

amsfonts

Problem 1. *Let A be a ring. Prove:*

(1.1) *If $x \in A$ is nilpotent, then $1 - x$ is invertible.*

Solution. *Proof.* Suppose that $x^n = 0$ for some $n \in \mathbb{N}$. Then,

$$(1 - x)(1 + x + x^2 + \cdots + x^{n-1}) = 1 - x^n = 1$$

□

(1.2) *The nilradical $N(A) = \{x \in A \mid x \text{ nilpotent}\}$ is an ideal of A .*

Solution. *Proof.* Let $x, y \in N(A)$, then $x^n = 0$ and $y^m = 0$ for some $n, m \in \mathbb{N}$. Then,

$$(x - y)^{n+m} = \sum_{k=0}^{n+m} (-1)^k \binom{n+m}{k} x^{n+m-k} y^k = 0$$

since $k \geq n$ or $n + m - k \geq m$ for all k . Thus, $x - y \in N(A)$. We have that $N(A)$ is an additive subgroup of A . Now, let $a \in A$. Then,

$$(ax)^n = a^n x^n = 0a = 0$$

so $ax \in N(A)$. Thus, $N(A)$ is an ideal of A .

□

(1.3) *$N(A)$ is contained in all prime ideals of A .*

Solution. *Proof.* Let $I \subset A$ be a prime ideal. Let $x \in N(A)$. Then, $x^n = 0 \in I$ for some $n \in \mathbb{N}$. Let us show by induction on n that this implies $x \in I$:

- If $n = 1$, then $x = 0 \in I$.
- Suppose that the statement is true for $n - 1$: $x^{n-1} = 0 \Rightarrow x \in I$. If $0 = x^n = x \cdot x^{n-1}$, since I is prime, $x \in I$ or $x^{n-1} \in I$. In the first case, we are done. The second case is just the inductive hypothesis.

□

(1.4) *$N(A)$ is the intersection of all prime ideals of A .*

Solution.

Claim. *Given $x \notin N(A)$, let Σ_x be the set of all ideals that do not contain any power of x . Then, Σ_x has a maximal element.*

Proof. We will use Zorn's lemma. Let us check the conditions:

Claim. Σ_x is a partially ordered set with respect to inclusion.

Claim. Σ_x is not empty.

Proof. Since $x \notin N(A)$, $0 \in \Sigma_x$. □

Claim. Every chain in Σ_x has an upper bound.

Proof. Let $\{I_\alpha\}_{\alpha \in S}$ be a chain in Σ_x . Then, $I = \bigcup_{\alpha \in S} I_\alpha$ is an ideal of A (One can check that if $x, y \in I$, then $x, y \in I_\alpha$ for some $\alpha \in S$, and then check the axioms from there). Let $x^n \in I$ for some $n \in \mathbb{N}$. Then, $x^n \in I_\alpha$ for some $\alpha \in A$. Since I_α is an ideal, $x \in I_\alpha$. Thus, $I \in \Sigma_x$. □

Now that we have verified the conditions of Zorn's lemma, we can conclude that Σ_x has a maximal element. □

Claim. Let $x \notin N(A)$. Then the maximal element $K(x)$ of Σ_x is prime.

Proof. Let $a, b \in A$ such that $ab \in K(x)$. By way of contradiction, suppose that $a \notin K(x)$ and $b \notin K(x)$. Then, $x^n \in (a)$ and $x^m \in (b)$ for some $m, n \in \mathbb{N}$, but $x^{n+m} \notin (ab) = (a)(b)$. Contradiction. □

Finally, we can prove the statement.

Claim. $N(A)$ is the intersection of all prime ideals of A .

