1: Rings and Ideals

Exercise 1

Let x be a nilpotent element of a ring A, ie. $x \in \sqrt{0}$. Show that $1+x$ is a unit of A and that in general, the sum of a unit and a nilpotent is a unit.

Proof. Observe that the factorization (n odd)

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

implies that, if x is nilpotent, for sufficiently large n the second factor on the right hand side is the multiplicative inverse of $1+x$ because the left hand side simplifies to 1 since $x^n = 0$ for sufficiently large n.

Now let u be any unit with inverse v, and y any nilpotent element. Then $v(u+y) = 1 + vy$ so that if we set $x = vy$ (which is clearly nilpotent) in the previous equation, we can conclude that $1 + vy$ is a unit. Thus $u + y = u(1 + vy)$ is also a unit and we are done. □

Exercise 4

Prove that for any polynomial ring $A[x]$, the Jacobson radical is equal to the nilradical. In symbols $\mathrm{Jac}\,(A[x]) = \sqrt{0}$.

Proof. For an arbitrary ring B, every maximal ideal is prime then clearly the nilradical is contained in the Jacobson radical:

$$\sqrt{0} = \bigcap_{\mathfrak{p}\text{ prime}} \mathfrak{p} \subseteq \bigcap_{\mathfrak{m}\text{ maximal}} \mathfrak{m} = \mathrm{Jac}\,(B)\,.$$

This means that the inclusion $\sqrt{0} \subseteq \mathrm{Jac}\,(A[x])$ is trivial. Next we will use the characterization of the Jacobson radical:

$$x \in \mathrm{Jac}\,(A[x]) \quad\Longleftrightarrow\quad 1 - \lambda x \text{ is a unit for all } \lambda \in A[x]. \tag{1}$$

Let $f \in \mathrm{Jac}\,(A[x])$. We use exercise 2.*ii* to prove that $f \in \sqrt{0}$, ie. f is nilpotent. If we write $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then exercise 2.*ii* reduces the problem to proving that a_i is nilpotent in A for all $i = 0, \ldots, n$.

Now, if we take $\lambda = -1$ in (**??**) then we conclude that

$$1 + f(x) = (1 + a_0) + a_1x + \cdots + a_nx^n$$

is a unit. By exercise 2.*i* this means that $1 + a_0$ is a unit in A and a_i is nilpotent for all $i = 1, \ldots, n$. Thus the only thing left to prove is that a_0 is nilpotent.

Since $1 + a_0$ is a unit in A, there is a $u \in A$ such that $u(1 + a_0) = u + ua_0 = 1$ which implies that $u = 1 - ua_0$. If we take $\lambda = u$ then $1 - uf(x) = u + a_1x + \cdots + a_nx^n$ is a unit

□

Exercise 6

A ring A is such that every prime ideal not contained in the nilradical contains a nonzero idempotent, that is for every ideal $I \leq A$ we have:

$$I \not\subseteq \sqrt{0} \quad \Longrightarrow \quad \exists e \in I \textbf{ such that } e^2 = e \neq 0.$$

Prove that $\sqrt{0} = \mathrm{Jac}\,(A)$ that is the Jacobson Radical is equal to the nilradical.

Proof. We know that (cf. Exercise 4) for any ring A, $\sqrt{0} \subseteq \mathrm{Jac}\,(A)$. So no we prove equality by contradiction: suppose $\sqrt{0}$ is contained strictly in $\mathrm{Jac}\,(A)$ and set $x \in \mathrm{Jac}\,(A) - \sqrt{0}$. Any such element satisfies $\langle x \rangle \not\subseteq \sqrt{0}$ so that by hypothesis the ideal $\langle x \rangle$ contains a nonzero idempotent e. Thus x divides e and we have the following formula:

$$e = \lambda x = \lambda^2 x^2 = e^2 \quad \Longrightarrow \quad \lambda x(1 - \lambda x) = 0. \tag{2}$$

Since $x \in \mathrm{Jac}\,(A)$ it satisfies the following equivalent property:

$$x \in \mathrm{Jac}\,(A) \quad \Longleftrightarrow \quad 1 - \lambda x \text{ is a unit for all } \lambda \in A.\text{(Prop. 1.9, pg 6)}$$

Thus we may cancel the factor inside the parenthesis of equation (**??**) and conclude $e = \lambda x = 0$; a contradiction. Thus $\mathrm{Jac}\,(A) = \sqrt{0}$. □

Exercise 7

Let A be a ring such that for all $x \in A$ there is an $n = n(x) > 1$ such that $x^n = x$. Prove that every prime ideal is maximal and thus $\mathrm{Jac}\,(A) = \sqrt{0}$.

