Cohen's Theorem

Daniel Murfet

March 29, 2005

Before proceeding, one should consult our notes on Hensel's Lemma, where some subtle differences in definitions between Zariski & Samuel and Atiyah & Macdonald are discussed. In these notes, a local ring is not assumed to be Noetherian and a ring is complete if every Cauchy sequence converges *and* the intersection $\cap_n \mathfrak{m}^n$ is zero (these follow A&M, not Z&S). However, with the conventions of Z&S the same statements with the same proofs are true. In Z&S local rings are Noetherian but completeness does not include the intersection requirement. But all we need is that A has one maximal ideal, limits for Cauchy sequences and $\cap_n \mathfrak{m}^n = 0$ - so either set of hypothesis will do.

Definition 1. Let A be a local ring A with maximal ideal $\mathfrak{m}$. We call A an *equicharacteristic* local ring if A has the same characteristic as its residue field $A/\mathfrak{m}$. A *field of representatives* for A is a subfield L of A which is mapped onto $A/\mathfrak{m}$ by the canonical mapping of A onto $A/\mathfrak{m}$. Since L is a field, the restriction of this mapping to L gives an isomorphism of fields $L \cong A/\mathfrak{m}$.

Lemma 1. *Let A be an equicharacteristic local ring with maximal ideal $\mathfrak{m}$ and characteristic $p \neq 0$. If $\mathfrak{m}^p = (0)$ then A admits a field of representatives.*

Proof. Let A^p be the set of all elements a^p where a ranges over A. Then A^p is obviously a subring of A. If a^p is any nonzero element of A, then since $\mathfrak{m}^p = (0)$ we must have $a \notin \mathfrak{m}$ and consequently a is a unit in A. If $ay = 1$ then y^p is an inverse for x^p in A^p, and therefore A^p is a *subfield* of A. Among all the subfields of A containing A^p, Zorn's Lemma produces a maximal subfield L. Let $\varphi : A \longrightarrow A/\mathfrak{m}$ be canonical. We claim that $\varphi(L) = A/\mathfrak{m}$.

Assume to the contrary that there is $\alpha \in A/\mathfrak{m}$ with $\alpha \notin \varphi(L)$. Since $\alpha^p \in \varphi(A^p) \subseteq \varphi(L)$ the minimal polynomial of α over $\varphi(L)$ is $x^p - \alpha^p$ (see our notes on purely inseparable extensions). Let $a \in A$ be a representative of α, $\varphi(a) = \alpha$. Then $a \notin L$ and the isomorphism $L \cong \varphi(L)$ induces a chain of ring isomorphisms

$$L[a] \cong L[x]/(x^p - a^p) \cong \varphi(L)[x]/(x^p - \alpha^p) \cong \varphi(L)(\alpha)$$

Hence $L[a]$ is a subfield of A, contradiciting the maximality of L. We conclude that $\varphi(L) = A/\mathfrak{m}$, completing the proof. □

Theorem 2. *An equicharacteristic complete local ring A admits a field of representatives.*

Proof. In the case in which A and $A/\mathfrak{m}$ both have characteristic 0 the Theorem has already been proved in a Corollary to Hensel's Lemma. So we may assume that the characteristic of A and $A/\mathfrak{m}$ is a prime $p \neq 0$.

Since $p \geq 2$ the maximal ideal $\overline{\mathfrak{m}} = \mathfrak{m}/\mathfrak{m}^2$ of the local ring $A/\mathfrak{m}^2$ satisfies the condition $\overline{\mathfrak{m}}^p = (0)$. Clearly $A/\mathfrak{m}^2$ satisfies the other conditions of the Lemma, so $A/\mathfrak{m}^2$ admits a field of representatives K_2. For $n \geq 1$ let ψ_n denote the canonical map $A/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}^n$, and notice that

$$\psi_n^{-1}(\mathfrak{m}/\mathfrak{m}^n) = \mathfrak{m}/\mathfrak{m}^{n+1} \tag{1}$$

For $n \geq 2$ the ring $A/\mathfrak{m}^n$ is an equicharacteristic local ring. We now construct by induction on $n \geq 2$, a representative field K_n of $A/\mathfrak{m}^n$ such that ψ_n induces an isomorphism of K_{n+1} onto K_n.

Suppose that K_n has already been constructed. The inverse image $\psi_n^{-1}(K_n)$ is a subring R of $A/\mathfrak{m}^{n+1}$ which contains the kernel $\mathfrak{p} = \mathfrak{m}^n/\mathfrak{m}^{n+1}$ of ψ_n. Let ξ be any element of R not in $\mathfrak{a}$.

Then the image ξ' of ξ under ψ_n is a nonzero element of K_n, and consequently is a unit in $A/\mathfrak{m}^n$. Hence $\xi' \notin \mathfrak{m}/\mathfrak{m}^n$, and it follows from (1) that $\xi \notin \mathfrak{m}/\mathfrak{m}^{n+1}$, so ξ is a unit in $A/\mathfrak{m}^{n+1}$. If η is the inverse of ξ in $A/\mathfrak{m}^{n+1}$ then $\psi_n(\eta) \in K_n$ and so by definition $\eta \in R$. Thus ξ is invertible in R and we have proved that R is a local ring with maximal ideal $\mathfrak{p}$. Since $\mathfrak{p} = \mathfrak{m}^n/\mathfrak{m}^{n+1}$ and $\mathfrak{m}^{2n} \subseteq \mathfrak{m}^{n+1}$ we have $\mathfrak{p}^2 = (0)$. Clearly both R and $R/\mathfrak{p} \cong K_n$ have characteristic p, so the Lemma shows the existence of a representative field K_{n+1} of R. Since $R/\mathfrak{p} \cong K_n$ it is easy to see that ψ_n induces an isomorphism of K_{n+1} onto K_n, and the canonical morphism $A/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}$ is the composition of ψ_n and $A/\mathfrak{m}^n \longrightarrow A/\mathfrak{m}$, so the fact that K_n is a representative field of $A/\mathfrak{m}^n$ implies that K_{n+1} is a representative field of $A/\mathfrak{m}^{n+1}$.