Proof. Let J be the intersection of all prime ideals of A . By 1.3, we know that $N(A) \subset J$. We want to prove that if $x \notin N(A)$, then $x \notin J$. Indeed, $J \subset K(x)$ because $K(x)$ is prime and $x \notin K(x)$ because $K(x)$ does not contain any power of x . □

Problem 2. Let A be a ring. Let $a_i \in A$ and $f = a_0 + a_1T + \cdots + a_nT^n \in A[T]$ be a polynomial. Prove:

(2.1) f is a unit in $A[T] \iff a_0$ is a unit in A and a_1, \dots, a_n are nilpotent.

Solution. *Proof.* We will show both implications separately.

(\Leftarrow) Let $a_i^{n_i} = 0$ for all $1 \leq i \leq n$. Consider $s = \sum_{i=1}^n n_i$. Let $h = -a_1T - \cdots - a_nT^n$ be the negative of the polynomial without the constant term. Then,

$$h^s = \left(-\sum_{i=1}^n a_i T^i \right)^s = (-1)^s \sum_{j_1 + \cdots + j_n = s} a_1^{j_1} \cdots a_n^{j_n} T^{j_1 + 2j_2 + \cdots + nj_n}$$

By the pigeonhole principle, in each term of the sum, there is at least one $j_k \geq n_k$ so $a_k^{j_k} = 0$, and thus $h^s = 0$. Then, h is nilpotent, so is $a_0^{-1} \cdot h$ and, by 1.1, $1 - a_0^{-1} \cdot h$ is invertible. Multiplying by a_0 , we get that $f = a_0 - h$ is also invertible.

(\Rightarrow) Suppose, there exists $g = b_0 + b_1T + \cdots + b_mT^m \in A[T]$ such that $1 = fg = \sum_{i=0}^{n+m} s_iT^i$, where $s_i = \sum_{j=0}^n a_jb_{i-j}$ and $b_k = 0$ for $k > m$ or $k < 0$. We first note that $1 = s_0 = a_0b_0 \Rightarrow a_0, b_0 \in A^*$. Next, suppose $n > 0$ (Otherwise, there is nothing to show).

Claim. Let $0 \leq k \leq m$. $a_n^{k+1}b_{m-k} = 0$

Proof. By total induction on k :

- If $k = 0$, then $0 = s_{n+m} = a_nb_m = (a_n)^{0+1}b_{m-0}$.
- Suppose that the statement is true for $0, \dots, k-1$. Then, $s_{n+m-k} = 0$ as $n+m-k \geq n > 0$. Therefore:

$$0 = a_n^k s_{n+m-k} = \sum_{j=0}^n a_n^k a_j b_{n+m-k-j} = a_n^{k+1} b_{m-k} + \sum_{j=0}^{n-1} a_n^k a_j b_{n+m-k-j}$$

Now, the terms in the sum are zero by the inductive hypothesis, as $j < n \Rightarrow -(n-k-j) < k \Rightarrow (n-k-j) + 1 \leq k$. Therefore, $a_n^{k+1}b_{m-k} = 0$ as we wanted to show. □

Now, by setting $k = m$, we get that $a_n^{m+1}b_0 = 0$. Since b_0 is a unit, $a_n^{m+1} = 0$ and a_n is nilpotent. We are almost done if we realize the following:

Claim. Let $p = c_0 + c_1T + \cdots + c_lT^l \in A[T]$ be an invertible polynomial such that c_l is nilpotent. Then, $q = c_0 + c_1T + \cdots + c_{l-1}T^{l-1}$ is also invertible.

Proof. Note that c_lT^l is nilpotent and so is $c_lT^lp^{-1}$. Then, $1 - c_lT^lp^{-1}$ is invertible by 1.1. Finally, because p is invertible, so is $q = p - c_lT^l = p(1 - c_lT^lp^{-1})$. □

We will prove that for $0 < k \leq n$, $a_0 + \cdots + a_kT^k$ is invertible and a_k is nilpotent by (reverse) induction on k .

