

Exercises, Algebra I (Commutative Algebra) – Week 8

Exercise 38. (Going-up property, 3 points)

Let us begin by proving that for a prime ideal $\mathfrak{p} \in A$ the closure $\overline{\{\mathfrak{p}\}}$ of the point $\mathfrak{p} \in \text{Spec}(A)$ is $V(\mathfrak{p})$:

By definition, we have $\overline{\{\mathfrak{p}\}} = \bigcap_{\substack{C \subset \text{Spec}(A) \text{ closed} \\ \{\mathfrak{p}\} \subset C}} C$. In Zariski topology, we get $\overline{\{\mathfrak{p}\}} = \bigcap_{\mathfrak{a} \subset \mathfrak{p}} V(\mathfrak{a})$.

For any $\mathfrak{a} \subset \mathfrak{p}$, if $\mathfrak{q} \in V(\mathfrak{p})$ i.e. $\mathfrak{p} \subset \mathfrak{q}$, we have in particular $\mathfrak{a} \subset \mathfrak{q}$ hence $V(\mathfrak{p}) \subset V(\mathfrak{a})$. Thus $V(\mathfrak{p}) \subset \bigcap_{\mathfrak{a} \subset \mathfrak{p}} V(\mathfrak{a})$. Obviously $\mathfrak{p} \in V(\mathfrak{p})$ and $V(\mathfrak{p})$ is closed, so $\bigcap_{\mathfrak{a} \subset \mathfrak{p}} V(\mathfrak{a}) \subset V(\mathfrak{p})$ i.e.

$$V(\mathfrak{p}) = \bigcap_{\mathfrak{a} \subset \mathfrak{p}} V(\mathfrak{a}) = \overline{\{\mathfrak{p}\}}.$$

(\Leftarrow) Assume φ is closed. Let $\mathfrak{q} \in \text{Spec}(B)$ and set $\mathfrak{p} = \mathfrak{q}^c = \varphi(\mathfrak{q})$. Then $\varphi(V(\mathfrak{q}))$ is a closed subset of $\text{Spec}(A)$ containing \mathfrak{p} . Thus $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}} \subset \varphi(V(\mathfrak{q}))$. In particular, for any $\mathfrak{p} \subset \mathfrak{p}' \in \text{Spec}(A)$, the inclusion of ideals translates into $\mathfrak{p}' \in V(\mathfrak{p})$, which yields $\mathfrak{p}' \in \varphi(V(\mathfrak{q}))$ i.e. there exists a $\mathfrak{q}' \in V(\mathfrak{q})$ such that $\mathfrak{q}'^c = \mathfrak{p}'$.

(\Rightarrow) We want to prove that $\varphi(V(\mathfrak{b}))$ is a closed subset for any ideal $\mathfrak{b} \subset B$. First, if $\mathfrak{b} = \mathfrak{q}$ is a prime ideal, then setting $\mathfrak{p} = \varphi(\mathfrak{q}) = \mathfrak{q}^c$, we have the easy inclusion $\varphi(V(\mathfrak{q})) \subset V(\mathfrak{p})$. For a $\mathfrak{p}' \in V(\mathfrak{p})$ (i.e. $\mathfrak{p} \subset \mathfrak{p}'$), by the going-up property, we can find a $\mathfrak{q}' \in V(\mathfrak{q})$ such that $\mathfrak{p}' = \varphi(\mathfrak{q}')$. So $V(\mathfrak{p}) \subset \varphi(V(\mathfrak{q}))$ i.e. $\varphi(V(\mathfrak{q})) = V(\mathfrak{p})$. Thus $\varphi(V(\mathfrak{q}))$ is a closed subset of $\text{Spec}(A)$.

Let us prove that any Noetherian topological space can be written as a finite union of irreducible closed subsets: Let X be a Noetherian topological space. Let us denote S the set of closed subset of X not satisfying the property. If $S \neq \emptyset$, we can find a $V \in S$ which is minimal in S : indeed start with a V_1 not satisfying the property. If it is not minimal, we can find a closed subset $V_2 \subset V_1$ not satisfying the property and if V_2 is not minimal, we can repeat the procedure to get a descending chain of closed subsets $\dots V_n \subset \dots \subset V_2 \subset V_1$. Since X is Noetherian, the chain becomes stationary $V_n = V_k$ for any $k \geq n$. Then V_n is minimal.