Proof. Let $\mathfrak{p}$ be a prime ideal of A and consider $x + \mathfrak{p} \in A/\mathfrak{p}$ any nonzero element. By hypothesis there is an $n \in \mathbb{N}$ such that $x^n = x$ or equivalently $x(x^{n-1} - 1) = 0$. Since $A/\mathfrak{p}$ is an integral domain, we may cancel out the x so that $x^{n-1} + \mathfrak{p} = 1 + \mathfrak{p}$. We conclude that x is a unit and $A/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is maximal. □

Exercise 8

Prove that the prime ideals of A, i.e. Spec (A), has minimal elements with respect to inclusion.

Proof. We shall prove this by applying Zorn's Lemma $\mathrm{Spec}\,(A)$. Let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots$ be a descending chain of prime ideals. If we prove that:

$$\mathfrak{p} = \bigcap_{i=1}^{\infty} \mathfrak{p}_i \quad \text{is prime,}$$

then every descending chain in $\mathrm{Spec}\,(A)$ has a minimum in $\mathrm{Spec}\,(A)$, in this case $\mathfrak{p}$. By Zorn's Lemma we would then conclude that $\mathrm{Spec}\,(A)$ has minimal elements with respect to inclusion.

Thus we have reduced the exercise to proving that the intersection of a descending sequence of prime ideals is again prime. Suppose, $fg \in \mathfrak{p}$, then there exists an $n \in \mathbb{N}$ such that $fg \in \mathfrak{p}_n$. Since $\mathfrak{p}_n$ is prime then $f \in \mathfrak{p}_n \subseteq \mathfrak{p}$ or $g \in \mathfrak{p}_n \subseteq \mathfrak{p}$; thus proving that $\mathfrak{p}$ is prime.

□

Exercise 10

Let A be a ring and $\sqrt{0}$ its nilradical. prove that the following are equivalent:

1. **A has exactly one prime ideal.**
2. **every element of A is a unit or nilpotent, ie. $A = U(A) \cup \sqrt{0}$.**
3. **$A/\sqrt{0}$ is a field or equivalently $\sqrt{0}$ is maximal.**

Proof. We prove that $1 \implies 2 \implies 3 \implies 1$ as follows:

$1 \implies 2$ Suppose A has one prime ideal $\mathfrak{p}$, then $(A, \mathfrak{p}, A/\mathfrak{p})$ is a local ring and $A - \mathfrak{p}$ is the set of units of A. On the other hand $\sqrt{0} = \{\text{nilpotents}\} = \mathfrak{p}$ so that $A = (A - \mathfrak{p}) \cup \mathfrak{p} = U(A) \cup \sqrt{0}$.

$2 \implies 3$ Let $a + \sqrt{0}$ be a nonzero element of $A/\sqrt{0}$, that is $a \notin \sqrt{0}$. By hypothesis we have $A = U(A) \cup \sqrt{0}$ so that a must be a unit in A. Units are preserved under projection so that $a + \sqrt{0}$ is a unit, and we may conclude that $A/\sqrt{0}$ is a field.

$3 \implies 1$ If $A/\sqrt{0}$ is a field, then $\sqrt{0} = \mathfrak{m}$ is maximal. This means that $\mathfrak{m} \in \operatorname{Spec}(A)$ and

$$\mathfrak{m} = \sqrt{0} = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}.$$

Thus $\mathfrak{m} \subseteq \mathfrak{p}$ for every prime $\mathfrak{p}$, but since $\mathfrak{m}$ is maximal this is only possible of $\mathfrak{m} = \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$. We conclude that $\sqrt{0}$ is the only prime ideal of A.

□

Exercise 12

Let $(A, \mathfrak{m}, k)$ be a local field. Prove that A contains no nontrivial idempotent. That is an element $e \neq 0, 1$ such that $e^2 = e$.

