Solutions for exercises, Algebra I (Commutative Algebra) – Week 6

Exercise 27. (Basic open sets)
Let $\mathfrak{p} \in \mathrm{Spec}(A_a)$, then $a \notin f^{-1}(\mathfrak{p})$ (otherwise, $f(a) \in \mathfrak{p}$ and since, by definition of the localization, $f(a)$ is invertible in A_a, we would get $\mathfrak{p} = (1)$; contradiction) i.e. $f^{-1}(\mathfrak{p}) \in D(a)$. So φ factorizes through $i : D(a) \hookrightarrow \mathrm{Spec}(A)$ i.e. $\varphi = i \circ \psi$ for a map $\psi : \mathrm{Spec}(A_a) \to D(a)$.
If $\mathfrak{q} \in D(a)$, then $f(\mathfrak{q})^e \in \mathrm{Spec}(A_a)$ and $f^{-1}(f(\mathfrak{q})^e) = \mathfrak{q}$ (i.e. ψ is surjective): indeed if $\frac{b}{a^k}\frac{c}{a^n} \in f(\mathfrak{q})^e$ we can write

$$\frac{b}{a^k}\frac{c}{a^n} = \frac{q}{a^m} \text{ in } A_a$$

for some $q \in \mathfrak{q}$ i.e. $a^\ell(a^m bc - qa^{k+n}) = 0$ in A for aome $\ell \geq 0$. So we have $a^{\ell+m}bc = a^{\ell+k+n}q \in \mathfrak{q}$; but since $a \notin \mathfrak{q}$ and $\mathfrak{q}$ is prime, we have $bc \in \mathfrak{q}$. Thus either $b \in \mathfrak{q}$ or $c \in \mathfrak{q}$ i.e. either $\frac{b}{a^k} \in f(\mathfrak{q})^e$ or $\frac{c}{a^n} \in f(\mathfrak{q})^e$. Moreover if $\frac{1}{1} \in f(\mathfrak{q})^e$ then we can write $\frac{1}{1} = \frac{q}{a^k}$ in A_a for some $k \geq 0$ and $q \in \mathfrak{q}$ i.e. $a^{k+m} = a^m q \in \mathfrak{q}$; but since $\mathfrak{q}$ is prime, we get $a \in \mathfrak{q}$; contradiction. So $\frac{1}{1} \notin f(\mathfrak{q})^e$. Thus $f(\mathfrak{q})^e \in \mathrm{Spec}(A_a)$.
Now, since $f(\mathfrak{q}) \subset f(\mathfrak{q})^e$, we have $\mathfrak{q} \subset f^{-1}(f(\mathfrak{q})^e)$. Conversely if $b \in f^{-1}(f(\mathfrak{q})^e)$ then $f(b) \in f(\mathfrak{q})^e$ i.e. $\frac{b}{1} = f(b) = \frac{q}{a^k}$ in A_a. Thus $a^{k+n}b = a^n q \in \mathfrak{q}$ and since $\mathfrak{q}$ is prime and $a \notin \mathfrak{q}$, $b \in \mathfrak{q}$. So $\mathfrak{q} = f^{-1}(f(\mathfrak{q})^e)$.

For any $\mathfrak{q} \in \mathrm{Spec}(A_a)$, $f(f^{-1}(\mathfrak{q}))^e = \mathfrak{q}$: indeed, we have by definition, $f(f^{-1}(\mathfrak{q})) \subset \mathfrak{q}$ so that $f(f^{-1}(\mathfrak{q}))^e \subset \mathfrak{q}$. Conversely, take $\frac{p}{a^k} \in \mathfrak{q}$, we have $\frac{p}{1} = a^k \frac{p}{a^k} \in \mathfrak{q}$ i.e. $f(p) = \frac{p}{1} \in \mathfrak{q}$. Thus $p \in f^{-1}(\mathfrak{q})$, consequently $\frac{p}{a^k} \in f(f^{-1}(\mathfrak{q}))^e$.
The map ψ is injective: indeed, if $f^{-1}(\mathfrak{p}_1) = f^{-1}(\mathfrak{p}_2)$ for $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Spec}(A_a)$. Then by the above discussion $\mathfrak{p}_1 = f(f^{-1}(\mathfrak{p}_1))^e = f(f^{-1}(\mathfrak{p}_2))^e = \mathfrak{p}_2$. Thus ψ is a bijection.

