Math 711: Lecture of October 20, 2004

Proof that conditions (1), (5), (6), and (7) are equivalent. We show that (1) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (1). Suppose that the ring is Henselian and that we have a monic polynomial F such that mod $PR[x]$ the image f of F has a simple root $\lambda \in K$. This gives a factorization $f = (x - \lambda)g$, and the fact that λ is a simple root means that $x - \lambda$ and g are relatively prime. Hence, the factorization lifts to a factorization $F = (x - r)G$ where $r \equiv \lambda \bmod P$. But then $F(r) = 0$. This shows that (1) $\Rightarrow$ (5).

Now suppose that (5) holds, and let S be a pointed étale extension of R. Then S is a localization of standard étale extension of R near Q lying over P, and so $S = (R[x]_g/F)_Q$ where F is monic, F' is invertible in S, and Q lies over P. Let λ denote the image of x in the residue field of S, which is K. Thus, if f is the image of F modulo $PR[x]$, we have that $f(\lambda) = 0$, and since F' is invertible in S, its image $f'(\lambda)$ in K is nonzero, so that λ is a simple root of F. Thus, we can choose $r \in R$ such that $F(r) = 0$, and it follows that $F = (x-r)G(x)$ for $G \in R[x]$. Since λ is a simple root of f, the image of $G(x)$ is invertible in S, which means that S is a localization of $R[x]/(x - r) \cong R$. Since $R \to S$ is a local map, we must have that $R = S$. Thus, (5) $\Rightarrow$ (6).

Assume that we have condition (6) and consider a system of equations as in (7). Let Q be the kernel of the map $R[X_1, \ldots, X_n] \to K$ that agrees with the quotient surjection $R \twoheadrightarrow R/P = K$ on R and sends $X_j \mapsto \lambda_j$, $1 \leq j \leq n$. Then the hypothesis implies that $S = R[X_1, \ldots, X_n]_Q/(F_1, \ldots, F_n)$ is a pointed étale extension of R, using part (b) of the Proposition in the Lecture Notes of September 27, and is therefore equal to R. Solving the equations in R so as to lift the solution $(\lambda_1, \ldots, \lambda_n)$ is equivalent to giving an R-algebra mapping $R[X_1, \ldots, X_n]/(F_1, \ldots, F_n) \to R$ so that under the composite $R[X_1, \ldots, X_n]/(F_1, \ldots, F_n) \to R \twoheadrightarrow K$ the elements x_j map to the elements λ_j, which is equivalent to the condition that Q map into P. Thus, giving a lifting of the solution to R is equivalent to giving a local R-algebra mapping $S \to R$. Since $R \cong S$ as R-algebras, there is a unique such mapping, and so the equations have a unique solution.

Finally, assume that (7) holds, let $F \in R[x]$ be monic of degree n, and suppose we have a factorization $f = gh$ over $K[x]$ where g, h are monic of degrees d and e respectively and $d + e = n$. Let $g = \sum_{j=0}^{d} \alpha_j x^j$ with all $\alpha_i \in K$ and $\alpha_d = 1$, and let $h = \sum_{i=0}^{k} \beta_k x^k$ with all $\beta_k \in K$ and $\beta_e = 1$. We seek to lift this factorization to $R[x]$. Proceed by letting the coefficients of the factors be unknown, i.e., we seek values for $Y_0, \ldots, Y_{d-1}$ and $Z_0, \ldots, Z_{e-1}$ in R such that

$$F = (x^d + Y_{d-1}x^{d-1} + \cdots + Y_1 x + Y_0)(x^e + Z_{e-1}x^{e-1} + \cdots + Z_1 x + Z_0).$$

Let $F = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ where the c_i are given elements of R. This leads to a system of n equations in the $d + e = n$ unknowns Y_j, Z_k by setting the coefficient of x^t, expressed in terms of the Y_j, Z_k, equal to c_t, $0 \leq t \leq n - 1$. After transposing c_t to the other side of the equation, the typical equation looks like:

$$\sum_{j+k=t} Y_j Z_k - c_t = 0$$

where $Y_d = 1$ and $Z_e = 1$ (these are *not* indeterminates) and where $0 \le j \le \min\{d, t\}$ and $0 \le k \le \min\{e, t\}$. We want to solve so that $Y_j \equiv \alpha_j$, $Z_k \equiv \beta_k$, $0 \le j \le d-1$, $0 \le k \le e-1$.

Explicitly, the first two equations are $Y_0Z_0 - c_0 = 0$ and $Y_0Z_1 + Y_1Z_0 - c_1 = 0$, while the last equation is $Y_{d-1} + Z_{e-1} - c_{n-1} = 0$. Of course, the factorization of $f = gh$ gives a solution in K^n in which α_j is the image of Y_j and β_k is the image of Z_k. To complete the proof, it suffices to show that the Jacobian determinant of these n equations with respect to $Y_0, \ldots, Y_{d-1}, Z_0, \ldots, Z_{d-1}$, evaluated at the point $(\alpha, \beta) \in K^n$, is nonzero: condition (7) will then allow us to lift this solution to R^n, giving the required factorization.

