Appendix B. Comparison with "classical" definition

In order to compare the given definition of schemes with the "classical" one, we will prove the following theorem:

Theorem 18. *Let $f : R \to S$ be a homomorphism between finitely generated rings so that for every finite ring A, the induced map $\mathrm{Hom}(S, A) \to \mathrm{Hom}(R, A)$ is a bijection. Then f is an isomorphism.*

In the paragraphs below R and S will always denote rings satisfying the conditions of the theorem. We first prove a special case:

Lemma 19. *Let $f : R \to S$ be a homomorphism of finite rings so that for every finite ring A the induced map $\mathrm{Hom}(S, A) \to \mathrm{Hom}(R, A)$ is a bijection. Then f is an isomorphism.*

Proof. Taking $A = R$ we see that there is a homomorphism $g : S \to R$ such that the composite $g \circ f : R \to S \to R$ is identity. For any finite ring A, consider the chain of maps

$$\mathrm{Hom}(R, A) \to \mathrm{Hom}(S, A) \to \mathrm{Hom}(R, A)$$

The second map is a bijection by assumption. The composite is the identity and in particular, a bijection. It follows that $\mathrm{Hom}(R, A) \to \mathrm{Hom}(S, A)$ is a bijection as well. Now, taking $A = S$ we see that we also have a homomorphism $h : R \to S$ so that the composite homomorphism $S \xrightarrow{g} R \xrightarrow{h} S$ is the identity. We then have

$$f = \mathrm{id}_S \circ f = h \circ g \circ f = h \circ \mathrm{id}_R = h$$

Thus $f \circ g = \mathrm{id}_S$ and $g \circ f = \mathrm{id}_R$, hence f and g are isomorphisms. □

Next, we show that the above condition is "inherited" by quotients.

Lemma 20. *Let $f : R \to S$ be as above. Let I be an ideal in R, then we obtain a homomorphism $R/I \to S/f(I)S$. For any finite ring A, the induced map $\mathrm{Hom}(S/f(I)S, A) \to \mathrm{Hom}(R/I, A)$ is a bijection.*

Proof. Consider the diagram

$$\begin{array}{ccc} \mathrm{Hom}(S, A) & \to & \mathrm{Hom}(R, A) \\ \uparrow & & \uparrow \\ \mathrm{Hom}(S/f(I)S, A) & & \mathrm{Hom}(R/I, A) \end{array}$$

The top row is a bijection. Let $g : S/f(I)S \to A$ be any element in the bottom left corner then the corresponding element $h : S \to A$ in the top left corner satisfies $h(f(I)S) = 0$. Thus $h \circ f : R \to A$ satisfies $h \circ f(I) = 0$. Thus it factors through a homomorphism $e : R/I \to A$. Thus we see that the elements in the bottom left corner are mapped to elements in the bottom right corner. Conversely, let $g : R/I \to A$ be an element in the bottom right corner and $h : R \to A$ be its image in the top right corner; then $h(I) = 0$. By assumption there is a homomorphism $e : S \to A$ such that $h = e \circ f$. It follows $e(f(I)) = 0$ and thus $e(f(I)S) = 0$. Thus e factors through an element $d : S/f(I)S \to A$ in the bottom left corner. In other words we have a bijection $\mathrm{Hom}(S/f(I)S, A) \to \mathrm{Hom}(R/I, A)$. □

Combining the above two lemmas we see that if I is any ideal in R such that R/I and $S/f(I)S$ are finite, then the map $R/I \to S/f(I)S$ is an isomorphism. We will now show that if R/I is finite then $S/f(I)S$ is "automatically" finite as well.