Proof. We prove that the only idempotents of A are 0 and 1. Let e be an idempotent of A. If $e \notin \mathfrak{m}$, then, since A is a local ring, e is a unit. However, an idempotent who is also a unit must be 1 because:

$$e \text{ is a unit and } e^2 = e \quad \implies \quad e = e^{-1}e^2 = e^{-1}e = 1. \tag{3}$$

Thus if $e \notin \mathfrak{m}$ then $e = 1$.

Now suppose that $e \in \mathfrak{m}$. This means that $1 - e \notin \mathfrak{m}$ because, $e + (1 - e) = 1 \notin \mathfrak{m}$, and thus $1 - e$ is a unit. On the other hand $1 - e$ is idempotent because:

$$(1 - e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e.$$

By (**??**) we necessarily have $1 - e = 1$ which implies that $e = 0$.

We conclude that the only two values e can have are 0 and 1 depending on wether e is in $\mathfrak{m}$ or not. Thus the local ring A does not contain nontrivial idempotents. □

Exercise 14

Let A be a ring and

$$\Sigma = \{I \leq A \mid x \textbf{ is a zero divisor } \forall x \in I\}.$$

Show that Σ has maximal elements and that these maximal elements are prime. Thus the set of zerodivisors is a union of prime ideals.

Proof. First we use Zorn's Lemma: let $I_1 \subseteq I_2 \subseteq \cdots$ an ascending chain in Σ and define $I = \cup I_n$. Clearly $I \in \Sigma$, because for all $x \in I$ there is an $n \in \mathbb{N}$ such that $x \in I_n$ and thus it's a zerodivisor.

Let J be a maximal element of Σ and suppose there are $f, g \notin J$ such that $fg \in J$. Now consider the ideal $J_f = J + \langle f \rangle$ that properly contains J and $x \in J_f$ of the form $x = j + \lambda f$ for some $\lambda \in A$. If we multiply this equation by g we have $xg = jg + \lambda fg \in J$ so that xg is a zerodivisor, so that there is a $\mu \in A$, $\mu \neq 0$ such that $xg\mu = 0$

Now suppose x is not a zero divisor, then $x\eta \neq 0$ for all $\eta \neq 0$. In particular, since $xg\mu = 0$ then necessarily $g\mu = 0$ so that g is a zero divisor.

Since the sum of zerodivisors is again a zerodivisor, we have that $J + \langle g \rangle$ consists of only zerodivisors, or in symbols $J + \langle g \rangle \in \Sigma$. However this contradicts the maximality of J, thus J must be a prime ideal.

Let D be the set of zerodivisors of A. Every element $x \in D$ generates an ideal $\langle x \rangle \in \Sigma$ which is contained in some maximal ideal of Σ. Thus $D \subseteq \cup I$ with $I \in \Sigma$ maximal. By definition each $I \subseteq D$ so that th other inclusion is also valid. We have thus proved that D is a union of prime ideals maximal in Σ.

□

Exercise 18

Let $X = \mathrm{Spec}\,(A)$ be endowed with the Zariski Topology. Prove the following

1. **The set $\{\mathfrak{m}\} \subseteq X$ is a closed point $\iff$ $\mathfrak{m}$ is maximal.**

2. **$\overline{\{\mathfrak{p}\}} = \mathbb{V}(\mathfrak{p})$**

3. **$\mathfrak{q} \in \overline{\{\mathfrak{p}\}} \iff \mathfrak{p} \subseteq \mathfrak{q}$.**

4. **X is a T_0-space (that is for all $\mathfrak{p} \neq \mathfrak{q}$ in X there exists an open neigborhood of $\mathfrak{p}$ which does not contain $\mathfrak{q}$ or vice versa).**

5. **$\mathrm{Spec}\,(A)$ is Hausdorff iff every prime ideal of A is maximal.**

Proof.

1. By the Zariski topology, $\{\mathfrak{m}\}$ is a closed set iff $\{\mathfrak{m}\} = \mathbb{V}(I)$ for some ideal $I \leq A$. This means that the only ideal that contains I is $\mathfrak{m}$. Thus $I = \mathfrak{m}$ and it is maximal. The other implication is trivial because $\mathbb{V}(\mathfrak{m}) = \{\mathfrak{m}\}$ since $\mathfrak{m}$ is maximal.

