   According to the first line of the solutions, the localisation of B at any of the maximal ideals $S^{-1}\mathfrak{p}_i$ is Noetherian. Furthermore, every element $\alpha \in B$ has only finitely many monomials, hence is contained in only finitely many maximal ideals $S^{-1}\mathfrak{p}_i$. By using the lemma we conclude that B is Noetherian.

Solutions Sheet 11

Integral Ring Extensions

1. Let $A \hookrightarrow B$ be an integral ring extension. Let $f : A \to k$ be a homomorphism to an algebraically closed field k. Prove that f can be extended to a homomorphism $B \to k$, which restricts to f on A.

   Solution: Let $\mathfrak{p} := \ker(f) \subset A$. Since k is a field, the ideal $\mathfrak{p}$ is prime. Using this and the universal property of the field of fractions we conclude that we can factor f as
$$A \to A/\mathfrak{p} \to K \to k$$
   where K is the field of fractions of $A/\mathfrak{p}$. On the other hand, by Lying over there is a prime ideal $\mathfrak{q} \subset B$ with $\mathfrak{q} \cap A = \mathfrak{p}$ and $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. Let L be the field of fractions of $B/\mathfrak{q}$. The inclusion $A/\mathfrak{p} \to B/\mathfrak{q}$ extends to an inclusion of fields $K \to L$. Since $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$, we conclude that L/K is an algebraic field extension. By a classical statement of algebra, we can thus lift the map $K \to k$ to a map $L \to k$. Together with the map $B \to B/\mathfrak{q} \to L$ this gives a lift of f.

2. Let $A \hookrightarrow B$ be an integral ring extension. Prove:

   (a) If $x \in A$ is a unit in B, then it is a unit in A.

   (b) The Jacobson radical of A is the contraction of the Jacobson radical of B.

   Solution:

   (a) Let $x \in A$ be a unit in B. Let $y \in B$ such that $xy = 1$. Since B is integral over A we conclude that y satisfies a polynomial equation
$$y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0$$
   for elements $a_0, \ldots, a_{n-1} \in A$. Multiplying it by x^{n-1} gives the equation
$$y + a_{n-1} + \cdots + a_1 x^{n-2} + a_0 x^{n-1} = 0$$
   And so $y \in A$.

   (b) By Lying over the maximal ideals of A are precisely the contractions of the maximal ideals of B. Since the Jacobson radical is the intersection of all maximal ideals we conclude the statement.

3. Let $A \hookrightarrow B$ be an integral ring extension. Let $\mathfrak{n} \subset B$ be a maximal ideal and denote $\mathfrak{m} := \mathfrak{n} \cap A$ for the corresponding maximal ideal in A. Is $B_{\mathfrak{n}}$ necessarily integral over $A_{\mathfrak{m}}$?

   Solution: No. Consider the rings $A := k[X^2 - 1] \subset k[X] =: B$, where k is a field. The ring B is integral over A, since the element X is integral over A. Let $\mathfrak{n} := (X - 1)$. This gives $\mathfrak{m} = (X - 1) \cap A = (X^2 - 1)$. We show that the element $\frac{1}{X+1}$ is not integral over $A_{\mathfrak{m}}$. Assume otherwise. Then there are polynomials $f_0, \dots, f_n \in A$ and $g_0, \dots, g_n \in A \smallsetminus \mathfrak{m}$ such that

$$\sum_{i=0}^{n} \frac{f_i}{g_i(X+1)^i} = \frac{1}{(X+1)^{n+1}}$$

   But the $g_0, \dots, g_n$ do not have a root at $X = \pm 1$. Thus the left hand side of the equation

$$\sum_{i=0}^{n} \frac{f_i(X+1)^{n-i}}{g_i} = \frac{1}{X+1}$$

   does not have a pole at $X = -1$. A contradiction.

4. Show that the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is not Noetherian.

   Solution: Denote by A the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. Let $p \in \mathbb{Z}$ be a prime number. For $n \geqslant 1$ let a_n be a root of $X^{2^n} - p$ such that $a_{n+1}^2 = a_n$. By construction, the a_n are in A. We prove that the ideals $(a_n)_{n \geqslant 1}$ form a strictly ascending chain of ideals in A. We only need to show that $a_{n+1} \notin (a_n)$. Assume otherwise. Then $a_{n+1} = b a_n$ for some element $b \in A$. But then $a_n = a_{n+1}^2 = b^2 a_n^2$. This proves that a_n is a unit in A. Since A is integral over $\mathbb{Z}[a_n]$, we use exercise 2.(a) to conclude that a_n is a unit in $\mathbb{Z}[a_n]$. However, in the ring $\mathbb{Z}[a_n] \cong \mathbb{Z}[X]/(X^{2^n} - p)$ the element X is not invertible, because p is not invertible in $\mathbb{Z}$. A contradiction.

