D-MATH Commutative Algebra HS 2018
Prof. Paul Nelson

Solutions sheet 1

Radical ideals, local rings and affine varieties

Important: all exercises in the present sheet assume familiarity with the contents of the first chapter of [1].

Let A be a commutative ring, k an algebraically closed field.

1. (From the lecture) Let $I \subset A$ be a subset such that $AI \subset I$, i.e. $xy \in I$ for all $x \in A$ and $y \in I$. Is it true that I is an ideal?

2. Let $\mathfrak{p} \subset A$ be a proper ideal. Show that the following are equivalent:

   (a) $\mathfrak{p}$ is a prime ideal;

   (b) if $\mathfrak{a}, \mathfrak{b} \subset A$ are ideals in A such that $\mathfrak{ab} \subset \mathfrak{p}$, then either $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.

3. Consider the non-commutative ring $\mathcal{M}_n(\mathbb{R})$ of square $n \times n$ matrices with real entries. Find a counterexample to show that the sum of two nilpotent elements need not be nilpotent.

   (Hence, if the ring is not commutative, the set of nilpotent elements is not necessarily an ideal.)

4. Let A be an integral domain with a finite number of elements. Show that A is a field. Deduce that in a finite commutative ring A every prime ideal is maximal.

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

   (a) $\mathfrak{a} \subset r(\mathfrak{a})$;

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

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

   (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 integer $k > 0$.

Solution. Let $\mathfrak{a} \subset A$ be an ideal. Recall that its radical is defined as

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some integer } n > 0\} \quad .$$

Let $x, y \in r(\mathfrak{a})$, then there are integers $n, m > 0$ such that $x^n \in \mathfrak{a}$ and $y^m \in \mathfrak{a}$. Now the bynomial theorem gives

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} \quad ;$$

in each term of the sum above, necessarily we must have that either the exponent of x is $\geqslant n$ or the exponent of y is $\geqslant m$. In both cases, $\mathfrak{a}$ being an ideal, we have that $x^k y^{n+m-k} \in \mathfrak{a}$ for all $0 \leqslant k \leqslant n+m$, which gives that $(x+y)^{n+m} \in \mathfrak{a}$, hence $x + y \in r(\mathfrak{a})$. If $x \in \mathfrak{a}$ and $a \in A$, then there exists an integer $n > 0$ such that $x^n \in \mathfrak{a}$. Commutativity of multiplication gives that $(ax)^n = a^n x^n \in \mathfrak{a}$, since $\mathfrak{a}$ is an ideal. Therefore $ax \in r(\mathfrak{a})$. The proof that $r(\mathfrak{a})$ is an ideal is thus concluded.

(a) Let $x \in \mathfrak{a}$, then in particular $x^n \in \mathfrak{a}$ for $n = 1$, so that $x \in r(\mathfrak{a})$.

(b) The previous point already gives $r(\mathfrak{a}) \subset r(r(\mathfrak{a}))$. Let $x \in r(r(\mathfrak{a}))$; then there exists an integer $n > 0$ such that $x^n \in r(\mathfrak{a})$. This in turns assures the existence of an integer $m > 0$ such that $x^{nm} = (x^n)^m \in \mathfrak{a}$, whence $x \in r(\mathfrak{a})$.

(c) First, $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ gives $r(\mathfrak{ab}) \subset r(\mathfrak{a} \cap \mathfrak{b})$. To conclude, we will show that $r(\mathfrak{a} \cap \mathfrak{b}) \subset r(\mathfrak{a}) \cap r(\mathfrak{b})$ and $r(\mathfrak{a}) \cap r(\mathfrak{b}) \subset r(\mathfrak{ab})$.
Let $x \in r(\mathfrak{a} \cap \mathfrak{b})$, so that $x^n \in \mathfrak{a} \cap \mathfrak{b}$ for some integer $n > 0$. This means that $x^n \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$, hence $x \in r(\mathfrak{a})$ and $x \in r(\mathfrak{b})$.
Let now $x \in r(\mathfrak{a}) \cap r(\mathfrak{b})$; we have $x^n \in \mathfrak{a}$ and $x^m \in \mathfrak{b}$ for some integers $n, m > 0$. This implies that $x^n x^m = x^{n+m} \in \mathfrak{ab}$, giving $x \in r(\mathfrak{ab})$.

