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 $a_1, \ldots, a_n$ are nilpotent.

   (b) f is nilpotent if and only if $a_0, \ldots, a_n$ 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 $a_1, \ldots, a_n$ 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 $a_1, \ldots, a_n$ 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.