Explicitly, the Jacobian matrix $\mathcal{J}$ is obtained by differentiating all of the polynomials we are setting equal to 0 by $Y_0, \ldots, Y_{d-1}$ and then $Z_0, \ldots, Z_{e-1}$. Each row is the sequence of partial derivatives with respect to one of the variables. The matrix is

$$\begin{pmatrix}
Z_0 & Z_1 & Z_2 & \cdots & Z_{e-1} & 1 & 0 & \cdots & 0 \\
0 & Z_0 & Z_1 & \cdots & Z_{e-2} & Z_{e-1} & 1 & \cdots & 0 \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
0 & 0 & \cdots & 0 & Z_0 & \cdots & Z_{e-2} & Z_{e-1} & 1 \\
Y_0 & Y_1 & Y_2 & \cdots & Y_{d-1} & 1 & 0 & \cdots & 0 \\
0 & Y_0 & Y_1 & \cdots & Y_{d-2} & Y_{d-1} & 1 & \cdots & 0 \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
 & & & & \cdots & & & & \\
0 & 0 & \cdots & 0 & Y_0 & \cdots & Y_{d-2} & Y_{d-1} & 1
\end{pmatrix}$$

There are d rows involving the Z_k and e rows involving the Y_j. Let $\mathcal{J}_0 = \mathcal{J}|_{(\alpha,\beta)}$ be this matrix after the α_j are substituted for the Y_j and the β_k for the Z_k.

Now consider instead the following problem: find polynomials u, v, not both 0, in $K[x]$ of degrees at most $e-1$ and $d-1$, respectively, such that $ug + vh = 0$. This problem has a solution if and only if g and h have a common factor w of positive degree. If they have such a factor, say w, for then we may write $g = vw$ and $h = -uw$ and we have that $ug + vh = 0$. On the other hand, if g and h have no common factor but we have $ug + vh = 0$ ($u = 0$ iff $v = 0$ here) then h divides u and g divides v, contradicting the degree bounds unless both vanish. Given g, h, we can look for u and v by letting their coefficients be unknowns. Suppose that $u = \sum_{k=0}^{e-1} B_k x^k$ and $v = \sum_{j=0}^{d-1} A_j x^j$. Setting the coefficients on powers of x equal to 0 gives a system of n linear equations in the n unknowns A_j B_k: the coefficients of these equations are functions of the coefficients α, β of g and h. Consider the $n \times n$ matrix $\mathcal{M}$ of this system of linear equations. The tth row may be thought of as the coefficients of A_j and B_k occurring in the coefficient of x^t in $ug + vh = 0$. Therefore, each column consists of the coefficients on some fixed A_j (or on some fixed B_k) as t varies. For A_j we get the coefficients in $A_j x^j h$, which is a row of $\mathcal{J}_0$. For B_k we get the coefficients in $B_k x^k g$, which is also a row of $\mathcal{J}_0$. With the columns suitably ordered, we see that $\mathcal{J}_0$ is the transpose of $\mathcal{M}$. Since g and h are relatively prime, the only element in the kernel of $\mathcal{M}$ is 0, so that $\mathcal{M}$ is invertible. Hence, $\mathcal{J}_0$ is invertible. $\square$

The determinant described in the proof above is an *eliminant* for f and g: when f and g are monic of fixed degrees but their non-leading coefficients are varying, it vanishes precisely on the set of n-tuples of non-leading coefficients such that f and g have a common factor (i.e., a common root in an algebraic closure of K), which shows that this set is Zariski closed. This is the classical approach to elimination theory, and has been largely hidden by recent methods. The theorem that a projective morphism is proper, i.e., gives a closed map even after base change, contains much the same sort of information. However, specific descriptions of the equations defining the closed sets are sometimes needed.

We want to construct the Henselization of the quasilocal ring R as the direct limit of all (up to isomorphism) pointed étale extensions of R. To make this idea precise, we need to study the category of pointed étale extensions of R. The following result contains the information we need.

Theorem. *Let (R, P, K) be a quasilocal ring and let S and T denote pointed étale R-algebras.*

(a) *If I is any proper ideal of R, then $R/I \to S/IS$ is a pointed étale extension.*
(b) *The maximal ideal of S is PS.*
(c) *There exists a pointed étale R-algebra U together with local R-algebra maps $S \to U$ and $T \to U$. In fact, one may take U to be $(S \otimes_R T)_Q$ where Q is the kernel of the composite R-algebra surjection $S \otimes_R T \twoheadrightarrow K \otimes_K K \cong K$.*
(d) *If $T = S$ in the construction in (c) just above, then $(S \otimes_R S)_Q \cong S$ via the obvious map that takes $(s \otimes s')/1$ to ss'.*
(e) *There is at most one local R-algebra homomorphism from S to T, and if there is such a homomorphism then T is pointed étale over S.*
(f) *If there are local R-algebra homomorphisms from S to T and from T to S then $S \cong T$ as local R-algebras. Moreover, this isomorphism is canonical.*
(g) *If the cardinality of R is finite so is the cardinality of S. In all other cases, R and S have the same cardinality. Therefore, there exists a set $\mathcal{R}$ of pointed étale extensions of R such that $\mathcal{R}$ contains exactly one representative from each isomorphism class of pointed étale extensions (isomorphism as local R-algebras). Moreover, $\mathcal{R}$ is partially ordered by the rule that $S \leq T$ if and only if there exists a local R-algebra map from S to T. With this partial ordering, $\mathcal{R}$ is a directed set.*

Proof. Part (a) is clear: this is base change so the map remains localized étale. It is clear that the map is still local and the the map of residue class fields does not change.