The open subset $D(a) \overset{i}{\subset} \mathrm{Spec}(A)$ is endowed with the induced topology (i.e. the open subsets of $D(a)$ are exactly of the form $i^{-1}(U)$ for an open subset U). By Lemma 9.9, φ is continuous and $\varphi = i \circ \psi$. So for an open subset $V \subset D(a)$, write $V = i^{-1}(U)$ for an open subset U thus $\psi^{-1}(V) = \psi^{-1}(i^{-1}(U)) = \varphi^{-1}(U)$ is an open set i.e. ψ is continuous.

Now let $D(\frac{b}{a^k}) \subset \mathrm{Spec}(A_a)$ be an open set with $b \in A$ and $k \geq 0$. We have $D(\frac{b}{1}) = D(\frac{b}{a^k})$ since a^k is invertible.
Then we have $\psi(D(\frac{b}{1})) = D(b) \cap D(a) = D(ab)$: indeed, if $\frac{b}{1} \notin \mathfrak{p}$ then $b \notin f^{-1}(\mathfrak{p})$ so $\psi(D(\frac{b}{1})) \subset D(b)$ and by definition of ψ, $\psi(D(\frac{b}{1})) \subset D(b) \cap D(a)$. Conversely, if $ab \notin \mathfrak{q}$ then if $\frac{ab}{1} \in f(\mathfrak{q})^e$, we have $\frac{ab}{1} = \frac{q}{a^m}$ for some $q \in \mathfrak{q}$ and $m \geq 0$ i.e. $a^{m+1+n}b = a^n q \in \mathfrak{q}$. Since $\mathfrak{q}$ is prime and does not contain a, we get $b \in \mathfrak{q}$; absurb. So $\frac{ab}{1} \notin f(\mathfrak{q})^e$. In particular $\frac{b}{1} \notin f(\mathfrak{q})^e$. Thus $\psi(D(\frac{b}{1})) = D(b) \cap D(a)$.
As a conclusion ψ is a bijective and open continuous map so it is a homeomorphism.

Exercise 28. (Consecutive localization)
As $A \backslash \mathfrak{p}_2 \subset A \backslash \mathfrak{p}_1$, for any $t \in A \backslash \mathfrak{p}_2$, $\frac{t}{1} \in A_{\mathfrak{p}_1}$ is invertible. So let us define $g : A_{\mathfrak{p}_2} \to A_{\mathfrak{p}_1}$ by $\frac{a}{t} \mapsto \frac{a}{t}$. It is a well-defined map: indeed if $\frac{a}{t} = \frac{a'}{t'}$ in $A_{\mathfrak{p}_2}$, we have $t''(at' - a't) = 0$ in A for

Solutions to be handed in before Monday May 18, 4pm.