Since V cannot be written as a finite union of irreducible closed subset, it is itself not irreducible so write it as $V = C_1 \cup C_2$ for two closed subsets satisfying $C_i \subsetneq V$, $i = 1, 2$. As V is minimal, $C_i \notin S$, $i = 1, 2$ so we can write $C_i = \bigcup_{k=1}^{n_i} W_{i,k}$ where $W_{i,k} \subset C_i$ are closed irreducible subsets. But then $V = \bigcup_{k=1}^{n_1} W_{1,k} \cup \bigcup_{k=1}^{n_2} W_{2,k}$, contradicting $V \in S$. Thus $S = \emptyset$.

In $\text{Spec}(A)$ (for any ring A), $V(\mathfrak{a})$ is an irreducible closed subset if and only if $\sqrt{\mathfrak{a}}$ is a prime ideal.

If $\sqrt{\mathfrak{a}}$ is a prime ideal, let $\mathfrak{a}_1, \mathfrak{a}_2$ be ideals such that $V(\sqrt{\mathfrak{a}}) = V(\mathfrak{a}) = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$. Then we have $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \sqrt{\mathfrak{a}_1 \cap \mathfrak{a}_2} = \sqrt{\mathfrak{a}}$. If $\mathfrak{a}_1 \setminus \sqrt{\mathfrak{a}} \neq \emptyset$ and $\mathfrak{a}_2 \setminus \sqrt{\mathfrak{a}} \neq \emptyset$ then take $a_1 \in \mathfrak{a}_1 \setminus \sqrt{\mathfrak{a}} \neq \emptyset$ and $a_2 \in \mathfrak{a}_2 \setminus \sqrt{\mathfrak{a}} \neq \emptyset$; we have $a_1 a_2 \in \mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \sqrt{\mathfrak{a}}$; contradicting $\sqrt{\mathfrak{a}}$ prime. Thus either $\mathfrak{a}_1 \subset \sqrt{\mathfrak{a}}$ (which yields $\sqrt{\mathfrak{a}_1} \subset \sqrt{\mathfrak{a}}$) or $\mathfrak{a}_2 \subset \sqrt{\mathfrak{a}}$ (which yields $\sqrt{\mathfrak{a}_2} \subset \sqrt{\mathfrak{a}}$). Together with $V(\mathfrak{a}_i) \subset V(\mathfrak{a})$ (by assumption), we get $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}_1}$ or $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}_2}$ i.e. $V(\mathfrak{a}) = V(\mathfrak{a}_1)$ or $V(\mathfrak{a}) = V(\mathfrak{a}_2)$.

Conversely, if $\sqrt{\mathfrak{a}}$ is not prime, take $a, b \notin \sqrt{\mathfrak{a}}$ such that $ab \in \sqrt{\mathfrak{a}}$. As $a \notin \sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \text{Spec}(A), \mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$ there is a prime ideal $\mathfrak{p}_a \subset \mathfrak{p}_a$ not containing a . Thus $(a) + \mathfrak{a} \subsetneq \mathfrak{p}_a$, in particular $V((a) + \mathfrak{a}) \subsetneq V(\mathfrak{a})$. Likewise, $V((b) + \mathfrak{a}) \subsetneq V(\mathfrak{a})$. But $V((a) + \mathfrak{a}) \cup V((b) + \mathfrak{a}) = V(((a) + \mathfrak{a}) \cdot ((b) + \mathfrak{a})) = V((ab) + \mathfrak{a}) = V(\mathfrak{a})$. So $V(\mathfrak{a})$ is not irreducible.

Putting things together, let $V(\mathfrak{b}) \subset \text{Spec}(B)$ be closed subset. As B is Noetherian, B/\mathfrak{b} is also Noetherian. So $V(\mathfrak{b}) \simeq \text{Spec}(B/\mathfrak{b})$ is a Noetherian topological space and as such can be written as a finite union of irreducible closed subsets, which, by the discussion above, are of the form $V(\mathfrak{q})$ for some prime ideal $\mathfrak{b} \subset \mathfrak{q}$. So we can find prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ containing \mathfrak{b} such that $V(\mathfrak{b}) = \cup_{i=1}^n V(\mathfrak{q}_i)$. Then $\varphi(V(\mathfrak{b})) = \varphi(\cup_{i=1}^n V(\mathfrak{q}_i)) = \cup_{i=1}^n \varphi(V(\mathfrak{q}_i))$ which is closed as finite union of closed subsets (by the first point) $V(\mathfrak{q}_i^c)$.