(d) If $\mathfrak{a} = (1) = A$, then $A \supset r(\mathfrak{a}) \supset \mathfrak{a} = A$, where the second inclusion is given by point (a). This gives $r(\mathfrak{a}) = A = (1)$.
Conversely, assume that $r(\mathfrak{a}) = (1)$. It suffices to show that $1 \in \mathfrak{a}$. Now $1 \in r(\mathfrak{a})$, hence for a certain positive integer we have $1 = 1^n \in \mathfrak{a}$.

(e) Clearly $\mathfrak{a}+\mathfrak{b} \subset r(\mathfrak{a})+r(\mathfrak{b})$ as a consequence of point (a). This yields $r(\mathfrak{a}+\mathfrak{b}) \subset r(r(\mathfrak{a}) + r(\mathfrak{b}))$.
Conversely, let $x \in r(r(\mathfrak{a}) + r(\mathfrak{b}))$. Then $x^n \in r(\mathfrak{a}) + r(\mathfrak{b})$ for some integer $n > 0$; this means that $x^n = y + z$ with $y^m \in \mathfrak{a}$ and $z^p \in \mathfrak{b}$ for some integers $m, p > 0$. Then $x^{n(m+p)} = (x^n)^{m+p} \in \mathfrak{a} + \mathfrak{b}$ by the binomial theorem and the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, thus $x \in r(\mathfrak{a} + \mathfrak{b})$.

(f) Assume that $\mathfrak{p} \subset A$ is a prime ideal, and fix an integer $k > 0$. Then part (c) gives $r(\mathfrak{p}^k) = r(\mathfrak{p})$ (by induction on k). Since any prime ideal is radical, $r(\mathfrak{p}) = \mathfrak{p}$.

6. Prove that every prime ideal is radical. Find a counterexample to show that the converse is not true.

7. Let $n > 0$ be a positive integer. Find the unique positive integer m such that $r((n)) = (m)$.

   (Recall that, given an element $a \in A$, the notation (a) stands for the principal ideal in A generated by a.)

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

   (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 first that f is a unit in $A[X]$, i.e. there exists $g \in A[X]$ such that $fg = 1$. Equalling the zero-order coefficients of this two polynomials, we get that $a_0 b_0 = 1$ in A where $g = \sum_{i=0}^{m} b_i X^i$, which means that a_0 is invertible in A.

   We claim that $a_n^{r+1} b_{m-r} = 0$ for all $0 \leqslant r \leqslant m$, and we prove this by induction on r. We already know that $a_n b_m = 0$, since $a_n b_m$ is the higher-order coefficient of the polynomial fg. Now assume that $a_n^{r'+1} b_{m-r'} = 0$ for all $r' < r$. Then

   $$0 = a_n^r \left(\sum_{i+j=n+m-r} a_i b_j \right) = a_n^{r+1} b_{m-r} + \sum a_i a_n^{n-i} a_n^{m-j} b_j \qquad (1)$$

   where the last sum runs over all pairs (i, j) such that $i + j = n + m - r$ and $j > m - r$. By induction hypothesis, each term of this sum vanishes, hence equality (1) reduces to $0 = a_n^{r+1} b_{m-r}$, which is precisely what we wanted.

   In particular, we get that $a_n^{m+1} b_0 = 0$. Since we know that b_0 is a unit in A, this shows that a_n is nilpotent in A.

   To conclude the proof, we show that $f - a_n X^n$ is a unit, so that we inductively deduce from the previous argument that $a_1, \ldots, a_{n-1}$ are nilpotent. We shall prove more generally that if $x, y \in R$ are elements of a commutative ring R

such that x is a unit and y is nilpotent (say $x^l = 0$ for some $l > 0$), then their sum $x + y$ is again a unit. Since $x + y = x(1 + x^{-1}y)$ and $x^{-1}y$ is again nilpotent, it suffices to show that $1 - a$ is a unit whenever a is nilpotent. Now

$$(1 - a)(1 + a + \cdots + a^n) = 1 - a^{n+1} = 0$$

for n sufficiently large, so that $1 - a$ is a unit.