some $t'' \in A\backslash\mathfrak{p}_2$; but since $t, t', t'' \in A\backslash\mathfrak{p}_2 \subset A\backslash\mathfrak{p}_1$, the equality $t''(at' - a't) = 0$ in A tells us that $\frac{a}{t} = \frac{a'}{t'}$ in $A_{\mathfrak{p}_1}$.
We have $g(1_{A_{\mathfrak{p}_2}}) = g(\frac{1}{1}) = \frac{1}{1} = 1_{A_{\mathfrak{p}_1}}$ and it is easy to check the rest of properties to show that g is a ring homomorphism.
Moreover given a $\frac{s}{t} \notin \mathfrak{p}_1 A_{\mathfrak{p}_2}$, we can choose a representant such that $s \in A\backslash\mathfrak{p}_1$ and $t \in A\backslash\mathfrak{p}_2$, then $g(\frac{s}{t}) = \frac{s}{t}$ is invertible in $A_{\mathfrak{p}_1}$ by definition. Thus $g(A_{\mathfrak{p}_2}\backslash\mathfrak{p}_1 A_{\mathfrak{p}_2}) \subset A^*_{\mathfrak{p}_1}$.
Let us prove that g is in fact the localization $A_{\mathfrak{p}_2} \to (A_{\mathfrak{p}_2})_{\mathfrak{p}_1 A_{\mathfrak{p}_2}}$. Consider a ring homomorphism $f : A_{\mathfrak{p}_2} \to B$ ($B \neq 0$) such that $f(A_{\mathfrak{p}_2}\backslash\mathfrak{p}_1 A_{\mathfrak{p}_2}) \subset B^*$ i.e. for any $s \in A\backslash\mathfrak{p}_1$ and $t \in A\backslash\mathfrak{p}_2$, $f(\frac{s}{t}) \in B^*$. Let us define $\overline{f} : A_{\mathfrak{p}_1} \to B$ by $\frac{a}{t} \mapsto f(\frac{a}{1})f(\frac{t}{1})^{-1}$. We know that $f(\frac{t}{1})$ is invertible for any $\frac{t}{1} \in A_{\mathfrak{p}_2}\backslash\mathfrak{p}_1 A_{\mathfrak{p}_2}$ and for $\frac{a}{t} = \frac{a'}{t'}$ in $A_{\mathfrak{p}_1}$ since $t''(at' - a't) = 0$ in A for some $t'' \in A\backslash\mathfrak{p}_1$, we get $f(\frac{t''}{1})(f(\frac{a}{1})f(\frac{t'}{1}) - f(\frac{a'}{1})f(\frac{t}{1})) = 0$ in B which, as $f(\frac{t''}{1})$ is invertible, can be written $f(\frac{a}{1})f(\frac{t'}{1}) = f(\frac{a'}{1})f(\frac{t}{1}) \in B$ and since $f(\frac{t}{1})$ and $f(\frac{t'}{1})$ are invertible in B, we get $f(\frac{a}{1})f(\frac{t}{1})^{-1} = f(\frac{a'}{1})f(\frac{t'}{1})^{-1}$ in B; so $\overline{f}$ is well-defined. It is not difficult to check that $\overline{f}$ is a ring homomorphism and for $\frac{a}{t} \in A_{\mathfrak{p}_2}$ ($t \in A\backslash\mathfrak{p}_2$), $\overline{f}(g(\frac{a}{t})) = \overline{f}(\frac{a}{t}) = f(\frac{a}{1})f(\frac{t}{1})^{-1}$ but since $\frac{t}{1} \in A_{\mathfrak{p}_2}$ is invertible we have $1 = f(\frac{1}{t}\frac{t}{1}) = f(\frac{1}{t})f(\frac{t}{1})$ i.e. $f(\frac{1}{t}) = f(\frac{t}{1})^{-1} \in B$. Thus $\overline{f}(g(\frac{a}{t})) = f(\frac{a}{1})f(\frac{t}{1})^{-1} = f(\frac{a}{t})$ i.e. $f = \overline{f} \circ g$.
Now, if $h : A_{\mathfrak{p}_1} \to B$ is a ring homomorphism such that $h \circ g = f$. Then for $a \in A$, $h(\frac{a}{1}) = h(g(\frac{a}{1})) = f(\frac{a}{1})$ in particular since for $t \in A\backslash\mathfrak{p}_1$, $f(\frac{t}{1})$ is invertible, $h(\frac{t}{1}) = f(\frac{t}{1})$ is invertible (and $\frac{t}{1} \in A_{\mathfrak{p}_1}$ is invertible, so $h(\frac{1}{t}) = f(\frac{t}{1})^{-1}$). Thus $h(\frac{a}{t}) = f(\frac{a}{1})f(\frac{t}{1})^{-1} = \overline{f}(\frac{a}{t})$ i.e. f factors uniquely through g.
So $g : A_{\mathfrak{p}_2} \to A_{\mathfrak{p}_1}$ satisfies the universal property of the localization $A_{\mathfrak{p}_2} \to (A_{\mathfrak{p}_2})_{\mathfrak{p}_1 A_{\mathfrak{p}_2}}$; thus it is the localization.