2. We will prove that $\mathbb{V}(\mathfrak{p})$ is the closure of the point-set $\{p\}$ by showing that any cloed set that contains $\{\mathfrak{p}\}$ also contains $\mathbb{V}(\mathfrak{p})$. Let $W = \mathbb{V}(I) \subseteq X$ be a closed set, for some ideal $I \leq A$, such that $\mathfrak{p} \in W$. This means that $I \subseteq \mathfrak{p}$ and thus, for every element $\mathfrak{q} \in \mathbb{V}(\mathfrak{p})$ we have $I \subseteq \mathfrak{p} \subseteq \mathfrak{q}$ so that $\mathfrak{q} \in \mathbb{V}(I)$. Therefore $\mathbb{V}(\mathfrak{p}) \subseteq \mathbb{V}(I) = W$ and we are done.

3. Trivial consequence of the previous result.

4. Let $\mathfrak{p} \neq \mathfrak{q}$ be different points of X. Then, there is a $f \in (\mathfrak{p} - \mathfrak{q})$ and the open set $X_f = X - \mathbb{V}(f)$ is an open neighborhood of $\mathfrak{q}$ that does not contain $\mathfrak{p}$. Indeed: $f \notin \mathfrak{q}$ iff $\langle f \rangle \not\subseteq \mathfrak{q}$ iff $\mathfrak{q} \notin \mathbb{V}(f)$ or equivalently $\mathfrak{q} \in X_f$. Negating the previous equivalences we also conclude that $f \in \mathfrak{p}$ iff $\mathfrak{p} \notin X_f$. Thus X_f is the desired neighborhood.

5. In a Hausdorff space, point-sets are closed. Thus $\overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$ for every prime ideal $\mathfrak{p}$ of A and by (1) we conclude that every prime ideal is maximal.

   Now lets assume that every prime ideal is maximal, in particular $\mathrm{Jac}\,(A) = \sqrt{0}$. We must prove that every pair of distinct points $\mathfrak{m}, \mathfrak{n} \in X$ can be seperated by distinct open neighborhoods, that is the are open sets $U, V \subseteq X$ such that $\mathfrak{m} \in U$ and $\mathfrak{n} \in V$, but $U \cap V = \emptyset$.

   Take $\mathfrak{m} \neq \mathfrak{n}$ two maximal ideals.

□

2: Modules

Exercise 1

Let $n, m \in \mathbb{Z}$ be two coprime integers. Prove that $(\mathbb{Z}/n\mathbb{Z}) \otimes (\mathbb{Z}/m\mathbb{Z}) = 0$

Proof. We shall prove that the zero module 0 has the universal property of the tensor product. Let G be any $\mathbb{Z}$-module (ie. abelian group) and φ a bilinear map $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \to G$; we must prove that φ factors through the zero module, that is $\varphi \equiv 0$.

Since n and m are coprime integers, there exist integers $a, b \in \mathbb{Z}$ such that $an + bm = 1$. This equation impies that

$$1 \equiv an \mod m \quad , \quad 1 \equiv bm \mod n. \tag{4}$$

Furthurmore, the chinese Remainder Theorem (cf. Proposition 1.10) states that the ring homomorphism

$$\mathbb{Z} \xrightarrow{\phi} \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \quad x \mapsto (x + n\mathbb{Z}, x + m\mathbb{Z})$$

is surjective and has $nm\mathbb{Z}$ as its kernel; thus

$$\frac{\mathbb{Z}}{nm\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

We can therefore compose this isomporphism with φ to produce a homomorphism $\hat{\varphi} : \mathbb{Z}/nm\mathbb{Z} \to G$ that vanishes identically to φ.

Now let $x \in \mathbb{Z}$. With the equations (**??**) in mind, we can calculate:

$$\hat{\varphi}(x) = \varphi(x + n\mathbb{Z}, x + m\mathbb{Z}) = \varphi(xbm + n\mathbb{Z}, x + m\mathbb{Z}) = bm\varphi(x + n\mathbb{Z}, x + m\mathbb{Z}) = bm\hat{\varphi}(x).$$

and similarly $\hat{\varphi}(x) = an\hat{\varphi}(x)$. If we add both of these equations we get:

$$\hat{\varphi}(x) + \hat{\varphi}(x) = (an + bm)\hat{\varphi}(x) = \hat{\varphi}(x)$$

and by the cancellation law (G is an abelian group) we may conclude that $\hat{\varphi}(x) = 0$ for all $x \in \mathbb{Z}$. Thus $\varphi \equiv 0$ and indeed factors through the zero module. Therefore $(\mathbb{Z}/n\mathbb{Z}) \otimes (\mathbb{Z}/m\mathbb{Z}) = 0$. □