Since A is complete we have ring isomorphisms $A \cong \widehat{A} \cong \varprojlim A/\mathfrak{m}^n$. So given any sequence of elements $(\eta_n)_{n \geq 1}$ with $\eta_n \in A/\mathfrak{m}^n$ there is precisely one element $y \in A$ admitting η_n as an $\mathfrak{m}^n$-residue for all n. Set $K_1 = A/\mathfrak{m}$ and let $\eta = \eta_1$ be any element of K_1. Consider the elements

$$\eta_2 = \psi_1^{-1}(\eta_1), \quad \eta_3 = \psi_2^{-1}(\eta_2), \quad \ldots \quad \eta_{n+1} = \psi_n^{-1}(\eta_n), \quad \ldots$$

with $\eta_i \in K_i$ for all $i \geq 1$. Denote by $u(\eta)$ the unique element of A defined by this sequence. It is readily verified that $u(0) = 0, u(1) = 1$ and $u(\eta + \eta') = u(\eta) + u(\eta'), u(\eta\eta') = u(\eta)u(\eta')$, so $u(K_1)$ is a subring of A. Furthermore, for every $\eta \neq 0$ in K_1 there exists an element η' in K_1 such that $\eta\eta' = 1$ whence $u(\eta')$ is the inverse of $u(\eta)$ in $u(K_1)$. Therefore $u(K_1)$ is a subfield of A, and by construction $\varphi(u(K_1)) = K_1 = A/\mathfrak{m}$ where $\varphi : A \longrightarrow A/\mathfrak{m}$ is canonical, so we have found a representative field of A. □

The following is Proposition 10.24 of A&M and Theorem 7 in Section 3 of Ch. VIII in Z&S.

Lemma 3. *Let B be a ring, $\mathfrak{a}$ an ideal of B, M an B-module, (M_n) an $\mathfrak{a}$-filtration of M. Suppose that B is complete in the $\mathfrak{a}$-topology and that M is Hausdorff in its filtration topology. Suppose also that $G(M)$ is generated over $G(B)$ by a finite set of homogenous elements $\xi_1, \ldots, \xi_n$ of degrees $n(i)$. If $x_i \in M_{n(i)}$ is equal to ξ_i in $M_{n(i)}/M_{n(i)+1}$ then the elements $x_1, \ldots, x_n$ generate M over B.*

Corollary 4. *An equicharacteristic complete regular local ring A is either a field or has dimension $d \geq 1$ and is isomorphic to a formal power series ring over a field in d variables.*

Proof. A regular local ring of dimension zero is a field, so assume $d \geq 1$, let $\mathfrak{m}$ be the maximal ideal of A and let $a_1, \ldots, a_d$ be a regular system of parameters with $\mathfrak{m} = (a_1, \ldots, a_d)$. By the previous Theorem, A admits a representative field K. From our notes on Analytic Independence there is a morphism of rings

$$\varphi : K[[x_1, \ldots, x_d]] \longrightarrow A$$

which is injective by Corollary 2 to Theorem 21, Section 9 (see our Regular local ring notes). The subring $B = K[[a_1, \ldots, a_d]]$ of A is a complete regular local ring with maximal ideal $\mathfrak{n}$ generated by $a_1, \ldots, a_d$ (in B), so we have $\mathfrak{m} \cap B = \mathfrak{n}$. Considering A as a B-module, we are in the situation of the preceeding Lemma. We claim that $G_{\mathfrak{m}}(A)$ is generated as a $G_{\mathfrak{n}}(B)$-module by the homogenous element 1 of order zero. We have

$$G_{\mathfrak{n}}(B) = B/\mathfrak{n} \oplus \mathfrak{n}/\mathfrak{n}^2 \oplus \ldots$$
$$G_{\mathfrak{m}}(A) = A/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \ldots$$

It is standard that $G_{\mathfrak{m}}(A) = (A/\mathfrak{m})[a_1, \ldots, a_d]$. So it suffices to show that any monomial $ka_1^{n_1} \ldots a_d^{n_d}$ in the a_i (which is a homogenous element of order $\sum n_i$ in $G_{\mathfrak{m}}(A)$) belongs to the submodule generated by 1. But the a_i all belong to $\mathfrak{n}$ and since K is a representative field $B/\mathfrak{n} \cong K \cong A/\mathfrak{m}$, so we can manufacture such a monomial in $G_{\mathfrak{n}}(B)$ and simply multiply it by $1 \in G_{\mathfrak{m}}(A)$ to produce the desired result. The preceeding Lemma now implies that A is generated over B by 1, that is, $A = B$. So A is isomorphic to a formal power series ring over a field in d variables, as required. □