

1. (a) This is clear if $R = K$. If not, choose $f \in R - K$ of degree $d > 0$, and replace f by a scalar multiple so that it has leading coefficient 1: say $f = x^d + c_{d-1}x^{d-1} + \cdots + c_0$. Then $x^d + c_{d-1}x^{d-1} + \cdots + c_0 - f = 0$ shows that x is integral over $K[f]$ and that $1, x, x^2, \dots, x^{d-1}$ span $K[x]$ as a $K[f]$ module, by a class result. (Or use induction on n to show that $x^n \in K[f]x^{d-1} + \cdots + K[f]x + K[f]$ for all n — the equation gives x^d , and, for the inductive step, multiply the expression for x^n by x and then substitute for the x^d term.) $K[f]$ is isomorphic to the polynomial ring in one variable over K , and is a PID. Therefore, since $K[x]$ is a finitely generated $K[f]$ -module, R is a finitely generated $K[f]$ -module: these generators along with f generate R over K .

(b) Let $f = x^3$, $g = x^4 + x$, and $h = x^5$. Then $g^2 = x^8 + 2x^5 + x^2$, and so $x^2 = g^2 - fh - 2h$. But then $x = g - (g^2 - fh - 2h)^2$.

2. Suppose that the closed sets in the family are $V(I_\lambda)$, $\lambda \in \Lambda$. The intersection is defined by the sum of the I_λ (which consists of all finite sums of elements from these ideals), and will be empty if and only if the sum is the unit ideal. But then $1 = i_1 + \cdots + i_n$ where $i_t \in I_{\lambda_t}$. But then $V(I_{\lambda_1}) \cap \cdots \cap V(I_{\lambda_n}) = \emptyset$, a contradiction.

3. Clearly, if $g = uf$ the g vanishes wherever f does. Conversely, if g vanishes wherever f does, define u to be $g(x)/f(x)$ when $f(x) \neq 0$ and 1 otherwise. Then $g = uf$. Note that if $f^{-1}(0) = g^{-1}(0)$ then u is a unit, so that $fR = gR$. This shows that if $f \in R$, the function g that is 1 where f is nonzero and 0 elsewhere is a unit times f , and $gR = fR$. Given any two functions f, g , choose units u and v such that uf and vg take on only the values 0 and 1. Then $uf + vg - (uf)(vg)$ vanishes precisely on $f^{-1}(0) \cap g^{-1}(0)$. This function generates the same ideal that f and g do. By induction, for functions $f_1, \dots, f_n \in R$ there is a function f that vanishes precisely where all of them do that is in the ideal they generate, and $fR = (f_1, \dots, f_n)R$. This shows that for any ideal I , the set of sets $f^{-1}(0)$ for f in I is a filter that uniquely determines I . Given \mathcal{F} , $\{f \in R : f^{-1}(0) \in \mathcal{F}\}$ is clearly an ideal, and distinct \mathcal{F} give distinct ideals. If X is finite there are only finitely many filters and, hence, finitely many ideals. If X is infinite it has an infinite strictly decreasing chain of subsets $X_1 \supset X_2 \supset \cdots$. Let \mathcal{F}_i be the filter of all sets containing X_i . This gives an infinite increasing chain of filters, and, hence, of ideals.

4. We prove much more. Note that any morphism $f : Y \rightarrow X$ gives a natural transformation T^f from h_X to h_Y : the needed map from $h_X(Z) = \text{Mor}(X, Z) \rightarrow \text{Mor}(Y, Z) = h_Y(Z)$ sends $g : X \rightarrow Z$ to $g \circ f$. Notice that the map $h_X(X) = \text{Mor}(X, X) \rightarrow \text{Mor}(Y, X) = h_Y(X)$ associated with T^f sends 1_X to f . The key point is that *every* natural transformation $T : h_X \rightarrow h_Y$ arises in this way, uniquely (uniqueness will be obvious, since we have already seen how to recover f from T_f). Given T , let $f = T_X(1_X) \in \text{Mor}(Y, X)$. For all Z , $T_Z : h_X(Z) = \text{Mor}(X, Z) \rightarrow h_Y(Z) = \text{Mor}(Y, Z)$. Fix $g : X \rightarrow Z$. Then the definition of a natural transformation yields a commutative diagram:

$$\begin{array}{ccc} \text{Mor}(X, X) & \xrightarrow{h_X(g)} & \text{Mor}(X, Z) \\ T_X \downarrow & & \downarrow T_Z \\ \text{Mor}(Y, X) & \xrightarrow{h_Y(g)} & \text{Mor}(Y, Z) \end{array}$$