Remark. This exercise can easily be generalized to any ring A as follows: let I and J be two coprime ideals, that is $I + J = \langle 1 \rangle$. By the Chinese Remainder Theorem we have that $I \cap J = IJ$ and that $A/(I \cap J) \cong (A/I) \times (A/J)$. This means that the image of any A-bilinear map $(A/I) \times (A/J) \to M$ (where M is an A-module) is the image of the induced map $A \twoheadrightarrow A/(I \cap J) \cong (A/I) \times (A/J) \to G$ because $A \twoheadrightarrow A/(I \cap J)$ is surjective. Therefore the equation $i + j = 1$, with $i \in I$ and $j \in J$ can be used in exactly the same manner to prove that:

$$\frac{A}{I} \otimes_A \frac{A}{J} = 0 \quad \text{if } I \text{ and } J \text{ are coprime.}$$

Exercise 2

Let A be a ring, I an ideal and M an A-module. Prove that $(A/I) \otimes_A M \cong M/IM$.

Proof. Since tensoring by M is right-exact, then the exact sequence $0 \to I \to A \to A/I \to 0$ induces the exact sequence:

$$I \otimes_A M \longrightarrow A \otimes_A M \longrightarrow \left(\frac{A}{I}\right) \otimes_A M \longrightarrow 0.$$

Observe that $A \otimes M$ and M are canonically isomorphic as A-modules via the natural map $a \otimes x \mapsto ax$. Also, this map restricted to the A-submodule $I \otimes M$ has image IM and thus $I \otimes M \cong IM$. Our original exact sequence is therefore turned into:

$$IM \longrightarrow M \longrightarrow \left(\frac{A}{I}\right) \otimes M \longrightarrow 0.$$

By the exactness property,

$$\frac{M}{IM} \cong \left(\frac{A}{I}\right) \otimes M,$$

and we are done

□

Exercise 4

Let $\{M_i\}_{i \in I}$ be a family of A-modules and $M = \bigoplus M_i$ be their direct sum. Prove that question of flatness may be reduced to its direct summands, that is:

$$M = \bigoplus_{i \in I} M_i \textbf{ is flat} \qquad \Longleftrightarrow \qquad M_i \textbf{ is flat for all } i \in I.$$

Proof. □

3: Rings and Modules of Fractions

Exercise 6

Let A be a non zero ring and let Σ be the set of multiplicatively closed subsets $S \subset A$ such that $0 \notin S$. Show that

1. **Σ has maximal elements with respect to containment.**
2. **$S \in \Sigma$ is maximal $\iff$ $A - S$ is a minimal prime.**

Proof. 1. We will define a parcial order on Σ in order to apply Zorn's Lemma, but first we slightly generalize Σ in the following manner: let $X \subseteq A$ an arbitrary subset and define

$$\Sigma(X) := \{S \in \Sigma \mid X \subseteq S\}.$$

Observe that $\Sigma(\emptyset) = \Sigma$ so that $\Sigma(X)$ indeed generalizes Σ. Furthermore, it is possible that $\Sigma(X)$ can be empty, for example if $0 \in X$, but empty sets trivially have maximal elements so we may discard these cases from consideration. Finally observe that if $X \subseteq X'$ then $\Sigma(X') \subseteq \Sigma(X)$ and in particular $\Sigma(X) \subseteq \Sigma$ for all $X \subseteq A$.

Now we fix a subset $X \subseteq A$ and define a partial order on $\Sigma(X)$. Set $S \leq S'$ if and only if $S \subseteq S'$ and let $\mathcal{C}$ be the ascending chain $S_1 \subseteq S_2 \subseteq \cdots$ in $\Sigma(X)$. Cleary the set $\bar{S} := \cup S_n$ is an upper bound to the chain $\mathcal{C}$. To apply Zorn's Lemma we must prove that $\bar{S} \in \Sigma(X)$. We assert that this is true:

- Since $S_n \in \Sigma$ for all $n > 0$, then $O \notin S_n$ for all n and thus $0 \notin \bar{S}$.
- Suppose $s, t \in \bar{S}$, then $s \in S_n$ and $t \in S_m$ for some $n, m > 0$. If $N = \max\{n, m\}$, then $S_n, S_m \subseteq S_N$ son that $s, t \in S_N$. Since S_N is multiplicatively closed we conclude that $st \in S_N \subseteq \bar{S}$ and thus $\bar{S}$ is multiplicatively closed.
- Since $X \subseteq S_n$ for all $n > 0$ by hypothesis then clearly $X \subseteq \bar{S}$.