5. Let A be an integral domain with field of fractions K. Let L/K be an algebraic field extension and B be the integral closure of A in L. Prove that the field of fractions of B is equal to L.

   Solution: Since L is a field containing B, it also contains the field of fractions of B. Conversely, let $S := A \smallsetminus (0)$. Since B is the integral closure of A in L we know that $S^{-1}B$ is the integral closure of $S^{-1}A = K$ in $S^{-1}L = L$. But the integral closure of K in L is L. Therefore we conclude that $L = S^{-1}B \subset \operatorname{frac}(B)$.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 12

Integral Extensions

1. Let A be a normal integral domain with field of fractions K. Let L/K be an algebraic field extension. Prove that an element $b \in L$ is integral over A if and only if its minimal polynomial over K lies in $A[X]$.

   Solution: Let $b \in L$ such that its minimal polynomial over K lies in $A[X]$. Since the minimal polynomial is monic we conclude that b is integral over A.

   Conversely assume that $b \in L$ is integral over A. Then there is a monic polynomial $P \in A[X]$ such that $P(b) = 0$. Let $M \in K[X]$ be the minimal polynomial of b over K. Since P is also an element in $K[X]$ we conclude that M divides P in $K[X]$. But all zeroes of P in an algebraic closure $\bar{L}$ of L are integral over A and so all zeroes of M in $\bar{L}$ are integral over A. Since the coefficients of a polynomial are polynomial expressions in the zeroes, we conclude that the coefficients of M are integral over A. Since they are in K and A is normal, we conclude that $M \in A[X]$.

2. Let A be a ring and G a finite group of automorphisms of A. Let A^G denote the subring of G-invariants of A, i.e. all $x \in A$ such that $\sigma(x) = x$ for all $\sigma \in G$.

   (a) Prove that A is integral over A^G.

   (b) If moreover A is a normal integral domain with field of fractions K and let L/K be a Galois extension with Galois group G. Let B denote the integral closure of A in L. Prove that $\sigma(B) = B$ for all $\sigma \in G$ and $B^G = A$.

   Solution:

   (a) Let $a \in A$. We define $g := \prod_{\sigma \in G}(X - \sigma(a))$. This is a polynomial, because G is a finite group. Furthermore $\sigma(g) = g$ for all $\sigma \in G$ and thus the coefficients of g are in A^G. So g is a monic polynomial in $A^G[X]$ with a as a zero, which proves the claim.

   (b) In the lecture, we have already seen that $\sigma(B) = B$ for all $\sigma \in G$. The inclusion $B^G \supset A$ follows from the fact that $B \supset A$ and G acts trivially on A. Conversely let $b \in B^G \subset B$. Then $b \in L^G = K$ and b is integral over A. Because A is normal, we conclude that $b \in A$. Hence $B^G \subset A$.

3. Let K be a field of characteristic zero. Find an explicit solution of Noether's Normalization Lemma for the following K-algebras:

   (a) $K[X, Y]/(XY)$

(b) $K[X,Y,Z,W]/(XY-ZW)$

(c) $K[X,Y,Z]/((XY-1)\cap(Y,Z))$

Solution: We find the solutions by following the proof of Noether's Normalisation Lemma.

(a) A solution is $K[X+Y]$.

(b) A solution is $K[X+Y,Z,W]$.

(c) A solution is $K[X+Y,X-Z]$.

4. Prove that every unique factorisation domain is normal.

   Solution: Let A be a unique factorisation domain with field of fractions K. Let $\frac{a}{b}\in K$ be integral over A with $a,b\in A$ relatively coprime. Thus there exists a monic polynomial $f=X^n+\sum_{i=0}^{n-1}c_iX^i\in A[X]$ such that $f(\frac{a}{b})=0$. Then we have $a^n+b\sum_{i=0}^{n-1}c_ia^ib^{n-i-1}=0$. This implies that b divides a^n. A contradiction to the unique factorisation property.

5. Let R be a ring and $A\subset B$ be R-algebras. Suppose that $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}\subset R$. Prove that B is integral over A.