If you now assume that a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent, then applying inductively the previous argument (namely that adding a nilpotent element to a unit yields a unit) it can be shown that f is a unit in $A[X]$.

(b) If $a_0, \ldots, a_n$ are nilpotent, then so is f, since $f \in (a_0, \ldots, a_n)$ (the ideal of $A[X]$ generated by $a_0, \ldots, a_n$) and since we know that the set of nilpotent elements is an ideal.

Conversely, if f is nilpotent in $A[X]$, then it is immediate to see that a_0 is nilpotent in A (by developing the power f^m). Hence $f - a_0$ is nilpotent. By repeating the argument, we deduce that a_1 is nilpotent in A, and inductively we get the same for all coefficients of f.

(c) It is evident that if such an $a \in A$ exists, then f is by definition a zero-divisor in $A[X]$.

Assume now that f is a zero-divisor, so that by definition there exists $g = \sum_{j=0}^{m} b_j X^j \neq 0 \in A[X]$ such that $fg = 0$. Without loss of generality, we may take g to be of lowest degree amongst all non-zero polynomials that annihilate f. We may write $g = X^s g'$, where $s \geqslant 0$ is an integer and $g' \in A[X]$ has non-vanishing constant term. Hence $0 = X^s f g'$. This clearly can hold if and only if $fg' = 0$, therefore by our assumption $g = g'$ and so g has non-vanishing constant term, i.e. $b_0 \neq 0$. We claim that $b_0 f = 0$, which will achieve the proof. This will follow from the fact that $a_{n-r} g = 0$ for all $0 \leqslant r \leqslant n$, an assertion that we now prove by induction.

We know that $a_n b_m = 0$ (it is the coefficient of highest degree of fg). Hence $a_n g$ has degree strictly lower than g and still annihilates f. By our assumtpion on g, $a_n g = 0$.

Assume that $a_{n-r} g = 0$ for all $0 \leqslant r < r_0$. We prove that this holds also for r_0. Notice that

$$0 = fg = \sum_{i=0}^{n} a_i g X^i = \sum_{i=0}^{n-r_0} a_i g X^i$$

the last equality holding by induction hypothesis. Thus $a_{n-r_0} b_m = 0$, whence $a_{n-r_0} g$ is a polynomial annihilating f with degree strictly smaller that g. Again, this forces $a_{n-r_0} g = 0$. The proof is completed.

9. * Prove that, in the ring $A[X]$, the Jacobson ideal is equal to the nilradical. *(Hint: use parts* (a) *and* (b) *of Exercise* 8 *and Proposition* 1.9 *of [1].)*

   Solution. In any commutative ring R, the nilradical ideal is contained in the Jacobson ideal (since every maximal ideal is prime). We need to show the reverse inclusion in the case $R = A[X]$ for some commutative ring A. Now let $f \in J(A[X])$ be in the Jacobson of $A[X]$; then $1 + x \cdot f$ is a unit in $A[X]$ by Proposition 1.9 of [1]. Exercise $8(a)$ gives that all coefficients of $x \cdot f$ are nilpotent in A. But the coefficients of $x \cdot f$ are precisely the same coefficients of f, hence f is nilpotent by Exercise $8(b)$. Therefore f is in the nipotent ideal of $A[X]$.

10. Let $A[[X]]$ denote the ring of formal power series $f = \sum_{n=0}^{\infty} a_n X^n$ with coefficients in A. Show that:

    (a) f is a unit in $A[[X]]$ if and only if a_0 is a unit in A;

    (b) if f is nilpotent, then a_n is nilpotent for all $n \geqslant 0$. Is the converse also true?;

    (c) f belongs to the Jacobson radical of $A[[X]]$ if and only if a_0 belongs to the Jacobson radical of A.