Now that we have $\bar{S} \in \Sigma(X)$, we may conclude that every ascending chain $\mathcal{C}$ in $\Sigma(X)$ has an upper bound $\bar{S}$ in $\Sigma(X)$. By Zorn's Lemma we conclude that $\Sigma(X)$ has maximal elements. In particular Σ has maximal elements.

2. We prove both implications:

($\Longrightarrow$) Let $S \in \Sigma$ be a maximal element. For now, let us assume that $A - S$ is an ideal of A; we will prove this at the end. It is clearly a prime ideal because if $a, b \in A$ then

$$a, b \notin A - S \quad \iff \quad a, b \in S \quad \stackrel{*}{\Longrightarrow} \quad ab \in S \quad \iff \quad ab \notin A - s,$$

where (*) follows from S being a multiplicative set. $A - S$ is also minimal among primes because if $\mathfrak{p} \subseteq A - S$ is a prime ideal, then $S \subseteq A - \mathfrak{p}$ and since $A - \mathfrak{p}$ is multiplicative by definition of prime ideales, then $A - \mathfrak{p} \in \Sigma$ (because $0 \in \mathfrak{p}$) and by the maximality of S we must have $S = A - \mathfrak{p}$ or equivalently $A - s = \mathfrak{p}$. We have thus proved that if $A - S$ is an ideal, then it is a prime ideal minimal among prime ideals. Thus we must only prove that $A - S$ is an ideal.

In order to prove that $A - S$ is an ideal, we characterize the elements of $A - S$ as follows: let $a \in A$, then whenever S is a maximal element of Σ then:

$$a \notin S \quad \iff \quad \frac{a}{1} \in \operatorname{Nil}(S^{-1}A). \tag{5}$$

Before we prove the above statement, we observer that it clearly implies that $A - S$ is an ideal. Indeed, if $a, b \in A - S$ and $c \in A$ are arbitrary, then $a/1, b/1 \in \mathrm{Nil}(S^{-1}A)$. Since $\mathrm{Nil}(S^{-1}A)$ is an ideal of $S^{-1}A$ then $a/1 - b/1 = (a-b)/1$ and $c/1 \cdot a/1$ are both elements of $\mathrm{Nil}(S^{-1}A)$. By (1) we conclude that $a - b, ca \in A - S$. Thus (1) proves that $A - S$ is an ideal and this finishes the proof of the second part.

In order to prove (1), first define the set $S_a \subseteq A$ as the product of the multiplicative sets S and $\{1, a, a^2, \ldots\}$. Cleary S_a is a multiplicative set. Since $1 \in S$ by definition, we have that $a \in S_a$. Additionally, since $1 \in \{1, a, a^2, \ldots\}$, then $S \subseteq S_a$. Therefore $a \notin S$ if and only if $S \subsetneq S_a$. On the other hand, by definiton $a/1 \in \mathrm{Nil}(S^{-1}A)$ if and only if $(a/1)^n = a^n/1 = 0/1$ for some $n > 0$. This equality happens in $S^{-1}A$ if and only if there exists an $s \in S$ such that $a^n s = 0$, but this is precisely the definition of 0 being an element of S_a. With these considerations we have just reduced the problem of proving (1) to proving:

$$S \subsetneq S_a \quad \Longleftrightarrow \quad 0 \in S_a. \tag{6}$$

It is clear that the direction ($\Longleftarrow$) follows from our hypothesis that $0 \notin S$. Suppose now that $0 \notin S_a$ so that, S_a being multiplicative, $S_a \in \Sigma$. However this contradicts the maximality of S because $S \subsetneq S_a$ and therefore we may conclude by contradiction that $0 \in S_a$. This concludes the proof of (1).