   Solution: Let $b\in B$. Let $\mathfrak{p}\subset R$ be a prime ideal. Since b is integral over $A_{\mathfrak{p}}$, we find elements $a_0,\dots,a_{n-1}\in A$ and $s_0,\dots,s_{n-1}\in R\setminus\mathfrak{p}$ such that

$$b^n+(a_{n-1}/s_{n-1})b^{n-1}+\dots+(a_0/s_0)=0$$

   Set $s_{\mathfrak{p}}:=s_0\dots s_{n-1}$. We multiply with $(s_{\mathfrak{p}})^n$ to find that $s_{\mathfrak{p}}b$ is integral over A. Let I be the ideal in R generated by $s_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ of R. We prove that $I=(1)$. If not, then I is contained in a maximal ideal $\mathfrak{m}$ of R. But $s_{\mathfrak{m}}\notin\mathfrak{m}$, which gives a contradiction. Since $I=(1)$ there is a finite linear combination $\sum_{\mathfrak{p}}'r_{\mathfrak{p}}s_{\mathfrak{p}}=1$ with $r_{\mathfrak{p}}\in R$. Multiplied by b this leads to $b=\sum_{\mathfrak{p}}'r_{\mathfrak{p}}s_{\mathfrak{p}}b$. As a sum of integral elements over A, we conclude that b is integral over A.

D-MATH
Prof. Paul Nelson

Commutative Algebra

HS 2017

Solutions Sheet 13

Valuation Rings

1. Let A be an integral domain. Prove:

   (a) A is a valuation ring if and only if for all pairs of ideals $\mathfrak{a}, \mathfrak{b} \subset A$ we have $\mathfrak{a} \subset \mathfrak{b}$ or $\mathfrak{b} \subset \mathfrak{a}$.

   (b) If A is a valuation ring and $\mathfrak{p} \subset A$ a prime ideal, then $A_\mathfrak{p}$ and $A/\mathfrak{p}$ are both valuation rings.

   Solution:

   (a) Assume that A is a valuation ring and let $\mathfrak{a}, \mathfrak{b} \subset A$ be two ideals. If $\mathfrak{a} \not\subset \mathfrak{b}$, choose an element $f \in \mathfrak{a} \smallsetminus \mathfrak{b}$. For all $g \in \mathfrak{b}$ we know that $\frac{f}{g} \notin A$, otherwise f would be in $\mathfrak{b}$. Since A is a valuation ring, we know that $\frac{g}{f} \in A$ and thus $g = \frac{g}{f} f \in \mathfrak{a}$. We conclude that $\mathfrak{b} \subset \mathfrak{a}$. Conversely, let $x := \frac{f}{g}$ be an element in the field of fractions of A. By assumption we have $(f) \subset (g)$ or $(g) \subset (f)$. Hence $x \in A$ or $x^{-1} \in A$.

   (b) By the inclusion preserving correspondence of ideals in A which contain $\mathfrak{p}$ (resp. are contained by $\mathfrak{p}$) and ideals in $A/\mathfrak{p}$ (resp. $A_\mathfrak{p}$), we conclude by (a) that $A/\mathfrak{p}$ (resp. $A_\mathfrak{p}$) is a valuation ring.

2. Let A be a valuation ring with field of fractions K. Prove that every ring B with $A \subset B \subset K$ is a localisation of A at a prime ideal.

   Solution: For every element $x \in K$ we have $x \in A$ or $x^{-1} \in A$, hence $x \in B$ or $x^{-1} \in B$, which proves that B is a valuation ring. Thus B has a unique maximal ideal $\mathfrak{n}$. Then $\mathfrak{p} := \mathfrak{n} \cap A$ is a prime ideal of A. Every element $a \in A \smallsetminus \mathfrak{p}$ is invertible in B, hence $A_\mathfrak{p} \subset B$. Conversely, let $x \in B$. If $x \in A$, then $x \in A_\mathfrak{p}$. Otherwise $x^{-1} \in A \subset B$. But then $x^{-1} \in B^\times = B \smallsetminus \mathfrak{n}$ and thus $x^{-1} \in A \smallsetminus \mathfrak{p}$. Hence $x \in A_\mathfrak{p}$. We conclude that $A_\mathfrak{p} = B$.

3. Let K be a field and consider the field $K(X)$.

   (a) Let $P \in K[X]$ be irreducible. Construct a normalized discrete valuation $\nu_P : K(X)^* \to \mathbb{Z}$ such that its valuation ring is $K[X]_{(P)}$.

   (b) Prove that $\tau : K(X)^* \to \mathbb{Z}$ defined by $\tau(\frac{f}{g}) = \deg(g) - \deg(f)$ is another valuation.

   (c) Prove that the valuations τ and ν_P for all irreducible polynomials $P \in K[X]$ are precisely all non-trivial valuations on $K(X)$ which are trivial on K.