- a_n has already been done.
- If $0 < k < n$, by hypothesis a_{k+1} is nilpotent and $a_0 + \cdots + a_{k+1}T^{k+1}$ is invertible. Then, $a_0 + \cdots + a_kT^k = (a_0 + \cdots + a_{k+1}T^{k+1}) - a_{k+1}T^{k+1}$ is invertible by the claim. Therefore, a_k is nilpotent.

(\Rightarrow) (Faster Version) Let f be a unit in $A[T]$.

Claim. Let $\mathfrak{p} \in \text{Spec}(A)$. Then, $a_i \in \mathfrak{p}$ for all $i \in \{1, \dots, n\}$.

Proof. $\mathfrak{p} \in \text{Spec}(A)$ implies that A/\mathfrak{p} is an integral domain. Consider the reduction $\pi : A[T] \rightarrow A/\mathfrak{p}[T]$ that takes each element $a \in A[T]$ to the class $\bar{a} \in A/\mathfrak{p}[T]$. Since A/\mathfrak{p} is an integral domain,

$$0 = \deg \bar{1} = \deg \bar{f} \cdot \overline{f^{-1}} = \deg \bar{f} + \deg \overline{f^{-1}}$$

In particular, $\deg \bar{f} = 0$ so, for all $i \in \{1, \dots, n\}$, $\bar{a}_i = \bar{0} \Rightarrow a_i \in \mathfrak{p}$. □

Since this holds for all $\mathfrak{p} \in \text{Spec}(A)$, we have that $\forall i \in \{1, \dots, n\}, a_i \in \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p} = N(A)$ (by 1.4). Finally, suppose that $f^{-1} = b_0 + b_1T + \dots + b_mT^m$. Given that $ff^{-1} = 1$ we have that $a_0b_0 = 1$, and thus a_0 is invertible.

□

(2.2) f is nilpotent $\iff a_0, \dots, a_n$ are nilpotent.

Solution. *Proof.* We will show both implications separately.

(\Leftarrow) Just use the same argument as in the previous part of the exercise, but directly on f , not on $h = a_0 - f$.

(\Rightarrow) If f is nilpotent, then $1 - f$ is invertible by 1.1. Thus, by the previous part, $-a_1, \dots, -a_n$ are nilpotent. Because $-a_i$ is nilpotent, a_i is nilpotent. We only have to prove that a_0 is nilpotent. By the other implication, h is nilpotent. Then, by 1.2, $a_0 = f + h$ is nilpotent.

□

(2.3) f is a zero divisor \iff there exists $a \in A, a \neq 0$ such that $af = 0$.

Solution. *Proof.* The backward implication is trivial because of the inclusion $A \subset A[T]$. For the forward implication, suppose that f is a zero divisor. Then, there exists $g \in A[T], g \neq 0$ such that $fg = 0$. Let $g = b_0 + \dots + b_mT^m$ be the minimum degree polynomial satisfying the condition $fg = 0$. Suppose that $m > 0$.

Claim. $\exists i \in \{1, \dots, n\}$ s.t. $a_i g \neq 0$

Proof. Suppose not. Then, $a_i g = 0$ for all $i \in \{1, \dots, n\}$. Then, $a_i b_m = 0$ for all $i \in \{1, \dots, n\}$. But then we have $b_m f = 0$ with $b_m \in A$, in contradiction with g being a polynomial with minimum degree. □

Take i maximal such that $a_i g \neq 0$. Then, $0 = fg = (a_0 + \dots + a_i T^i)(b_0 + \dots + b_m T^m) + \sum_{j=i+1}^n T^j a_j g = (a_0 + \dots + a_i T^i)(b_0 + \dots + b_m T^m)$, and $a_i b_m = 0$. Thus, we have a polynomial $g' = a_i g \neq 0$ with degree $m - 1$ satisfying $f(a_i g) = a_i(fg) = 0$, in contradiction with g being of minimal degree. □

Problem 3. Describe $\text{spec}(\mathbb{Z}[T])$ **Solution.** Suppose that $\mathfrak{p} \subset \mathbb{Z}[T]$ is an ideal. We will distinguish three cases:

