September 29, 2005

see also pages 181-182 in
Documenta Mathematica, Extra Volume Suslin (2010).

Frank Grosshans has pointed out that the proof of sublemma A.5.1 is not convincing after the reduction to the affine case.

Let me take another way, much more slowly, making sure that this time there is an actual proof. If I remember correctly the argument below is basically the original one. Sometimes it is better not to simplify.

So we are at the stage where $Y = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$, $A \subset B$. Both $A$ and $B$ are of finite type over the algebraically closed field $k$ of characteristic $p > 0$, $B$ is finite over $A$, $X \to Y$ is bijective (between $k$ valued points). [We will not use that it is actually a bijection of scheme theoretic points.] Then sublemma A.5.1 claims that for all $b \in B$ there is an $m$ with $b^{p^m} \in A$. We will argue by induction on the Krull dimension of $A$.

Say $B$ as an $A$-module is generated by $d$ elements $b_1, \ldots, b_d$. Let $\mathfrak{p}_1$, $\ldots \mathfrak{p}_s$ be the minimal prime ideals of $A$.

Suppose we can show that for every $i$, $j$ we have $m_{i,j}$ so that $b_j^{p^{m_{i,j}}} \in A + \mathfrak{p}_i B$. Then for every $i$ we have $m_i$ so that $b^{p^{m_i}} \in A + \mathfrak{p}_i B$ for every $b \in B$. Then $b^{p^{m_1 + \cdots m_s}} \in A + \mathfrak{p}_1 \cdots \mathfrak{p}_s B$ for every $b \in B$. As $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ is nilpotent, one finds $m$ with $b^{p^m} \in A$ for all $b \in B$. The upshot is that it suffices to prove the sublemma for the inclusion $A/\mathfrak{p}_i \subset B/\mathfrak{p}_i B$. [It is an inclusion because there is a prime ideal $\mathfrak{q}_i$ in $B$ with $A \cap \mathfrak{q}_i = \mathfrak{p}_i$.] Therefore we further assume that $A$ is a domain.

Let $\mathfrak{r}$ denote the nilradical of $B$. If we can show that for all $b \in B$ there is $m$ with $b^{p^m} \in A + \mathfrak{r}$, then clearly we can also find an $u$ with $b^{p^u} \in A$. So we may as well replace $A \subset B$ with $A \subset B/\mathfrak{r}$ and assume that $B$ is reduced. But then at least one component of $\mathrm{Spec}(B)$ must map onto $\mathrm{Spec}(A)$, so bijectivity implies there is only one component. In other words, $B$ is also a domain.

Choose $t$ so that the field extension $\mathrm{Frac}(A) \subset \mathrm{Frac}(AB^{p^t})$ is separable. (So it is the separable closure of $\mathrm{Frac}(A)$ in $\mathrm{Frac}(B)$.) As $X \to \mathrm{Spec}(AB^{p^t})$ is also bijective, we have that $\mathrm{Spec}(AB^{p^t}) \to \mathrm{Spec}(A)$ is bijective. It clearly suffices to prove the sublemma for $A \subset AB^{p^t}$. So we replace $B$ with $AB^{p^t}$

and further assume that $\mathrm{Frac}(B)$ is separable over $\mathrm{Frac}(A)$.

Now the idea is that $X \to Y$ has a degree which is the degree of the separable field extension. But the degree must be one because of bijectivity.

Suppose, to contradict, $\mathrm{Frac}(B) \neq \mathrm{Frac}(A)$. Choose $b$ in $B$ outside $\mathrm{Frac}(A)$. It has a separable minimal polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over $\mathrm{Frac}(A)$, with $a_i \in A$. We localize to make it monic and then invert its discriminant: As $f$ is separable, there is a nonzero $s'$ in the intersection of $A$ with $f(x)A[x] + f'(x)A[x]$. Put $s = a_n s'$. The maps $\mathrm{Spec}(B[1/s]) \to \mathrm{Spec}(A[b][1/s])$ and $\mathrm{Spec}(A[b][1/s]) \to \mathrm{Spec}(A[1/s])$ are surjective and their composite is bijective, so both are bijective. The ring $A[b][1/s]$ is a free $A[1/s]$-module with basis 1, $b$, $\ldots b^{n-1}$. Choose $\phi : A[1/s] \to k$. We have that $A[b][1/s] \otimes_\phi k$ equals $k[x]/(\phi(a_n)x^n + \phi(a_{n-1})x^{n-1} + \cdots + \phi(a_0))$, which has more than one maximal ideal because the polynomial $\phi(a_n)x^n + \phi(a_{n-1})x^{n-1} + \cdots + \phi(a_0)$ is separable and $k$ is algebraically closed. We have arrived at the desired contradiction.

So we now are considering the case that $\mathrm{Frac}(B) = \mathrm{Frac}(A)$. Let Let $\mathfrak{c}$ be the conductor of $A \subset B$. So $\mathfrak{c} = \{ \ b \in B \mid bB \subset A \ \}$. We know it is nonzero. If it is the unit ideal then we are done. Suppose it is not. By induction applied to $A/\mathfrak{c} \subset B/\mathfrak{c}$ (we need the induction hypothesis for the original problem without any of the intermediate simplifications) we have that for each $b \in B$ there is an $m$ so that $b^{p^m} \in A + \mathfrak{c} = A$. We are done.

WvdK