Exercise 39. (Cusp, 4 points)

First $y^2 - x^3$ is irreducible in $k(x)[y]$: indeed assume we can write $y^2 - x^3 = (y - p(x))(y - q(x))$; then $p(x) + q(x) = 0$ and $p(x)q(x) = -x^3$ i.e. $p(x) = -q(x)$ and $q(x)^2 = x^3 \in k(x)$; but x^3 is not a square in $k(x)$. So $y^2 - x^3$ is irreducible in $k(x)[y]$, a fortiori in $k[x, y]$. Thus $A = k[x, y]/(y^2 - x^3)$ is integral.

Since $x \notin (y^2 - x^3)$ (for degree reasons), $\bar{x} \neq 0$ in A thus $\frac{\bar{y}}{\bar{x}} \in Q(A)$. A direct calculation shows that $\frac{\bar{y}^2}{\bar{x}} - \bar{x} = \frac{\bar{y}^2 - \bar{x}^3}{\bar{x}} = 0$ so $T^2 - x \in A[T]$ annihilates $\frac{\bar{y}}{\bar{x}}$ i.e. $\frac{\bar{y}}{\bar{x}}$ is integral over A .

Assume $\frac{\bar{y}}{\bar{x}} \in A$; then there is a $p \in k[x, y]$ such that $\bar{p} \in A$ satisfies $\bar{p}^2 - \bar{x} = 0$ i.e. there is a $q \in k[x, y]$ such that $p^2 - x = (y^2 - x^3)q$. Looking at $(0, 0)$, we see that p has zero constant term.

Let us define, now $f : k[x, y] \rightarrow k[t]$, by $x \mapsto t^2, y \mapsto t^3$ (extend by k -algebra rules). By direct calculation $(y^2 - x^3) \subset \ker(f)$. So that $f(p)^2 - t^2 = 0$ in $k[t]$; which gives $f(p) = t$. But $\text{im}(f)$ contains no element of degree 1. So there is no such p i.e. $\frac{\bar{y}}{\bar{x}} \notin A$. Thus A is not normal. In particular, we cannot have $A \simeq k[t]$ as rings.

Now, let $p \in \ker(f)$, and let us write the division of p by $y^2 - x^3$ (in fact in $k(x)[y]$ and use that $y^2 - x^3$ is monic), $p = (y^2 - x^3)q + r$ in $k[x, y]$, with $\deg_y(r) \leq 1$. So we can write $r = r_1(x)y + r_2(x)$. Taking the image by f , we get $0 = f(p) = f(r) = r_1(t^2)t^3 + r_2(t^2)$; but any monomial of $r_1(t^2)t^3$ has odd degree and any monomial in $r_2(t^2)$ has even degree. Thus $r_2(t^2) = 0$ and $r_1(t^2) = 0$ so (writing down the coefficients) $r_1 = 0 = r_2$ i.e. $\ker(f) = (y^2 - x^3)$. Thus there is an induced injection $\bar{f} : A \hookrightarrow k[t]$.

We get from that and the universal property of localization (look at the composition $A \hookrightarrow k[t] \hookrightarrow k(t)$), a field extension (by abuse of notations, let us denote it the same way) $\bar{f} : Q(A) \hookrightarrow k(t)$. In $k[t] \hookrightarrow k(t)$, we have $t = \frac{\bar{f}(\bar{y})}{\bar{f}(\bar{x})} = \bar{f}(\frac{\bar{y}}{\bar{x}})$. Thus $t^2 - \bar{f}(\bar{x}) = 0$ in $k(t)$ i.e. t is algebraic over $Q(A)$. But since $T^2 - f(x) \in f(A)[T]$, the identity says that t is integral over $A \simeq f(A)$, so $A \hookrightarrow k[t]$ is integral (Prop 11.6).

We get a map $\varphi : \mathbb{A}_k^1 \rightarrow \text{Spec}(A) = V(y^2 - x^3) \subset \text{MaxSpec}(k[x, y])$.