11. * Fix an element $x_0 \in \mathbb{R}^n$. Denote by $\mathcal{U} := \{U \subset \mathbb{R}^n \text{ open} : x_0 \in U\}$ the set of open neighborhoods of x_0, and define the set

$$S := \{(U, f) : U \in \mathcal{U},\ f \colon U \to \mathbb{R} \text{ continuous}\} \quad .$$

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

    Solution. Define a map $\varphi \colon R \to \mathbb{R}$ by setting $\varphi([U, f]) = f(x_0)$. It is straightforward to check that the map is well-defined and it is a ring homomorphism. Define $I = \ker \varphi$. Then I is an ideal in R, and since $R/I \simeq \mathbb{R}$ is a field, I is a maximal ideal. We claim that it is the unique maximal ideal of R (which shows that R is a local ring by definition). By Proposition 1.6 i) in [1] it suffices to show that each $[(U, f)] \in R \smallsetminus I$ is invertible in R.

    Assume thus that $([U, f]) \in R$ is such that $f(x_0) \neq 0$. Since f is continuous, there exists an open neighborhood V of x_0 in $\mathbb{R}^n$ such that $f(x) \neq 0$ for all $x \in V$. Hence on V the function f^{-1} is well-defined and continuous. This gives that $[(V, f^{-1})]$ is an inverse in R of $[(U, f)]$.

12. *Given a subset $T \subset k^n$, we say that T is an *algebraic set* (or, as in the lecture, a *variety*) if there exists a set $S \subset k[X_1, \ldots, X_n]$ such that $T = Z(S)$.

(a) Prove that the set of all algebraic sets in k^n is closed under finite unions and arbitrary intersections. Deduce that the set

$$\tau = \{V \subset k^n : k^n \smallsetminus V \text{ is an algebraic set}\}$$

is the set of open sets for a topology on k^n, which will be henceforth called the *Zariski topology* on k^n.

(b) Describe the Zariski topology on an algebraically closed field k.

(c) Prove that the Zariski topology on $\mathbb{C}^n$ is strictly coarser than the euclidean topology.

Solution.

(a) The empty set $\varnothing \subset k^n$ is an algebraic set, for example $\varnothing = Z(\{1\})$. If $T_1 = Z(S_1)$ and $T_2 = Z(S_2)$ are algebraic sets, then $T_1 \cup T_2 = Z(S_1 S_2)$, where

$$S_1 S_2 = \{f_1 f_2 : f_1 \in S_1,\ f_2 \in S_2\} \quad ,$$

hence $T_1 \cup T_2$ is an algebraic set. Hence the set of all algebraic sets is closed under finite unions.

The whole space k^n is an algebraic set, since $k^n = Z(\{0\})$. If $T_i = Z(S_i)$ is an algebraic set for all $i \in I$, then $\bigcap_{i\in I} T_i = Z(\bigcup_{i\in I} S_i)$, which shows that $\bigcap_{i\in I} T_i$ is also an algebraic set. We have thus shown that the set of algebraic sets is also closed under arbitrary intersections.

We conclude that the set τ of all complements of algebraic sets is closed under arbitrary unions and finite intersections. This makes it into the set of open sets for a topology on k^n.

(b) If k is an algebraically closed field, then every non-invertible polynomial $f \in k[X]$ factors into linear terms: $f = a_0 \prod_{i=1}^{\deg(f)} (X - a_i)$, with $a_1, \ldots, a_{\deg(f)} \in k$. Hence $V(f) = \{a_1, \ldots, a_{\deg(f)}\}$. Since any proper algebraic set is the set of common zeros of a finite number of non-constant polynomials, it is clear that any algebraic set is finite. Conversely, if $\{a_0, \ldots, a_n\} \subset k$ is a finite set, then it is precisely the zero-set of the polynomial $f = (X - a_0) \cdots (X - a_n)$.

We have thus shown that closed sets are precisely finite sets together with the whole set k. Therefore the Zariski topology on k is precisely the cofinite topology.