In conclusion, if S is maximal, then $A - S$ is an ideal by (1), it is a prime ideal because S is multiplicatively closed and it is minimal among primes becuase S is maximal.

($\Longleftarrow$) Suppose $A - S$ is a prime ideal minimal among prime ideals. Since $A - S$ is prime then S is multiplicatively closed. Indeed, if $s, t \in S$ then $s, t \notin A - S$ so that by primality $st \notin A - S$ and thus $st \in S$. Furthurmore since $1 \notin A - S$, then $1 \in S$ and therefore S is multiplicatively closed. Since $0 \in A - S$ we have $0 \notin S$ and thus $S \in \Sigma$.

Now suppose that $S' \in \Sigma$ is such that $S \subseteq S'$. In particular $S' \in \Sigma(S)$ and by the first part of the proof, there exists $S'' \in \Sigma(S)$, maximal among elements of $\Sigma(S)$. Now suppose that $S''' \in \Sigma$ is such that $S'' \subseteq S'''$, since $S \subseteq S'' \subseteq S'''$, then $S''' \in \Sigma(S)$ and by the maximality of S'' in $\Sigma(S)$ we have $S'' = S'''$ and thus S'' is a maximal element of Σ that contains S. By the part of the proof ($\Longrightarrow$) we have that $A - S''$ is a prime ideal and since $S \subseteq S' \subseteq S''$ implies $A - S'' \subseteq A - S' \subseteq A - S$ then $A - S''$ is a prime ideal contained in the minimal prime ideal $A - S$. Thus we must have $A - S'' = A - S$ and therefore $S = S''$ which implies that $S = S'$. This proves that S is a maximal element in Σ.

$\square$

(*Remark*) A consequence of exercise 6 is the following statement: Let D be the set of non zero zero-divisors of some ring A, then

$$\mathfrak{p} \subset A \text{ is a minimal prime ideal} \quad \Longrightarrow \quad \mathfrak{p} \subseteq D \cup \{0\}.$$

First set $S := A - \mathfrak{p}$ so that $A - S = A - (A - \mathfrak{p}) = \mathfrak{p}$; y exercise 6.2, S is a maximal element of Σ (since $A - (A - \mathfrak{p}) = \mathfrak{p}$). Also set $T := A - (D \cup \{0\})$ so that T es multiplicatively closed.[1]

Now suppose by contradiction that $\mathfrak{p} \not\subseteq D \cup \{0\}$, that is there exists $t \in \mathfrak{p}$ (i.e. $t \notin S$) such that $t \notin D \cup \{0\}$ (i.e. $t \in T$). That is $S \neq T$ and in particular the set $ST = \{st \mid s \in S, t \in T\}$ contains S because $1 \in T$ and the containment is strict because $t = 1 \cdot t \in ST - S$. Since $S \subsetneq ST$, then $0 \in ST$ becuase otherwise, $0 \notin ST$ would imply that $ST \in \Sigma$ which would contradict the maximality of S. Thus there exist $s \in S$ (i.e. $s \notin \mathfrak{p}$) and $t \in T$ (i.e. $t \notin D \cup \{0\}$) such that $st = 0$. However, since t is a non zero zero-divisor then necesarily $s = 0$, but this contradicts the choice of s because $0 \in \mathfrak{p}$. Thus the original assumption that $\mathfrak{p} \not\subseteq D \cup \{0\}$ cannot be true and thus $\mathfrak{p} \subseteq D \cup \{0\}$.

[1] To prove this take $a, b \in T$ (i.e. $a, b \notin D \cup \{0\}$) and suppose that $ab \notin T$ (i.e. $ab \in D \cup \{0\}$). If $ab = 0$, then a and b are both zero divisors since $a, b \neq 0$ by hypothesis. However this contradicts that $a, b \notin D$ and thus $ab \neq 0$ and we may assume that $ab \in D$. By definition there exists $c \in A - \{0\}$ such that $abc = a(bc) = b(ac) = 0$. Since $a, b \notin D \cup \{0\}$, we necesarrily have $bc = ac = 0$ and applying the same reasoning again we conclude that $c = 0$ which contradictions the choice of c. We may therefore conclude that $ab \in T$ and thus T is a multiplicatively closed set becuase in addition $1 \in T$ becuase $1 \notin D \cup \{0\}$ since $A \neq 0$.