Exercise 29. (Comparing basic open sets)
If $\emptyset \neq D(a) \subset D(b)$ then $\{\mathfrak{p},\ a \notin \mathfrak{p}\} \subset \{\mathfrak{p},\ b \notin \mathfrak{p}\}$. If $\frac{b}{1} \in A_a$ is not a unit, it is contained in a maximal (thus prime) ideal $\mathfrak{m} \subsetneq A_a$. Using $D(a) \simeq \mathrm{Spec}(A_a)$ we see that $a \notin \mathfrak{m}$ (or more precisely the contraction of $\mathfrak{m}$ in A) but $b \in \mathfrak{m}$ (or more precisely the contraction of $\mathfrak{m}$ in A), contradicting $D(a) \subset D(b)$. Thus $\frac{b}{1} \in A_a$ is a unit.
Conversely, assume $\frac{b}{1} \in A_a$ is a unit (and $a \notin \mathfrak{N}$ otherwise $D(a) = \emptyset \subset D(b)$ is trivial). Let $a \notin \mathfrak{p}$ with $\mathfrak{p} \in \mathrm{Spec}(A)$. If $b \in \mathfrak{p}$, we get $\frac{ab}{1} \in \mathfrak{p}A_a$. But since $\frac{b}{1} \in A_a$ is a unit by assumption and $\frac{a}{1} \in A_a$ is a unit by construction of the localization, $\frac{ab}{1} \in \mathfrak{p}A_a$ tells that $\mathfrak{p}A_a$ is not a prime ideal (and $A_a \neq 0$ since $a \notin \mathfrak{N}$), contradicting $\mathrm{Spec}(A_a) \simeq D(a)$. Thus $b \notin \mathfrak{p}$ i.e. $D(a) = \{\mathfrak{p},\ a \notin \mathfrak{p}\} \subset D(b) = \{\mathfrak{p},\ b \notin \mathfrak{p}\}$.

If $\frac{b}{1} \in A_a$ is a unit, define $g : A_b \to A_a$ by $\frac{x}{b^k} \mapsto \frac{x}{1}(\frac{b^k}{1})^{-1}$. It is well-defined: if $\frac{x}{b^k} = \frac{y}{b^\ell}$ then $b^n(b^\ell x - b^k y) = 0 \in A$. In particular $\frac{b^n}{1}(\frac{b^\ell}{1}\frac{x}{1} - \frac{b^k}{1}\frac{y}{1}) = 0 \in A_a$ but since $\frac{b}{1}$ is a unit, $\frac{b^\ell}{1}\frac{x}{1} = \frac{b^k}{1}\frac{y}{1} \in A_a$. Thus $\frac{x}{1}(\frac{b^k}{1})^{-1} = \frac{y}{1}(\frac{b^\ell}{1})^{-1} \in A_a$.
It is a ring homomorphism: $g(1_{A_b}) = g(\frac{1}{1}) = \frac{1}{1} = 1_{A_a}$ and check additivity and g respects products.
Moreover $g(\frac{a}{1}) = \frac{a}{1} \in A_a$ is invertible in A_a. Denoting $f : A \to A_b$, a direct calculation shows that $g \circ f : A \to A_a$ is given by $x \mapsto \frac{x}{1}$.