the makes the diagram commute. We can compute the image of 1_X in $\text{Mor}(Y, Z)$ two ways. Using the top and right arrows, we get $T_Z(g \circ 1_x) = T_Z(g)$. Using the left and bottom arrows, we get $g \circ f$. Thus, $T_Z(g) = g \circ f$ always, which is exactly what we wanted to show. But then natural transformations $h_X \rightarrow h_Y$ and $h_Y \rightarrow h_X$ whose composition in either order is the identity natural transformation (from $h_X \rightarrow h_X$ or from $h_Y \rightarrow h_Y$) must come from morphisms $f : Y \rightarrow X$ and $f' : X \rightarrow Y$ whose composition in either order is the identity on X or Y .

5. Suppose that f is R -linear. Then $(r/s)f(m) = (r/s)f((s/s)m) = (r/s)sf((1/s)m) = rf((1/s)m) = f((r/s)m)$. \square

6. (a) Let $f = 1 - e$. We claim that the map $\alpha : R \rightarrow Re \times Rf$ with $\alpha(r) = (re, rf)$ is a ring isomorphism. That it is a homomorphism is completely straightforward, using that $e^2 = e$ and $f^2 = f$. The map $\beta : Re \times Rf \rightarrow R$ via $(re, r'f) \mapsto re + r'f$ is likewise easily checked to be a ring homomorphism, using that $e^2 = e$, $f^2 = f$, and $ef = 0$. $\beta(\alpha(r)) = re + rf = r(e + f) = r \cdot 1_R = r$, and $\alpha(\beta((re, r'f))) = \alpha(re + r'f) = ((re + r'f)e, (re + r'f)f) = (re, r'f)$. Re and Rf are nonzero because they contain e and f , respectively, both of which are not 0. \square

(b) Let e' be any lifting of e and $f' = 1 - e'$. Then $e' + f' = 1$, and $e'f' = u$ is nilpotent: mod N , it is $e(1 - e)$. Pick n such that $(e'f')^n = (e')^n(f')^n = 0$. First method: mod N , $(e')^n \equiv e^n = e$, and $(f')^n = f$. Thus, $u = (e')^n + (f')^n \equiv 1 \pmod{N}$. No prime P contains u (or $P \supseteq N$ and $1 \in P$), and so u has inverse v in R : $uv \equiv 1 \pmod{N}$ as well. (Or: $u = 1 + n$ with $n^s = 0$ implies $v = 1 - n + n^2 - \dots + (-1)^{s-1}n^{s-1}$ is u^{-1} .) Let $e^* = (e')^nv$ and $f^* = (f')^nv$. Then $e^*f^* = 0$, and $e^* + f^* = uv = 1$. Second method: raise both sides of the equation $e' + f' = 1$ to the N th power, where $N \geq 2n - 1$. Let e^* be the sum of all the terms on the left, including e'^N , where the exponent on e' is at least n . Let f^* be the sum of the remaining terms, one of which is f'^N ; all terms in f^* are divisible by f'^n . If we consider e^* mod N , we get e^N plus a sum of terms that are divisible by $e(1 - e)$ and so are 0. Thus, e^* mod N is e . By construction, $e^* + f^* = 1$. But every term in e^*f^* is divisible by $e'^nf'^n = 0$, and so $e^*f^* = 0$. Thus, e^* is idempotent. \square

(c) Since $e(1 - e) = 0$, every prime contains e or $1 - e$. No prime contains both, since $e + (1 - e) = 1$. $V(e)$ cannot be all of $\text{Spec}(R)$ unless e is nilpotent. But $e^n = e$ for all n , so that e is nilpotent if and only if $e = 0$. A similar comment applies to $V(1 - e)$. \square

For the converse, suppose that $V(I)$ and $V(J)$ are disjoint closed sets whose union is $\text{Spec}(R)$. Since no prime contains both I and J , $I + J = R$, and we can choose $e \in I$ and $f \in J$ such that $e + f = 1$. Since every prime contains I or contains J , every prime contains ef , i.e., ef is nilpotent. Since $V(e) \supseteq V(I)$ and $V(f) \supseteq V(J)$ while $V(e)$ and $V(f)$ are still disjoint, we must have $V(e) = V(I)$ and $V(f) = V(J)$. Since $V(I)$ is proper, e is not nilpotent, and similarly for f . By part (b) we may modify e by adding a nilpotent (and f by subtracting the same nilpotent) to obtain e' and f' that are idempotent with $f' = 1 - e'$. We have that $V(I) = V(e) = V(e')$ and $V(J) = V(f) = V(f')$, and that e' and f' are non-trivial idempotents. \square