1. $\mathfrak{p} = (0)$. (0) is a prime ideal of $\mathbb{Z}[T]$ since $\mathbb{Z}[T]$ is an integral domain.
2. $\mathfrak{p} = (f)$ is a principal ideal generated by a non-zero polynomial $f \in \mathbb{Z}[T]$. There are two possibilities:
 - $\deg f = 0 \Leftrightarrow f = n \in \mathbb{Z}$. Suppose (n) is a prime ideal. In this case, it is clear by the inclusion $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}[T]$ that $(n) = (n)^e$ is prime in \mathbb{Z} . Conversely, let $p \in \mathbb{Z}$ be a prime number. $\mathbb{Z}[T]/(p) \cong \mathbb{Z}/(p)[T]$ is an integral domain since $\mathbb{Z}/(p)$ is a field (in particular, an integral domain). We obtain the ideals (p) where $p \in \mathbb{Z}$ is prime.
 - $\deg f > 0$.

Claim. (f) is prime $\Rightarrow f$ is primitive.

Proof. Otherwise, there is some non-unit $p \in \mathbb{Z}$ that divides all coefficients of f . Then $f = pg$ for some $g \in \mathbb{Z}[T]$, which is a non-trivial factorization of f . f is not irreducible, so it is not prime (since \mathbb{Z} is a domain). \square

Claim. (f) is prime $\Rightarrow f$ is irreducible in $\mathbb{Q}[T]$.

Proof. Suppose $f = gh$ is a non-trivial factorization, for some $g, h \in \mathbb{Q}[T]$ (in particular, since all non-zero elements of \mathbb{Q} are units, $\deg g, \deg h > 0 \Rightarrow \deg g, \deg h < \deg f$). Taking a common denominator n and multiplying by it, we obtain $nf = \tilde{g}\tilde{h}$ in $\mathbb{Z}[T]$. By the left side, this belongs to (f) , but \tilde{g}, \tilde{h} do not belong to (f) since they have strictly smaller degree than f . \square

Claim. These conditions are also sufficient: if f is irreducible in $\mathbb{Q}[T]$ and primitive, then (f) is prime.

Proof. Consider the natural inclusion $\phi : \mathbb{Z}[T] \rightarrow \mathbb{Q}[T]$. We will extend and then contract the ideal (f) of $\mathbb{Z}[T]$. By taking a common denominator and factors:

$$(f)^{ec} = \mathbb{Z} \cap (f)_{\mathbb{Q}} = \mathbb{Z}[T] \cap \left\{ \frac{n}{m}fh \mid n, m \in \mathbb{Z}, h \in \mathbb{Z}[T] \text{ primitive} \right\}$$

We know that $(f) \subset (f)^{ec}$. We will prove the other inclusion and therefore equality. Indeed, take $g = \frac{n}{m}fh \in (f)^{ec}$ of the form described above. For any prime $p \mid m$, we have shown that (p) is prime in $\mathbb{Z}[T]$. Furthermore, f, h are primitive, so p does not divide them $\Rightarrow p \mid n$. We can cancel p in the fraction, and repeat the process for all prime factors of m . Therefore, $g \in (f)_{\mathbb{Z}}$. Now, as f is irreducible in $\mathbb{Q}[T]$, which is a PID, $(f)_{\mathbb{Q}} = (f)_{\mathbb{Z}}^e$ is prime in $\mathbb{Q}[T]$. Therefore, so is $(f) = (f)^{ec} \subset \mathbb{Z}[T]$. \square

With all these claims, this case yields ideals of the form (f) where $f \in \mathbb{Z}[T]$ is irreducible and primitive.

3. \mathfrak{p} is not principal. I don't know how to do this case. Idea: Consider the gcd of all the generators in $\mathbb{Q}[T]$, we have bezout coefficients, so we can write it as a linear combination of them with rational coefficients.