Solution:

(a) For an element $x \in K(X)^*$ let $f, g \in K[X] \setminus \{0\}$ such that P does neither divide f nor g and such that $x = P^n \frac{f}{g}$ for some $n \in \mathbb{Z}$. Then we set $\nu_P(x) := n$. This is a well-defined map $K(X)^* \to \mathbb{Z}$. It follows directly that it is normalized. For $x, y \in K(X)^*$ let $f, g, h, k \in K[X] \setminus \{0\}$ such that $x = P^{\nu_P(x)} \frac{f}{g}$ and $y = P^{\nu_P(y)} \frac{h}{k}$. Assume without loss of generality that $\nu_P(y) \geqslant \nu_P(x)$. Then we see that $\nu_P(xy) = \nu_P(x) + \nu_P(y)$ and

$$x + y = P^{\nu_P(x)} \left(\frac{fk + P^{\nu_P(y) - \nu_P(x)} hg}{gk} \right)$$

The denominator cannot be divisible by P, so we have $\nu_P(x + y) \geqslant \nu_P(x) = \min\{\nu_P(x), \nu_P(y)\}$. Thus ν_P is a valuation. By definition it follows directly that the valuation ring of ν_P is $K[X]_{(P)}$.

(b) Let $\varphi : K(X) \to K(X)$ be the field isomorphism induced by $\varphi(X) = \varphi(X^{-1})$. Let ν_X be the valuation from (a) for $P := X \in K[X]$. We observe that $\tau = \nu_X \circ \varphi$. Hence τ is a valuation.

(c) Let ν be a nontrivial valuation of $K(X)$ which is trivial on K. We want to find its valuation ring A. It certainly contains K. Suppose first that $X \in A$, so $K[X] \subset A$. Let $\mathfrak{m}$ be the maximal ideal of A. Then $\mathfrak{m} \cap K[X]$ is a prime ideal, which is non-zero, because otherwise $K(X) \subset A$, contrary to the nontriviality of ν. Since $K[X]$ is a principal ideal domain, there is an irreducible polynomial $P \in K[X]$ such that $(P) = \mathfrak{m} \cap K[X]$. We conclude that $K[X]_{(P)} \subset A$. Conversely, by exercise 2, we know that A is a localisation of $K[X]_{(P)}$ at a prime ideal, hence a localisation of $K[X]$ at a prime ideal contained in (P). But the only such prime ideals are (0) and (P), where the former is not possible by the assumption $A \neq K(X)$. Hence $A = K[X]_{(P)}$. Since also $\nu(P) = 1$, we conclude that the valuation ν is the same as ν_P defined in (a).

Suppose $X \notin A$. Then $X^{-1} \in A$, so $K[X^{-1}] \subset A$. We use the automorphism φ defined in the proof of (b) and see that $K[X] \subset \varphi(A)$. We do the same argument as before for $\varphi(A)$ with the addition that $P = X$ in this case, because $X^{-1} \notin \varphi(A)$. We then find that $\nu_X = \nu \circ \varphi$. Since φ is its own inverse we conclude that $\nu = \tau$.

4. Prove that an algebraically closed field does not admit any non-trivial discrete valuations.

Solution: Let ν be a valuation of an algebraically closed field k. Pick $a \in k$ such that $\nu(a) > 0$. Then $\sqrt{a} \in k$, since k is algebraically closed and $\nu(\sqrt{a}) = \frac{1}{2}\nu(a)$. Doing this repeatedly, there are elements in k with arbitrary small valuations. Hence the valuation cannot be discrete.

5. Let $a \in \mathbb{C}$. Let A be the ring of functions, which are holomorphic in some disc centered at a. Prove that A is a discrete valuation ring and find a uniformizer.

   Solution: By a shift we can assume without loss of generality that $a = 0$. Via taylor series we can identify A with the ring $\mathbb{C}[[X]]$. Its field of fractions is $\mathbb{C}((X))$. We know that a power series is invertible if and only if its constant term is non-zero. Thus every non-zero element $x \in \mathbb{C}((X))$ can be written as $x = X^n f$, where f is an invertible element of $\mathbb{C}[[X]]$, for some $n \in \mathbb{Z}$. We set $\nu(x) := n$. One can directly check that this defines a discrete valuation on $\mathbb{C}((X))$ with valuation ring $\mathbb{C}[[X]]$. Furthermore, the element X is a uniformizer.

6. Describe the spectrum of a discrete valuation ring.

   Solution: A discrete valuation ring A has only two prime ideals, namely the zero ideal (0) and the maximal ideal $\mathfrak{m}$. We have that $V(0) = \mathrm{spec}(A)$ and $V(\mathfrak{m}) = \mathfrak{m}$ are the only closed subsets of $\mathrm{spec}(A)$. Hence $\varnothing$ and (0) are the only open subsets. We conclude that $\mathrm{spec}(A)$ consists of two points, one of which is closed, but not open and the other one is open, but not closed.