Lemma 21. *Let $f : R \to S$ be as in the theorem. For any maximal ideal m in R, the ideal $f(m)S$ in S also a maximal ideal.*

Proof. Since R is finitely generated R/m is a finite field by Hilbert's Nullstellensatz. Thus $\mathrm{Hom}(S, R/m) \to \mathrm{Hom}(R, R/m)$ is a bijection and so the homomorphism $R \to R/m$ must factor through S; moreover, this factorisation is unique. Let n be the kernel of this factorisation. Then n is a maximal ideal containing $f(m)S$ such that $R/m \to S/n$ is an isomorphism. Now, let n' be any maximal ideal in S containing $f(m)S$. Then, the composite $R \to S \to S/n'$ factors through R/m. Thus, S/n' is a finite field extension of R/m. If this extension has degree > 1 then if q is the cardinality of R/m, the map $x \mapsto x^q$ is a non-trivial automorphism of S/n' which is identity on R/m. Thus we obtain two maps $S \to S/n'$ which restrict to the same map $R \to S/n'$ contradicting the hypothesis. Thus $R/m \to S/n'$ is an isomorphism. But then this isomorphism gives a map $S \to R/m$ which restricts to the natural map $R \to R/m$; there is a unique such map by hypothesis. Since that map has kernel n, we see that $n' = n$.

In other words, we see that $f(m)S$ is contained in a unique maximal ideal n in S. Thus $S/f(m)S$ is an Artinian ring. By the earlier discussion we see that $R/m \to S/f(m)S$ is an isomorphism. In other words $f(m)S = n$ is a maximal ideal for every maximal ideal m in R. Conversely, if n is any maximal ideal in S, then $f^{-1}(n) = m$ is the kernel of the composite $R \to S \to S/n$ which is a map to a finite field; hence m is a maximal ideal. It follows that *every* maximal ideal in S is of the form $f(m)S$ for a maximal ideal m in R. □

Now, if I is any ideal such that R/I is finite then there are finitely many maximal ideals $m_1, \ldots, m_k$ and positive integers $r_1, \ldots, r_k$ such that $I \supset m_1^{r_1} \cdot m_2^{r_2} \cdots m_k^{r_k}$. As seen above $n_i = f(m_i)S$ is a maximal ideal. The relations

$$f(I)S \supset f(m_1^{r_1} \cdots m_k^{r_k})S = n_1^{r_1} \cdots n_k^{r_k}$$

shows that the ring $S/f(I)S$ is finite as well. It follows that for any ideal I such that R/I is finite, the map $R/I \to S/f(I)S$ is an isomorphism.

On the other hand suppose J is any ideal in S such that S/J is finite and let $I = f^{-1}(J)$; then R/I is a subring of S/J and thus also finite. We have seen above that this implies that $R/I \to S/f(I)S$ is an isomorphism. But the inverse image of $J/f(I)S$ under this is the zero ideal in R/I. Thus we have $J = f(I)S$. To summarise,

Lemma 22. *Let $f : R \to S$ be as in the conditions of the theorem. The map $I \mapsto f(I)S$ is a one-one correspondence between ideals of finite index in R and ideals of finite index in S. The map $J \mapsto f^{-1}(J)$ is the inverse correspondence from ideals J in S to ideals in R. Moreover, the natural homomorphism $R/I \to S/f(I)S$ is an isomorphism for such ideals.*

Thus the original condition has been re-stated intrinsically in terms of ideals. Next we wish to prove that the given homomorphism is "closed". That is to say given a prime ideal Q in S, let m be a maximal ideal in R that contains the prime ideal $P = f^{-1}(Q)$. We wish to prove that there is a maximal ideal n in S which contains Q and satisfies $f^{-1}(n) = m$. To do this we can restrict our attention to $R/P \to S/f(Q)S$. Since $f^{-1}(f(P)S) \subset f^{-1}(Q) = P$, the latter homomorphism is also injective.

Lemma 23. *Let $f : R \to S$ be an injective homomorphism of finitely generated rings with R a domain. We have a factoring of f as follows*

$$R \to R[X_1, \ldots, X_a] = R_1 \to R_1[t_1, \ldots, t_b] = R_2 \to S$$

where

(1) *R_1 is a polynomial ring over R.*
(2) *There is a non-zero element r of R_1 such that for each i, the element $rt_i \in R_2$ satisfies a monic polynomial over R_1. Other than this relation there are no further relations among the t_i in R_2.*
(3) *$R_2 \to S$ is the quotient by an ideal that intersects R_1 in the zero ideal.*