By part (b), S/PS is a pointed étale extension of the field $K = R/P$: since it is local, it is a field, and so $K \to S/PS$ must be an isomorphism. This proves (b).

To prove (c), first note that the statement that the tensor product of two étale algebras is étale is left as an exercise: cf. the first problem of Problem Set #2. The composite

$$R \to S \otimes_R T \to K \otimes_K K \to K$$

is isomorphic with the quotient surjection $R \twoheadrightarrow R/P = K$, and so $R \to (S \otimes_R T)_Q$ is local, and the induced map of residue class fields is an isomorphism.

Note that the map $S \otimes_R S \to S$ sends Q onto the maximal ideal of S, and is surjective. Since S is a localization of a finitely presented R-algebra, the kernel I of $S \otimes_R S \to S$ is a finitely generated ideal I_0, and since S is formally étale and therefore formally unramified over R, $I_0^2 = I_0$. Let $I = I_0(S \otimes_R S)_Q$, the kernel of the map $(S \otimes_R S)_Q \twoheadrightarrow S$. Then I is finitely generated and contained in the maximal ideal, and $I^2 = I$. It follows from Nakayama's lemma that $I = 0$, and so $(S \otimes_R S)_Q \to S$ is an isomorphism. This completes the proof of (d).

Suppose that there are two local R-algebra homomorphisms from $S \to T$, call them f and g. Then there is an R-algebra homomorphism $S \otimes_R S \to T$ that sends $s \otimes s' \mapsto f(s)g(s')$, and, with notation as in part (d), it carries Q into the maximal ideal of T and so induces a map $(S \otimes_R S)_Q \to T$ whose value on $s \otimes 1/1$ is $f(s)$ and whose value on $1 \otimes s/1$ is $g(s)$. But under the isomorphism of $(S \otimes_R S)_Q \cong S$ established in (d), both $s \otimes 1$ and $1 \otimes s$ map to s, i.e., $s \otimes 1/1 = 1 \otimes s/1$ in $(S \otimes_R S)_Q$. It follows that $f(s) = g(s)$, and this establishes the first statement in (e).

Now suppose that we have local R-algebra maps $R \to S \to T$ where S and T are pointed étale over R. We want to show that T is pointed étale over S. The module of differentials $\Omega_{T/S} = 0$ simply because $\Omega_{T/R} = 0$, and so T is formally unramified over S. It follows from the structure theory that we may write $T = U/I$ where U is a local ring of an étale S-algebra. We know that all of the residue class fields are isomorphic. Thus, to complete the proof, it will suffice to show that $I = 0$. We know that I is finitely generated. Consider the exact sequence $0 \to I \to U \to T \to 0$. Since T is R-flat, we have that $\mathrm{Tor}_1^R(K, T) = 0$. Therefore the sequence remains exact when we apply $K \otimes_R \_$, giving $0 \to I/PI \to U/PU \to T/PT \to 0$. Since U and T are both pointed étale over R, the map $U/PU \to T/PT$ is an isomorphism: these quotients are both K, by part (b). It follows that $I/PI = 0$, and then $I = (0)$ by Nakayama's lemma.

Part (f) is then immediate because the compositions of the two maps must be the respective identity maps on S and T: the only local R-algebra map from $S \to S$ (or $T \to T$) is the identity. The isomorphisms are obviously unique, since there is at most one local R-algebra map from $S \to T$ or $T \to S$.

Let $|\ \ |$ indicate cardinality. Then $|R[x]/(F)|$ is $|R|^n$ for F monic of degree n. Elements of $W^{-1}T$ are parametrized by $T \times W$ and so $|W^{-1}T| \leq |T|^2$. It follows that $|R| \leq |S| \leq |R|^{2n}$ for any pointed étale extension S of R (note that $R \hookrightarrow S$ here). Therefore, $|S|$ is finite if $|R|$ is and $|S| = |R|$ otherwise. The existence of the set $\mathcal{R}$ is then immediate from the axiom of choice. The relation $\leq$ is transitive because one can compose local R-algebra maps, and we have a partially ordered set using (f). The set is directed because of (c). This proves (g). $\square$

It is easy to see that the construction $(S \otimes_R T)_Q$ in part (c) gives the coproduct of S and T in the category of pointed étale R-algebras and local R-algebra homomorphisms.