If $D(a) = D(b)$ then $\frac{a}{1} \in A_b$ is invertible and $\frac{b}{1} \in A_a$ is also invertible. Let us prove that g is an isomorphism of rings. g injective: if $\frac{x}{1}(\frac{b^k}{1})^{-1} = g(\frac{x}{b^k}) = 0 \in A_a$ then since $\frac{b^k}{1}$ is a unit in A_a, $\frac{x}{1} = 0 \in A_a$ i.e. $a^n x = 0 \in A$ for some $n \geq 0$. Thus $\frac{a^n x}{1} = 0 \in A_b$. But $\frac{a^n x}{1} = (\frac{a}{1})^n \frac{x}{1}$ and $\frac{a}{1}$ is a unit in A_b, so $\frac{x}{1} = 0 \in A_b$. In particular $\frac{x}{b^k} = 0 \in A_b$ i.e. g is injective.
g surjective: since $\frac{a}{1} \in A_b$ is invertible, we get $1 = g(1) = g((\frac{a}{1})^{-1}\frac{a}{1}) = g((\frac{a}{1})^{-1})g(\frac{a}{1}) = g((\frac{a}{1})^{-1})\frac{a}{1}$ as g is a ring homomorphism. Thus $g((\frac{a}{1})^{-1}) = g(\frac{a}{1})^{-1} = (\frac{a}{1})^{-1} = \frac{1}{a} \in A_a$. So for $\frac{x}{a^k} \in A_a$, we have $g(((\frac{a}{1})^{-1})^k \frac{x}{1}) = g((\frac{a}{1})^{-1})^k \frac{x}{1} = \frac{1}{a^k}\frac{x}{1} = \frac{x}{a^k}$. Thus g is surjective.

[the wording of the exercise should have been more precise: $A_a \overset{f}{\simeq} A_b$ with $f(\frac{a}{1}) = \frac{a}{1}$ and $f^{-1}(\frac{b}{1}) = \frac{b}{1}$] Now assume that there is such a ring isomorphism $f : A_a \to A_b$. We have $\frac{a}{1}f(\frac{1}{a}) = f(\frac{a}{1})f(\frac{1}{a}) = f(\frac{a}{1}\frac{1}{a}) = f(1) = 1$ thus $\frac{a}{1}$ is a unit in A_b. By the first part of the exercise $D(b) \subset D(a)$.
Likewise, $\frac{b}{1}f^{-1}(\frac{1}{b}) = f^{-1}(\frac{b}{1})f^{-1}(\frac{1}{b}) = f^{-1}(\frac{b}{1}\frac{1}{b}) = f^{-1}(1) = 1$ thus $\frac{b}{1}$ is invertible in A_a. Using again the first part of the exercise $D(a) \subset D(b)$.

Exercise 30. (Disconnected Spec(A) and idempotents)
If Spec(A) is disconnected, we can write it as disjoint union of two closed subsets $\mathrm{Spec}(A) = V(\mathfrak{a}) \coprod V(\mathfrak{b})$ for $\mathfrak{a}, \mathfrak{b} \subset A$ ideals such that $V(\mathfrak{a}) \neq \emptyset$ and $V(\mathfrak{b}) \neq \emptyset$. So we have $\mathrm{Spec}(A) = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$ i.e. for any $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$ i.e. $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{N}$.
We have $\emptyset = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b})$ i.e. no prime ideal contains $\mathfrak{a} + \mathfrak{b}$; since any proper ideal is contained in a maximal (thus prime) ideal, $\mathfrak{a} + \mathfrak{b} = (1)$. So we can write $1 = a + b$, for a $a \in \mathfrak{a}$ and a $b \in \mathfrak{b}$. We have $ab \in \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{N}$ i.e. $(ab)^n = 0$ for some $n > 0$. Now, $1 = (a+b)^n = a^n + b^n + (ab)\underbrace{\sum_{i=1}^{n-1} a^{i-1}b^{n-i-1}}_{=y}$ and as aby is nilpotent, $1 - aby$ is invertible. Let us denote z its inverse. We have

$$za^n = (za^n)(\underbrace{z(1 - aby)}_{=1}) = (za^n)(z(a^n + b^n)) = (za^n)^2 + (z^2a^nb^n) = (za^n)^2.$$

So za^n is idempotent.
As $a \in \mathfrak{a} \subset \mathfrak{p}$ for at least one prime $\mathfrak{p} \in \mathrm{Spec}(A)$ ($V(\mathfrak{a}) \neq \emptyset$), $za^n \in \mathfrak{a}$ cannot be a unit (in particular cannot be 1). Moreover if $za^n = 0$, as z is invertible $a^n = 0$; thus $1 = b^n + (ab)y$ and aby is nilpotent. So b^n (in particular b) is a unit. Thus $\mathfrak{b} = (1)$; contradiction with $V(\mathfrak{b}) \neq \emptyset$. So za^n is an idempotent $\neq 0, 1$.