Proof. Since S is finitely generated we can choose a maximal collection of elements X_1, ..., X_a of S that are algebraically independent over (the quotient field of) R. Then $R_1 = R[X_1, \ldots, X_a]$ is the polynomial ring over R and is a subring of S. The remaining generators of S are algebraically dependent on the X_i's. Thus each of them satisfies an equation of the form $r_0T^d + r_1T^{d-1} + \cdots + r_d$ for some elements r_j in R_1. Moreover, we can assume that r_0 is non-zero in such an equation. Let r be the product in R_1 of polynomials r_0 corresponding to different generators of S. Since R is a domain, so is R_1 and the polynomial r is non-zero. For each generator S choose a polynomial of the above form with leading coefficient r (one such such clearly exists) and let R_2 be the ring obtained from R_1 by adjoining the roots of these equations. We have a natural map $R_2 \to S$; let $\mathfrak{a}$ be the kernel. Since $R_1 \to S$ factors through R_2 and is injective, it follows that $\mathfrak{a}$ intersects R_1 in the zero ideal. □

Let Q_1, ..., Q_r be the minimal primes in S or equivalently a minimal primes in R_2 that contains the kernel of $R_2 \to S$. Since R_1 meets this kernel in the zero ideal, the intersection of the prime ideals $Q_i \cap R_1$ in R_1 is a nilpotent ideal. Since R_1 is a domain there is an index i such that $Q_i \cap R_1 = (0)$. Let Q denote the prime ideal Q_i for any such index i.

Let m be a maximal ideal in R such that r is not contained in the prime ideal $m[X_1, \ldots, X_a]$ of R_1. Since R_1 is a domain we see that $Q_r \cap (R_1)_r$ is the zero ideal. Now, $(R_2)_r$ is a finite free module over $(R_1)_r$ and so (by the going up theorem) there is a prime ideal Q' in R_2 which contains Q and restricts to $m[X_1, \ldots, X_a]$ in R_1. Similarly, for any maximal ideal n' in R_1 that contains $m[X_1, \ldots, X_a]$ and does not contain r, there is a maximal ideal n in R_2 that contains Q' (and hence Q) that lies over n'.

Now, if $a > 0$ (i. e. $R \neq R_1$) then there are at least two (in fact infinitely many) such maximal ideals n'. But then we see that we have at least two maximal ideals in S that lie over a given maximal ideal m in R contradicting lemma 22. Thus we must have $R = R_1$.

Again, if $\tilde{Q}$ is another minimal prime in R_2 that contains the kernel of $R_2 \to S$ and such that $\tilde{Q} \cap R_1 = (0)$, then as above we can find a prime ideal $\tilde{Q}'$ which contains $\tilde{Q}$ and lies over m and is distinct from Q'. Now there are distinct maximal ideals n' and $\tilde{n}'$ in R_2, that contain Q' and $\tilde{Q}'$ respectively. This again contradicts lemma 22. It follows that there is a *unique* minimal prime Q containing the kernel of $R_2 \to S$ such that $Q \cap R = (0)$.

Now suppose that Q_0 is another miminal prime in S, or equivalently a minimal prime in R_2 that contains the kernel of $R_2 \to S$. We must have $Q_0 \cap R \neq (0)$. However, we have the lemma

Lemma 24. *Let $f : R \to S$ be a homomorphism of finitely generated rings with R a domain. Let Q be a minimal prime in S such that $f^{-1}(Q)$ is non-zero. Then there is a maximal ideal n in S and an integer k such that if $m = f^{-1}(n)$, then $R/m^k \to S/n^k$ is not an isomorphism.*

Proof. Let x be an element of all the minimal primes of S other than Q. Replacing S by its localisation S_x at x, we can assume that Q is the unique minimal prime in S. Then Q consists of nilpotent elements. Since $f^{-1}(Q)$ is non-zero and R is a domain it follows that $R \to S$ has a non-zero kernel. Now let n be *any* maximal ideal in S and $m = f^{-1}(m)$. The homomorphism of local rings $R_m \to S_n$ has a non-zero kernel. The result follows by the Artin-Rees lemma. □

On the other hand, for our given homomorphism $R \to S$ we know that $R/m^k \to S/n^k$ must be an isomorphism for all k. It follows that there is no such prime ideal Q_0 in S.

