Solutions to Sheet 1

Exercise 1

Determine the nilradical, the Jacobson radical and the units for each ring A below:

1. k a field and $A = k[T]$,
2. k a field and $A = k[\epsilon, T]/(\epsilon^2)$,
3. $n \geq 1$, k a field and $A = k[\![T_1, \dots, T_n]\!]$.

Solution.

1. *Nilradical.* If B is any commutative ring without zero divisors, then $B[T]$ doesn't have zero divisors. Indeed, if $f, g \in B[T]$ with $fg = 0$, we can look at the leading terms of f and g, obtaining $f = 0$ or $g = 0$. We now obtain $\mathrm{Nil}(A) = (0)$ as every element in the nilradical is a zero divisor.

   Units. Obviously, $k^\times \subset k[T]^\times$. We have the additive degree map $\deg : k[T]^\times \to \mathbb{N}_0$. If we have elements $f, g \in k[T]$ with $fg = 1$, then $0 = \deg(fg) = \deg(f) + \deg(g)$, thereby $\deg(f) = \deg(g) = 0$ and $f, g \in k^\times$. This shows that $k^\times \supset k[T]^\times$, and we have equality.

   Jacobson radical. Note that if B is any commutative ring and $f \in \mathrm{Jac}(B)$, then $1+f \in B^\times$. Indeed, if we had $1 + f \notin B^\times$, we'd find some maximal ideal $\mathfrak{m}$ containing $1 + f$ (by Zorn's lemma). But now $f \in \mathfrak{m}$ (as $f \in \mathrm{Jac}(B)$) and $1 + f \in \mathfrak{m}$, hence $1 \in \mathfrak{m}$. This is a contradiction. Thereby we obtain that every $f \in \mathrm{Jac}(A)$ has degree 0. As $A^\times \cap \mathrm{Jac}(A) = \emptyset$, we find $\mathrm{Jac}(A) = 0$. (As $\mathrm{Jac}(A) \supset \mathrm{Nil}(A)$, this is stronger than $\mathrm{Nil}(A) = 0$.)

2. *Nilradical and Jacobson radical.* We claim that if $I \subset \mathrm{Nil}(A)$, there is an equality $\mathrm{Nil}(A)/I = \mathrm{Nil}(A/I)$. Indeed, this can be seen directly by writing the nilradical as the intersection of prime ideals. The same statement is true for the Jacobson radical.

   We apply this statement with $I = (\varepsilon)$. As $\varepsilon^2 = 0$, we have $I \subset \mathfrak{p}$ for every prime ideal, hence $(\varepsilon) \subset \mathrm{Jac}(A)$. As $A/(\varepsilon) \cong k[T]$, we have $(0) = \mathrm{Nil}(A/(\varepsilon)) = \mathrm{Nil}(A)/(\varepsilon)$. This shows $\mathrm{Nil}(A) = (\varepsilon)$.

   The same proof, but with Jac in place of Nil, (and maximal ideals instead of prime ideals) shows that $\mathrm{Jac}(A) = (\varepsilon)$.

   Units. There are probably smarter ways to do this, but let's try brute force. Suppose we have $f = f_1 + \varepsilon f_2$ and $g = g_1 + \varepsilon g_2$, where $f_i, g_i \in k[T]$, such that $fg = 1$. Now $1 = f_1 g_1 + \varepsilon(f_1 g_2 + f_2 g_1)$. It follows that $f_1 \in k^\times$, and we clam that this is also sufficient for $f \in A^\times$. Indeed, up to multiplication with a constant in $k^\times$, f is of the form $1 + \varepsilon f_2$, and now f admits an inverse $f^{-1} = 1 - \varepsilon f_2$.

3. *Units.* We first claim that every $f \in A$ with non-zero constant term is invertible. Indeed, after multiplying with a unit $c \in k^\times$ we may assume that $f = 1 + R$ with $R \in (T_1, \dots, T_n)$. Now, f admits the inverse $f^{-1} = \frac{1}{1-(1-f)} = \sum_{n=0}^{\infty} (1-f)^n \in k[\![T_1, \dots, T_n]\!]$.

   Jacobson radical. We first claim that A is a local ring, i.e., a ring with a unique maximal ideal. Indeed, we have seen that every element not lying in the ideal $\mathfrak{m} = (T_1, \dots, T_n)$ is invertible, hence $\mathfrak{m}$ is an ideal that contains all other ideals.

Nil radical. We want to show that A is reduced. More generally, we prove the following statement, from where the claim follows by induction.

If B is reduced, $B[\![T]\!]$ is reduced.

for the sake of contradiction, assume that $f \in B[\![T]\!]$ is a non-zero power series with $f^n = 0$. Write $f = a_d T^d + a_{d+1} T^{d+1} + \dots$ with $a_d \neq 0$. Now $f^n = 0$ implies $a_d^n = 0$, so $a_d = 0$ by reducedness of B. Hence $f = 0$.