Assume from now on, that k is algebraically closed.

For $\lambda \in k, x - \lambda^2, y - \lambda^3 \in f^{-1}((t - \lambda))$ since $t^2 - \lambda^2 = (t - \lambda)(t + \lambda)$ and $t^3 - \lambda^3 = (t - \lambda)(t^2 + \lambda t + \lambda^2)$. Thus $(x - \lambda^2, y - \lambda^3) \subset f^{-1}((t - \lambda))$. But $(x - \lambda^2, y - \lambda^3)$ is a maximal ideal in $k[x, y]$ so $(x - \lambda^2, y - \lambda^3) = f^{-1}((t - \lambda))$. Thus the restriction of φ to the MaxSpec is given by $\varphi' : \text{MaxSpec}(k[t]) \rightarrow \text{MaxSpec}(k[x, y]), \lambda \mapsto (\lambda^2, \lambda^3)$. It is easy to see that the fibers of φ' (once (λ^2, λ^3) given, $\lambda = \lambda^3/\lambda^2$) consist of one point when they are not empty. So we get a bijection $\varphi' : \text{MaxSpec}(k[t]) \simeq \text{MaxSpec}(A)$ but as we have seen by the failure of A to be normal A is not isomorphic to $k[t]$.

Exercise 40. (Ring of invariants, 3 points)

1. It was part of the solution of Exercise 35. Let us quickly repeat the argument (see last week's solutions): for $a \in A$, set $f = \prod_{g \in G} (x - g(a)) \in A[x]$ and is monic; it is a degree $|G|$ polynomial and $f(a) = a$ (as one of the $g \in G$ is the identity). As A is commutative, the coefficients of f are the evaluation of elementary symmetric functions in $|G|$ -variables at $(g(a))_{g \in G}$. For a $g_0 \in G, t_{g_0} : G \rightarrow G, g \mapsto g_0 \cdot g$ is a bijection because injective (G is a group) self-map of a finite set (thus surjective by cardinality). Since g_0 is a ring homomorphism (and as such respects sums and products), the coefficients of f are left invariant by g_0 ; and it is so, for any $g_0 \in G$ so the coefficients of f are, in fact, in A^G , which means $f \in A^G[x]$. Thus a is integral over A^G .

2. Let us first prove (by induction) the result stated as (corrected) hint: the case of one prime is obvious. Let $k \geq 1$, such that for any $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ prime ideals and an ideal \mathfrak{a} , $\mathfrak{a} \not\subset \mathfrak{p}_i, \forall i$ implies $\mathfrak{a} \not\subset \cup_{i=1}^k \mathfrak{p}_i$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_{k+1}$ be prime ideals (none being contained in another otherwise the induction hypothesis gives the result) and \mathfrak{a} an ideal such that $\mathfrak{a} \not\subset \mathfrak{p}_i$ for any i . By induction hypothesis, there is a $x \in \mathfrak{a} \setminus \cup_{i=1}^k \mathfrak{p}_i$. We claim that there is a $y \in (\mathfrak{a} \cdot \prod_{i=1}^n \mathfrak{p}_i) \setminus \mathfrak{p}_{k+1}$; otherwise $\mathfrak{a} \cdot \prod_{i=1}^n \mathfrak{p}_i \subset \mathfrak{p}_{k+1}$ but since no \mathfrak{p}_i is contained in \mathfrak{p}_{k+1} for any $i \leq k$, we can find $p_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{k+1}$; then for any $a \in \mathfrak{a}$, $a \cdot p_1 \cdots p_k \in \mathfrak{p}_{k+1}$ thus $a \in \mathfrak{p}_{k+1}$ i.e. $\mathfrak{a} \subset \mathfrak{p}_{k+1}$ contradiction. So we can choose $y \in \mathfrak{a} \cdot \prod_{i=1}^n \mathfrak{p}_i \setminus \mathfrak{p}_{k+1}$. Then $x + y \in \mathfrak{a}$ and if for some $i \leq k$, $x + y \in \mathfrak{p}_i$, then $x \in \mathfrak{p}_i$ contradiction. Thus $x, x + y \in \mathfrak{a} \setminus \cup_{i=1}^k \mathfrak{p}_i$. If $x \notin \mathfrak{p}_{k+1}$ then we have found an $x \in \mathfrak{a} \setminus \cup_{i=1}^{k+1} \mathfrak{p}_i$; otherwise $x \in \mathfrak{p}_{k+1}$ but then $x + y \notin \mathfrak{p}_{k+1}$ (otherwise $y \in \mathfrak{p}_{k+1}$; contradiction) i.e. we have found $x + y \in \mathfrak{a} \setminus \cup_{i=1}^{k+1} \mathfrak{p}_i$.