Conversely, if there is a $e \in A\backslash\{0,1\}$ idempotent, then $(1-e)^2 = 1 - 2e + e^2 = 1 - e$ so $1-e$ is also idempotent. We also have $(1-e)e = e - e^2 = 0$. Let us denote $p : A \to A/(e)$ the quotient by the principal ideal generated by e. Let us define $s : A/(e) \to A$ by $\overline{x} \mapsto (1-e)x$ where for $\overline{x} \in A/(e)$, $x \in A$ designates any element such that $p(x) = \overline{x}$. The map s is well-defined: if $p(y) = p(x) = \overline{x}$, we can write $y - x = ez$ for some $z \in A$; then

$$(1-e)y = (1-e)x + (1-e)ez = (1-e)x + 0 \cdot z = (1-e)x.$$

It is not difficult to check that s is a homomorphism of A-modules. Moreover

$$p \circ s(\overline{x}) = p((1-e)x) = p((1-e)x + ex) = p(x) = \overline{x}$$

as $ex \in \ker(p)$. Thus s is a section of the surjective homomorphism of A-modules p i.e. the exact sequence

$$0 \to (e) \to A \to A/(e) \to 0$$

splits i.e. $A = (e) \oplus A/(e)$ as A-modules. Now, we see that s identifies $A/(e)$ with the principal ideal $(1-e) \subset A$: by definition $\mathrm{im}(s) \subset (1-e)$ and the equality $p \circ s = \mathrm{id}_{A/(e)}$ shows that $p_{|(1-e)} : (1-e) \to A/(e)$ is surjective. If $x \in \ker(p) \cap (1-e)$ then $x = (1-e)y$ for some $y \in A$ and $p(x) = 0$ i.e. $x \in (e)$, so let us write $x = ez$ for some $z \in A$. Then

$$(1-e)x = (1-e)ez = 0 \text{ and } ex = e(1-e)y = 0 \text{ thus } x = (1-e)x + ex = 0. \qquad (*)$$

So $p_{|(1-e)}$ is injective i.e. induces an isomorphism of A-modules $(1-e) \simeq A/(e)$. So $A \simeq (e) \oplus (1-e) \simeq (e) \times (1-e)$ as A-modules. But for any $\overline{x}, \overline{y} \in A/(e)$, $s(\overline{xy}) = (1-e)xy = (1-e)^2xy = (1-e)x \cdot (1-e)y = s(\overline{x})s(\overline{y})$ and in particular $s(\overline{x}) = s(\overline{1 \cdot x}) = s(\overline{1})s(\overline{x}) = (1-e)s(\overline{x})$. So s

carries the ring structure of $A/(e)$ to $(1-e)$ with $1-e$ as the unity of $(1-e)$ (associativity and distributivity are inherited from the corresponding properties for $A/(e)$).
The ideal (e) as also a ring structure, e being the unity: for any $x, y \in A$, $ex \cdot ey = e^2xy = exy$ and in particular $e \cdot ex = e^2x = ex$ (associativity and distributivity are inherited from the corresponding properties for A).
Moreover, those ring structures are compatible with the ring structure of A:

$$xy = ((1-e)x + ex)((1-e)y + ey) = (1-e)^2xy + 2\underbrace{(1-e)e}_{=0}xy + e^2xy = (1-e)xy + exy.$$

Thus the decomposition $A \simeq (e) \times (1-e)$ is actually a decomposition as rings.