Exercise 2

Prove the *Chinese remainder theorem*: Let A be a ring and $\mathfrak{a}, \mathfrak{b} \subset A$ two ideals such that $\mathfrak{a} + \mathfrak{b} = A$. Then the map

$$A/\mathfrak{a} \cap \mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}, \quad r + \mathfrak{a} \cap \mathfrak{b} \mapsto (r + \mathfrak{a}, r + \mathfrak{b})$$

is an isomorphism. Moreover, show that $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$, where $\mathfrak{a} \cdot \mathfrak{b}$ is the smalles ideal in A containing all products ab wth $a \in A$, $b \in B$. Show $a \cap b = ab$. Show that map has kernel $a \cap b$ and that homomorphism is surjective.

Solution. We first show that this map is well-defined, and indeed a homomorphism of rings. This is evident for the reduction-mod-$\mathfrak{a}$ and reduction-mod-$\mathfrak{b}$ maps $A \to A/\mathfrak{a}$ and $A/\mathfrak{b}$. By the universal property of the product of rings we obtain the map $A \to A/\mathfrak{a} \times A/\mathfrak{b}$. The kernel of this homomorphism is given by the elements in A which lie simultaneously in $\mathfrak{a}$ and $\mathfrak{b}$, hence we obtain an injective map

$$A/(\mathfrak{a} \cap \mathfrak{b}) \to A/\mathfrak{a} \times A/\mathfrak{b}.$$

To show surjectivity, it suffices to construct elements $a, b \in A$ such that $a \mapsto (0, 1)$ and $a \mapsto (1, 0)$. As $\mathfrak{a} + \mathfrak{b} = A$, there are elements $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. These are the elements we are looking for! Indeed, as $a = 1 - b$ we find that a reduces to 1 mod $\mathfrak{b}$, and as $a \in \mathfrak{a}$ we find $(a + \mathfrak{a}, a + \mathfrak{b}) = (\mathfrak{a}, 1 + \mathfrak{b})$.

Remark. There is a more general version of the chinese remainder theorem which we will need in exercise 4. Namely, if $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ is a finite set of pairwise coprime ideals (meaning that for any choice $1 \leq i < j \leq n$ we have $\mathfrak{a}_i + \mathfrak{a}_j = A$), there is an isomorphism

$$A/(\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n) \cong A/\mathfrak{a}_1 \times \dots \times A/\mathfrak{a}_n.$$

To see this, one can either generalize the proof given above, or use induction after showing that the coprimality assumption implies that the ideals $(\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_{n-1})$ and $\mathfrak{a}_n$ are coprime.

We now show that $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$. The inclusion $\mathfrak{a} \cap \mathfrak{b} \supset \mathfrak{a} \cdot \mathfrak{b}$ is obvious, as all products ab lie in both $\mathfrak{a}$ and $\mathfrak{b}$. To show the reverse inclusion, let $f \in \mathfrak{a} \cap \mathfrak{b}$. Again, let $a + b = 1$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Then $fa + fb = f$, and the left hand side lies in $\mathfrak{a} \cdot \mathfrak{b}$ by definition.

Remark. Note that this statement is wrong if we drop the assumption that $\mathfrak{a} + \mathfrak{b} = 1$. Indeed, take for example $\mathfrak{a} = (4)$, $\mathfrak{b} = (6)$ as ideals of $\mathbb{Z}$. Then $\mathfrak{a}\mathfrak{b} = (24)$, while $\mathfrak{a} \cap \mathfrak{b} = (12)$. However, the assumption that $\mathfrak{a} + \mathfrak{b} = A$ is not necessary. In the case $A = k[X, Y]$, $\mathfrak{a} = (X)$ and $\mathfrak{b} = (Y)$ we still have $\mathfrak{a}\mathfrak{b} = (XY) = \mathfrak{a} \cap \mathfrak{b}$ even though $\mathfrak{a} + \mathfrak{b} = (X, Y) \neq A$.

Exercise 3

Recall that an element $e \in A$ in a ring A is called idempotent if $e^2 = e$.

1. Let A be a ring. Show that the map $e \mapsto (A_1 \coloneqq eA, A_2 \coloneqq (1-e)A)$ induces a bijection between the set $\mathrm{Idem}(A)$ of idempotents of A and the set of decompositions $A = A_1 \times A_2$ of rings.

2. Let $A = \mathbb{Z}/133\mathbb{Z}$. Determine $\mathrm{Idem}(A)$.

Solution.

1. The exercise does not make clear what it means by a decomposition. In the scope of this exercise, a decomposition of A is an isomorphism $\delta : A \to A_1 \times A_2$, where A_1 and A_2 are any two rings. We say that two decompositions $\delta_1 : A \to A_1 \times A_2$ and $\delta_2 : A \to B_1 \times B_2$ are isomorphic iff there are isomorphisms $\varphi_i : A_i \to B_i$, $i = 1, 2$ such that $(\varphi_1, \varphi_2) \circ \delta_1 = \delta_2$. We define the set D_A as the set of isomorphism classes of the set[1] of decompositions, and we'll show that the map specified in the exercise gives a bijection $\mathrm{Idem}(A) \to D_A$.

   First, note that $(1-e)^2 = (1-e)$ for any idempotent e.