Now let $\mathfrak{q}_1, \mathfrak{q}_2 \in \varphi^{-1}(\mathfrak{p})$. For a $a \in \mathfrak{q}_1$, set $b = \prod_{g \in G} g(a)$; as $\text{id}_A \in G$, $b \in \mathfrak{q}_1$ and for any $g \in G$, $g(b) = \prod_{h \in G} g \circ h(a) = \prod_{h' \in G} h'(a) = b$ so $b \in A^G$ i.e. $b \in \mathfrak{q}_1 \cap A^G = \mathfrak{q}_1^c = \varphi(\mathfrak{q}_1) = \mathfrak{p}$. But we also have $\mathfrak{p} = \varphi(\mathfrak{q}_2) = \mathfrak{q}_2 \cap A^G$ thus $b = \prod_{g \in G} g(a) \in \mathfrak{q}_2$ i.e. (\mathfrak{q}_2 prime) $g_a(a) \in \mathfrak{p}_2$ for some $g_a \in G$. Thus $\mathfrak{q}_1 \subset \cup_{g \in G} g^{-1}(\mathfrak{q}_2)$. The $g^{-1}(\mathfrak{q}_2)$ are prime ideals so by the above discussion, there is a g such that $\mathfrak{q}_1 \subset g^{-1}(\mathfrak{q}_2)$. But we have $\mathfrak{q}_1 \cap A^G = \mathfrak{p} = \mathfrak{q}_2 \cap A^G = g^{-1}(\mathfrak{q}_2) \cap A^G$ so that by the 5th step of the proof of the Going-up theorem (Thm 11.33), we get $\mathfrak{q}_1 = g^{-1}(\mathfrak{q}_2)$, proving transitivity of G on $\varphi^{-1}(\mathfrak{p})$. So we have a surjective map $G \twoheadrightarrow \varphi^{-1}(\mathfrak{p})$, proving that $\varphi^{-1}(\mathfrak{p})$ is finite.

Exercise 41. (Circle as a spectrum, 4 points)

When $k = \mathbb{C}$. We can define the ring automorphism $\mathbb{C}[x, y] \rightarrow \mathbb{C}[x, y]$ given by $x \mapsto x - iy$, $y \mapsto x + iy$ (the inverse being defined by $x \mapsto (x + y)/2$, $y \mapsto (x - y)/2i$) by which we can see that we can take $x' = x + iy$ and $y' = x - iy$ as indeterminates (i.e. $\mathbb{C}[x', y'] \simeq \mathbb{C}[x, y]$). Under this change of variable, we have $x^2 + y^2 - 1 = (x + iy)(x - iy) - 1 = x'y' - 1$ so $A \simeq \mathbb{C}[x', y']/(x'y' - 1)$.

Let us define $g : \mathbb{C}[x'] \rightarrow \mathbb{C}[x', y']/(x'y' - 1)$ the composition of the natural ring homomorphisms. Then $g(x')$ is invertible since $g(x')\overline{y'} = 1$. Now for a $f : \mathbb{C}[x'] \rightarrow B$ a ring homomorphism such that $f(x') \in B^*$, define $\overline{f} : \mathbb{C}[x', y']/(x'y' - 1) \rightarrow B$ by $x' \mapsto f(x')$ and $y' \mapsto f(x')^{-1}$ (extend by ring rules). It is well defined because it is induced by the corresponding map $f' : \mathbb{C}[x', y'] \rightarrow B$ for which we see that $(x'y' - 1) \subset \ker(f')$. It is easy to check that it is a ring homomorphism through which f factorizes ($f = \overline{f} \circ g$). Moreover if $h : \mathbb{C}[x', y']/(x'y' - 1) \rightarrow B$ is another ring homomorphism such that $f = h \circ g$, we have $h(x') = h(g(x')) = f(x') = \overline{f}(x')$. Since $x' \in \mathbb{C}[x', y']/(x'y' - 1)$ is invertible (y' being its inverse), we have $h(y') = h(x'^{-1}) = h(x')^{-1} = f(x')^{-1} = \overline{f}(x')^{-1} = \overline{f}(x'^{-1}) = \overline{f}(y')$. Thus $h = \overline{f}$ proving uniqueness of the factorization of f through g . As a conclusion $g : \mathbb{C}[x'] \rightarrow \mathbb{C}[x', y']/(x'y' - 1)$ is the localization of $\mathbb{C}[x']$ with respect to $\{x'^k, k \geq 0\}$.