Now looking at $p : A \to A/(e)$ we have $\mathrm{Spec}(A/(e)) \simeq V(e)$. the projection on (e) is just given by $x \mapsto ex$. Whose kernel is $(1-e)$: if $ex = 0$ then $x = (1-e)x + ex = (1-e)x \in (1-e)$. On the other hand for any $y \in A$, $e(1-e)y = 0 \cdot y = 0$.
Thus $\mathrm{Spec}((e)) \simeq V((1-e))$. Since by (*), $(e) \cap (1-e) = 0 \subset \cap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$, we get $V(e) \cup V(1-e) = V((e) \cap (1-e)) = \mathrm{Spec}(A)$.
Moreover, $V(e) \cap V(1-e) = V((e) + (1-e))$ and $1 = e + (1-e) \in (e) + (1-e)$. Thus $(e) + (1-e) = A$ i.e. $V((e) + (1-e)) = \emptyset$. As a conclusion: $V(e) \coprod V(1-e) = \mathrm{Spec}(A)$.

Exercise 31. (Irreducible $\mathrm{Spec}(A)$)

- $\Leftarrow$ Since $(D(a))_{a \in A}$ is a basis of the Zariski topology, it is sufficient to see that $D(a) \cap D(b) \neq \emptyset$ for any pair of non-empty $D(a), D(b)$. So let $D(a) \neq \emptyset$ and $D(b) \neq \emptyset$. If $D(a) \cap D(b) = \emptyset$, we have $D(ab) = \emptyset$ i.e. $ab \in \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$ i.e. $ab \in \cap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathfrak{N}$. By assumption, either $a \in \mathfrak{N}$ or $b \in \mathfrak{N}$ i.e. either $D(a) = \emptyset$ or $D(b) = \emptyset$. Contradiction. Thus $D(a) \cap D(b) \neq \emptyset$.

- $\Rightarrow$ If $ab \in \mathfrak{N} = \cap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p}$, then $V(ab) = \mathrm{Spec}(A)$ i.e. $D(ab) = \emptyset$. But $D(ab) = D(a) \cap D(b)$. Since the Zariski topology on $\mathrm{Spec}(A)$ is irreducible, $D(a) = \emptyset$ or $D(b) = \emptyset$ which means $a \in \cap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathfrak{N}$ or $b \in \cap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \mathfrak{N}$. Thus $\mathfrak{N}$ is prime.

Exercise 32. (Idempotent ideals)

(i)$\Rightarrow$(ii) As $A/\mathfrak{a}$ is projective, it is in particular flat. We have the exact sequence

$$0 \to \mathfrak{a} \xrightarrow{i} A \xrightarrow{p} A/\mathfrak{a} \to 0 \tag{*}$$

and since $A/\mathfrak{a}$ is projective, the exact sequence splits

$$\begin{tikzcd} & & & A/\mathfrak{a} \arrow[dl, dashed] \arrow[d, "\mathrm{id}_{A/\mathfrak{a}}"] & \\ 0 \arrow[r] & \mathfrak{a} \arrow[r] & A \arrow[r] & A/\mathfrak{a} \arrow[r] & 0 \end{tikzcd}$$

i.e. $A \simeq \mathfrak{a} \oplus A/\mathfrak{a}$ as A-modules. So there is a (projection) surjective homomorphism of A-modules $\pi : A \to \mathfrak{a}$. Thus $\mathfrak{a}$ is finitely generated (by $\pi(1)$).

(ii)$\Rightarrow$(iii) By assumption $\mathfrak{a}$ is a finite A-module and since $\mathfrak{a}$ is an ideal, $\mathfrak{a}^2 = \mathfrak{a} \cdot \mathfrak{a} \subset \mathfrak{a}$. Now since $A/\mathfrak{a}$ is flat, tensoring the exact (*) with $A/\mathfrak{a}$ gives the exact sequence

$$0 \to \mathfrak{a} \otimes A/\mathfrak{a} \to A/\mathfrak{a} \stackrel{p \otimes \mathrm{id}}{\to} A/\mathfrak{a} \otimes_A A/\mathfrak{a} \to 0.$$