(c) Let $Z \subset \mathbb{C}^n$ be Zariski-closed set, i.e. an algebraic set. Then there exists a finite set $S \subset \mathbb{C}[X_1, \ldots, X_n]$ such that

$$Z = \{P \in \mathbb{C}^n : f(P) = 0 \text{ for all } P \in S\} = \bigcap_{f\in S} V(f) \quad .$$

Now each set $V(f)$ is closed for the euclidean topology, since it is the inverse image of the closed set $\{0\} \subset \mathbb{R}$ under a polynomial (hence continuous for the euclidean topology) function. Since arbitrary intersections of closed sets are closed, this shows that Z is closed for the euclidean topology. We have thus shown that the Zariski topology is coarser than the euclidean topology. We shall now prove that it is strictly coarser, namely that we can find a set $A \subset \mathbb{C}^n$ which is closed for the euclidean topology but not for the Zariski topology. Consider $A = \mathbb{Z} \times \{0\}^{n-1}$ as a subset of $\mathbb{C}^n$. It is clearly a closed set for the euclidean topology. For the purpose of contradiction, assume that there exists a finite, non-empty set $S = \{f_1, \ldots, f_m\} \subset \mathbb{C}[X_1, \ldots, X_n]$ such that $A = V(S)$. For all $1 \leqslant i \leqslant m$, f_i is a polynomial in n complex variables such that $f_i(p, 0, \ldots, 0) = 0$ for all $p \in \mathbb{Z}$. Hence $f_i = f_i' + g_i$ where f_i' is a polynomial in $\mathbb{C}[X_1]$ such that $f_i'(p) = 0$ for all $\mathbb{Z}$. This forces $f_i' = 0$. Therefore f_i vanishes on $\mathbb{C} \times \{0\}^{n-1}$. This clearly contradicts the assumption that $A = V(S)$.

13. Let $X \subset k^n$ be a subset. Define

$$I(X) = \{f \in k[X_1, \ldots, X_n] : f(P) = 0 \text{ for all } P \in X\} \quad .$$

Show that $I(X)$ is an ideal in $k[X_1, \ldots, X_n]$ and that it is radical.

14. * Let $X, X' \subset k^n$ and $S, S' \subset k[X_1, \ldots, X_n]$ be subsets. Show the following inclusions (see exercise 13 for notation):

(a) $X \subset Z(S) \iff S \subset I(X)$;

(b) $Z(S \cup S') = Z(S) \cap Z(S')$;

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

(d) $S \subset S' \implies Z(S) \supset Z(S')$;

(e) $X \subset X' \implies I(X) \supset I(X')$;

(f) $S \subset I(Z(S))$ and $X \subset Z(I(X))$;

(g) $Z(S) = Z(I(Z(S)))$ and $I(X) = I(Z(I(X)))$.

Solutions.

(a) Assume that $X \subset Z(S)$, which means that for all $P \in X$, $f(P) = 0$ for all $f \in S$. This is clearly equivalent to say that $S \subset I(X)$.

(b) A point $P \in k^n$ is in $Z(S \cup S')$ if and only if $f(P) = 0$ for all $P \in S \cup S'$, hence if and only if $f(P) = 0$ for all $P \in S$ and $g(P) = 0$ for all $g \in S'$. This is equivalent to $P \in Z(S) \cap Z(S')$.

(c) We can argue in the same fashion as in part (c).

(d) Assume that $S \subset S'$ and let $P \in Z(S')$. Then, for all $f \in S'$, $f(P) = 0$. In particular, for all $f \in S$, $f(P) = 0$, hence $P \in Z(S)$, so that $Z(S) \supset Z(S')$.

(e) It is completely analogous to part (d).

(f) Assume that $f \in S$ and let $P \in Z(S)$. Then by definition of $Z(S)$ we have $f(P) = 0$. Hence f vanishes on all points in $Z(S)$, which by definition means that $f \in I(Z(S))$. The second inclusion is proved in a similar manner.

(g) Part (f) gives the inclusion $Z(S) \subset Z(I(Z(S)))$. Moreover, $S \subset I(Z(S))$ (again by part (f)); part (d) thus gives $Z(S) \supset Z(I(Z(S)))$. The same argument applies to the second equality in (g).

References

[1] M.Atiyah, Y.McDonald (1994), *Introduction to commutative algebra*, Addison-Wesley Publishing Company.