So we have a ring isomorphism $A \simeq \mathbb{C}[x']_{x'}$. But $\mathbb{C}[x']$ is factorial and the localization of a factorial ring is factorial.

When $k = \mathbb{R}$. One idea is to use again a polynomial ring with one variable. Euclidean division by the monic polynomial $x^2 + y^2 - 1$ yields that for any $f \in \mathbb{R}[x][y]$ ($\subset \mathbb{R}(x)[y]$) there is a unique $(f_1, f_2) \in \mathbb{R}[x]^2$ such that $f = f_1(x)y + f_2(x) \pmod{x^2 + y^2 - 1}$. Define $N : A \rightarrow \mathbb{R}[x]$ by $\overline{f} \mapsto (x^2 - 1)f_1(x)^2 + f_2(x)^2$. By the above uniqueness it is a well-defined map (not a ring

homomorphism at all). Moreover

$$\begin{aligned}
N((f_1(x)y + f_2(x))(g_1(x)y + g_2(x))) &= N(f_1g_1y^2 + (f_1g_2 + f_2g_1)y + f_2g_2) \\
&= N(f_1g_1(y^2 + x^2 - 1 - x^2 + 1) + (f_1g_2 + f_2g_1)y + f_2g_2) \\
&= N((f_1g_2 + f_2g_1)y + (1 - x^2)f_1g_1 + f_2g_2) \\
&= (x^2 - 1)(f_1g_2 + f_2g_1)^2 + ((1 - x^2)f_1g_1 + f_2g_2)^2 \\
&= (x^2 - 1)((f_1g_2)^2 + (f_2g_1)^2 + 2f_1f_2g_1g_2 + (f_1g_1)^2(x^2 - 1) \\
&\quad - 2f_1f_2g_1g_2) + (f_2g_2)^2 \\
&= N(f_1(x)y + f_2(x))N(g_1(x)y + g_2(x))
\end{aligned}$$

So N is multiplicative.

We have in A , $y^2 = 1 - x^2 = (1 - x)(1 + x)$. If $y|(1 - x)$ in A , then as N is multiplicative $x^2 - 1 = N(y)N(1 - x) = (1 - x)^2$ in $\mathbb{R}[x]$ which is not true so $y \nmid (1 - x)$. Likewise $y \nmid (1 + x)$, $(1 - x) \nmid y$ and $(1 + x) \nmid y$.

Let us prove moreover that $y \in A$ is irreducible: assume $y = fg$, then $x^2 - 1 = N(f)N(g)$ in $\mathbb{R}[x]$. If $\deg(N(f)) = 2$ then $N(g) \in \mathbb{R}^*$ i.e. there is a $a \in \mathbb{R}^*$ such that $g = a$ in A i.e. g is invertible. Likewise if $\deg(N(g)) = 2$, f is invertible. If $\deg(N(f)) = 1 = \deg(N(g))$, then ($\mathbb{R}[x]$ is factorial) $N(f), N(g) \in \{x - 1, x + 1\}$. Assume $N(f) = x + 1$ and write $f = f_1y + f_2$; we have $(x^2 - 1)f_1^2 + f_2^2 = N(f) = x + 1$ in $\mathbb{R}[x]$; thus $x + 1 | f_2^2$ i.e. $x + 1 | f_2$ (since $x + 1$ is irreducible) so either $\deg(f_2^2) \geq 4$ and its leading coefficient is positive or $f_2 = 0$. But the leading coefficient of $(x^2 - 1)f_1^2$ is also positive. But the sum $(x^2 - 1)f_1^2 + f_2^2$ has degree 1 = $\deg(x + 1)$ which is not possible. Using similar arguments for the case $N(f) = x - 1$, we get that y is irreducible.