   We have show that the map really is a map! That is, we show that for any idempotent element $e \in A$, there is an isomorphism $\delta_e : A \cong eA \times (1-e)A$, where eA and $(1-e)A$ carry the ring structure of A, but with identity given by e and $(1-e)$, respectively. Surjectivity is clear, and injectivity boils down to the calculation $\mathrm{Ker}(\delta_e) = (e) \cap (1-e) = (e) \cdot (1-e) = (0)$.

   Next, note that we also have a map $D_A \to \mathrm{Idem}(A)$ given by sending $\delta : A \to A_1 \times A_2$ to $e_\delta \coloneqq \delta^{-1}(1, 0)$. This map does not depend on the isomorphism class of δ as ring homomorphisms preserve the multiplicative unit. One quickly verifies that $\mathrm{Idem}(A) \to D_A \to \mathrm{Idem}(A)$ is the identity. The last thing to see is that $D_A \to \mathrm{Idem}(A) \to D_A$ is the identity as well, which is the same as showing that for a given decomposition $\delta : A \to A_1 \times A_2$, there is an isomorphism $\delta \cong \delta_{e_\delta}$. Such an isomorphism is the same as isomorphisms $\varphi_1 : e_\delta A \to A_1$, $\varphi_2 : (1 - e_\delta)A \to A_2$. As δ sends the ideal $(e) \subset A$ to the ideal generated by $(1, 0)$ in $A_1 \times A_2$, it is evident that there are such isomorphisms.

2. Note that $133 = 19 \times 7$, hence by the chinese remainder theorem $\mathbb{Z}/133 \cong \mathbb{Z}/19 \times \mathbb{Z}/7$. The right hand side is a product of fields, and it is clear that the only idempotents there are given by $(0,0), (1,0), (0,1), (1,1)$. As $1 = 19 \cdot 3 - 7 \cdot 8$, the isomorphism from the chinese remainder theorem is given by $(a, b) \mapsto 57b + 77a$, and we find that the non-trivial idempotents are given by 57 and 77.

Exercise 4

Let k be a field and let $k \to A$ be a ring homomorphism such that A is finite dimensional over k (i.e., regarded as a k-vector space, A has finite dimension).

1. Show that A is a field if A is an integral domain.

2. Deduce that each prime ideal in A is maximal.

3. Deduce that if A is reduced, then A is isomorphic to a finite product of finite field extensions l/k.

[1] Actually I'm not sure if this really is a set, but whatever. The decompositions will certainly form a category (a groupoid), with morphisms the isomorphisms we described. The isomorphism classes do form a set as they all are represented by quotients of A.

Solution.

1. Let $x \in A$ be nonzero. Let $\varphi : A \to A$ be the map obtained by multiplication with x, i.e., $\varphi(a) = xa$. Now φ is a morphism of k-vector spaces (as $\varphi(\lambda a+b) = \lambda\varphi(a)+\varphi(b)$ for $\lambda \in k$, $a, b \in A$.), and it is injective by the fact that A is an integral domain. Indeed, if $xa = 0$, we find $a = 0$ as there are no zero divisors and $x \neq 0$. But now φ is an injective morphism between k-vector spaces of the same dimension, hence an isomorphism. In particular, we find some element $x^{-1} \in A$ such that $1 = \varphi(x^{-1}) = xx^{-1}$. Hence every non-zero element of A has an inverse, and A is a field.

2. Let $\mathfrak{p} \in A$ be a prime ideal. We apply what we showed in part 1) to $A/\mathfrak{p}$. As $\mathfrak{p}$ is prime, $A/\mathfrak{p}$ is an integral domain. But also, the composition $k \to A \to A/\mathfrak{p}$ turns $A/\mathfrak{p}$ into a k-vector space with $\dim_k(A/\mathfrak{p}) \leq \dim_k(A)$ (surjective maps between vector spaces reduce dimension). In particular, $A/\mathfrak{p}$ is finite-dimensional over k. Now part 1) gives that $A/\mathfrak{p}$ is a field, and as an ideal is maximal if and only it's quotient ring is a field, we find that $\mathfrak{p}$ is maximal.

3. Let M be the set of maximal (or prime, they are the same by the above) ideals of A. We want to apply the chinese remainder theorem, but a priori we can't, because M might be infinite. We claim however that in our situation, M is finite. To show this, suppose that $(\mathfrak{m}_1, \mathfrak{m}_2, \dots)$ be an infinite sequence of elements in I. By the chinese remainder theorem, there is for any $N \in \mathbb{N}$ an isomorphism

$$A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_N) \cong A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_N.$$

The left-hand side has dimension $\leq \dim_k(A)$, as it is a quotient of A. Meanwhile, the right-hand side has dimension $\geq N$, as every quotient $A/\mathfrak{m}_i$ is a non-trivial k-vector space and thereby has dimension at least 1. If we choose $N > \dim_k(A)$, we arrive at a contradiction. Now $M = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$ is finite, and applying the chinese remainder theorem again yields the desired decomposition. All factors are field extensions of k of degree $\leq \dim_k(A)$, in particular finite.

Max von Consbruch, email: s6mavonc@uni-bonn.de. Date: April 17, 2023