We have thus proved that there is a unique prime ideal Q in S that lies over a given prime ideal P in R and $f^{-1}(Q) = P$. The "closed"-ness condition is an immediate corollary.

Let us note that if $R[X]$ is the polynomial ring over a ring R, then $\mathrm{Hom}(R[X], A)$ is naturally identified with $\mathrm{Hom}(R, A) \times A$. Thus, if $g : R[X] \to S[X]$ denotes the natural extension of the above homomorphism to the corresponding polynomial rings then, for any finite ring the induced map $\mathrm{Hom}(S[X], A) \to \mathrm{Hom}(R[X], A)$ is a bijection whenever $\mathrm{Hom}(S, A) \to \mathrm{Hom}(R, A)$ is a bijection. In particular, we can apply the above lemmas to the homomorphism g as well.

Lemma 25. *Let $f : R \to S$ be as in the theorem and $g : R[X] \to S[X]$ be the induced homomorphism on polynomial rings in one variable. Let α be any element of S and $\mathfrak{b}$ be the ideal $(X - \alpha)S[X]$ in $S[X]$. Let $\mathfrak{a}$ be the ideal $g^{-1}((X - a)S[X])$. Then $\mathfrak{a}$ contains a* monic *polynomial.*

Proof. Let A be any ring and $\mathfrak{a}$ be an ideal in the polynomial ring $A[X]$. Let $\mathfrak{a}_1$ denote the ideal $\mathfrak{a} \cdot A[X, X^{-1}]$ in the ring $A[X, X^{-1}]$. We have

$$\mathfrak{a}_1 = \{P(X) \cdot X^{-n} | P(X) \in \mathfrak{a} \text{ and } n \geq 0 \text{ an integer } \}$$

Let $\mathfrak{a}_2$ be the restriction $\mathfrak{a}_1 \cap A[X^{-1}]$ of this ideal to $A[X^{-1}]$. We have

$$\mathfrak{a}_2 = \{P(X) \cdot X^{-d} | P(X) \in \mathfrak{a} \text{ and } d = \deg(P(X))\}$$

The *content* $c(\mathfrak{a})$ of the ideal $\mathfrak{a}$ is defined as the image of $\mathfrak{a}_2$ in $A[X^{-1}]/(X^{-1}) = A$. Clearly,

$$c(\mathfrak{a}) = \{a \in A | \exists P(X) \in \mathfrak{a} \text{ such that } P(X) = aX^d + \text{ lower degree terms } \}$$

Returning to the rings R and S let us use the subscripts 1 and 2 to denote the above constructions applied to ideals in $R[X]$ and $S[X]$; specifically to the ideals $\mathfrak{a}$ and $\mathfrak{b}$.

We want to show that the content $c(\mathfrak{a})$ of the ideal $\mathfrak{a}$ in $R[X]$ is the unit ideal. Suppose that $c(\mathfrak{a}) \subset m$ for some maximal ideal m in R. The ideal $\tilde{m} = m[X^{-1}] + X^{-1}R[X^{-}1]$ is then a maximal ideal in $R[X^{-1}]$ which contains $\mathfrak{a}_2$. Moreover, by the above description of $\mathfrak{a}_2$ it is clear that $\mathfrak{a}_2 = g_2^{-1}(\mathfrak{b}_2)$, where $g_2 : R[X^{-1}] \to S[X^{-1}]$ is the natural homomorphism. Applying the "going-up" which has been proved above, it follows that there should exist a prime ideal $\tilde{p}$ containing $\mathfrak{b}_2$ such that $g_2^{-1}(\tilde{p}) = \tilde{m}$. But $\mathfrak{b}_2$ is the ideal generated by $1 - \alpha X^{-1}$ and X^{-1} lies in $\tilde{m}$. Thus $\tilde{p}$

would have to be the unit ideal which contradicts its primality. It follows that $c(\mathfrak{a})$ is the unit ideal. $\square$

From this lemma we see that S is integral over R. Now the result that $R/m \to S/f(m)S$ is an isomorphism for all maximal ideals m implies theorem 18 by Nakayama's lemma.