Thus $y^2 = (1 - x)(x + 1)$ gives two distinct (with distinct irreducible elements) decompositions of y^2 ; in particular A is not factorial.

Exercise 42. (Extending ring homomorphisms into fields, 3 points)

Since $(0) \in \text{Spec}(K)$, the ideal $\mathfrak{p} := \ker(f) = f^{-1}(0)$ is prime; thus A/\mathfrak{p} is integral, $\bar{f} : A/\mathfrak{p} \rightarrow K$ is injective and f factorizes through \bar{f} .

Since $A \hookrightarrow B$ is integral, by the Going-up theorem (Thm 11.33), $\text{Spec}(B) \twoheadrightarrow \text{Spec}(A)$ is surjective so that there is a $\mathfrak{q} \in \text{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. Now the kernel of the composition $A \hookrightarrow B \rightarrow B/\mathfrak{q}$ is $\mathfrak{q} \cap A = \mathfrak{p}$ so there is an induced injective ring homomorphism $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ which, by the first step of the proof of the Going-up theorem, is integral.

Of course, B/\mathfrak{q} is integral so we can look at the natural injection $B/\mathfrak{q} \hookrightarrow Q(B/\mathfrak{q})$. We have an induced injection $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q} \hookrightarrow Q(B/\mathfrak{q})$ which, by the universal property of the localization (or of the fraction field) factorizes through $A/\mathfrak{p} \hookrightarrow Q(A/\mathfrak{p})$. Let us prove that the field extension $Q(B/\mathfrak{q})/Q(A/\mathfrak{p})$ is algebraic: Let $\frac{b}{d} \in Q(B/\mathfrak{q})$ then as B/\mathfrak{q} is integral over A/\mathfrak{p} , $A/\mathfrak{p}[d]$ is a finite A/\mathfrak{p} -module, hence $Q(A/\mathfrak{p})[d] \subset Q(B/\mathfrak{q})$ is a finite dimensional vector space. So $d \in Q(B/\mathfrak{q})$ is algebraic over $Q(A/\mathfrak{p})$; thus $d^{-1} \in Q(A/\mathfrak{p})[d]$ (mimic the proof of step 3 of the proof of the Going-up theorem). Thus $\frac{b}{d} \in Q(A/\mathfrak{p})[b, d] = Q(A/\mathfrak{p})[d][b] \subset Q(B/\mathfrak{q})$ but since b is integral over A/\mathfrak{p} it is in particular algebraic over $Q(A/\mathfrak{p})$, hence integral over $Q(A/\mathfrak{p})[d]$ i.e. $Q(A/\mathfrak{p})[d][b]$ is a finite $Q(A/\mathfrak{p})[d][b]$ -module hence $Q(A/\mathfrak{p})[b, d]$ is a finite dimensional $Q(A/\mathfrak{p})$ -vector space. As a consequence $\frac{b}{d} \in Q(A/\mathfrak{p})[b, d]$ is algebraic.

Now by the universal property of localization, the injective ring homomorphism $\bar{f} : A/\mathfrak{p} \hookrightarrow K$ factorizes through $A/\mathfrak{p} \hookrightarrow Q(A/\mathfrak{p})$ so we get a field extension $\overline{\bar{f}} : Q(A/\mathfrak{p}) \hookrightarrow K$. Since K is algebraically closed and $Q(B/\mathfrak{q})/Q(A/\mathfrak{p})$ is algebraic, by a classical result on field extension, there is a field extension $g : Q(B/\mathfrak{q}) \hookrightarrow K$ extending $\overline{\bar{f}}$.

Thus we have a commutative diagram:

$$\begin{array}{ccccccc} A & \longrightarrow & A/\mathfrak{p} & \hookrightarrow & Q(A/\mathfrak{p}) & \hookrightarrow & K \\ \downarrow & & \downarrow & & \downarrow & \nearrow & \\ B & \longrightarrow & B/\mathfrak{q} & \hookrightarrow & Q(B/\mathfrak{q}) & & \end{array}$$

(where the the composition of the map in the first line is equal to f) which gives us the extension.