Now using the tensor identity (4) $M \otimes A/\mathfrak{a} \simeq M/\mathfrak{a}M$, we get $\mathfrak{a} \otimes_A A/\mathfrak{a} \simeq \mathfrak{a}/\mathfrak{a}^2$ and $A/\mathfrak{a} \otimes_A A/\mathfrak{a} \simeq A/\mathfrak{a}$. Moreover $p \otimes \mathrm{id} : A/\mathfrak{a} \simeq A \otimes A/\mathfrak{a} \to A/\mathfrak{a} \simeq A/\mathfrak{a} \otimes A/\mathfrak{a}$ is the identity $a \otimes p(b) = 1 \otimes a \cdot p(b) = p(a)p(b) = p(ab) \mapsto 1 \otimes p(ab) = p(ab)$. In particular its kernel is 0. But the exactness of the above sequence tells us that $\mathfrak{a}/\mathfrak{a}^2 = \ker(p \otimes \mathrm{id})$; thus $\mathfrak{a}/\mathfrak{a}^2 = 0$ i.e. $\mathfrak{a} = \mathfrak{a}^2$.

(iii)⇒(iv) Since the finite A-module, $\mathfrak{a}$ satisfies $\mathfrak{a}\cdot\mathfrak{a}=\mathfrak{a}$, Nakayama lemma (ii) gives us a $b\in 1+\mathfrak{a}$ such that $b\mathfrak{a}=0$. Write $b=1-\alpha$ with $\alpha\in\mathfrak{a}$. For any $a\in\mathfrak{a}$, we have $(1-\alpha)a=0$ i.e. $a=\alpha a$. Hence $\mathfrak{a}\subset(\alpha)$. But since $\alpha\in\mathfrak{a}$, $(\alpha)\subset\mathfrak{a}$ i.e. $\mathfrak{a}=(\alpha)$.
Moreover, we have in particular (since $\alpha\in\mathfrak{a}$) $\alpha=\alpha\cdot\alpha=\alpha^2$ i.e. α is idempotent.

(iv)⇒(v) We have the inclusion $i:\mathfrak{a}\subset A$ so we only have to define a projection $\beta:A\to\mathfrak{a}$ such that $\beta\circ i=\mathrm{id}_{\mathfrak{a}}$ to prove that $\mathfrak{a}$ is a direct summand. Let us define $\beta:A\to\mathfrak{a}=(e)$ by $a\mapsto ea$. It is obviously a homomorphism of A-modules and $p\circ i(ea)=p(ea)=e^2a=ea$. So β shows that $\mathfrak{a}$ is a direct summand.

(v)⇒(i) Let us denote $\beta:A\to\mathfrak{a}$ a projection (i.e. $\beta\circ i=\mathrm{id}_{\mathfrak{a}}$ for $i:\mathfrak{a}\hookrightarrow A$ the natural inclusion) exhibiting $\mathfrak{a}$ as direct summand. Then the exact sequence (*) splits: define $\alpha:A/\mathfrak{a}\to A$ by $\overline{a}\mapsto a-i(\beta(a))$ where for $\overline{a}\in A/\mathfrak{a}$, $a\in A$ designates any element such that $p(a)=\overline{a}$. It is well-defined: if $a,A'\in A$ satisfy $p(a)=p(a')$ then $a-a'\in\mathfrak{a}$ so we can write $a-a'=i(a-a')$; thus

$$a-a'-i(\beta(a-a'))=a-a'-i\circ\underbrace{\beta\circ i}_{=\mathrm{id}_{\mathfrak{a}}}(a-a')=a-a'-i(a-a')=0\in A$$

i.e. $a-i(\beta(a))=a'-i(\beta(a'))$.
It is easy to prove that α is a homomorphism of A-modules. Moreover for $\overline{a}\in A/\mathfrak{a}$, $p\circ\alpha(\overline{a})=p(a-\underbrace{i(\beta(a))}_{\in\mathfrak{a}})=p(a)=\overline{a}$ thus $p\circ\alpha=\mathrm{id}_{A/\mathfrak{a}}$.
So $A\simeq\mathfrak{a}\oplus A/\mathfrak{a}$ as A-modules. Thus $A/\mathfrak{a}$ is a direct summand of the free module A, as such it is projective.