Math 711: Lecture of October 15, 2004

Before giving the proof of the Theorem stated at the end of the previous lecture, we want to discuss the general problem of when a module-finite extension of a quasilocal domain decomposes.

Let (R, P, K) be quasilocal and let S be a module-finite extension of R. For every maximal ideal Q of S, S/Q is a field integral over $R/(Q \cap R)$, and so $R/(Q \cap R)$ is a field: that is, every maximal ideal of S lies over P, the unique maximal ideal of R. Since S/PS is module-finite over $K = R/P$, it is zero-dimensional. The maximal ideals of S correspond bijectively to the prime ideals of the Artin local ring S/PS, and so there are finitely many of them, say $Q_1, \ldots, Q_r$. Let $q_j = Q_j/PS$, $1 \le j \le r$. Then

$$S/PS \cong \prod_{j=1}^{r} (S/PS)_{q_j}$$

and $(S/PS)_{q_j} \cong (S/PS)_{Q_j}$, $1 \le j \le r$. Note that since P is contained in every Q_j, PS is contained in every maximal ideal of S, i.e., it is contained in the Jacobson radical of S. It is now clear that S decomposes if and only if $S \cong \prod_j S_{Q_j}$.

There are 2^r idempotents in S/PS: S/PS is a product of r indecomposable factors, and for each subset $\mathcal{S}$ of the factors there is a unique idempotent that corresponds to 1 in the factors that are in $\mathcal{S}$ and 0 in the factors in the complementary subset.

In the product ring S/PS, we shall refer to the idempotent e_j the corresponds to 1 in the factor $(S/PS)_{Q_j}$ and 0 in the other factors as the idempotent *associated with* Q_j or with $q_j = Q_j/PS$. It is characterized among the idempotents by the condition that $e_j \notin q_j$ while $e_j \in q_i$ for $i \neq j$. It is then easy to see that S decomposes if and only if all idempotents of S/PS lift to idempotents of S, and it suffices if the idempotents e_j lift. (Any other idempotent is a sum of mutually distinct e_j or 0.) An idempotent e of S lifts e_j if and only if $e \notin Q_j$ while $e \in Q_i$ for $i \neq j$. The reason is that the image of e in S/PS is an idempotent with the corresponding membership property, and this means that the image must be e_j.

We next consider exactly what it means for $S = R[x]/(F)$ to decompose when F is monic and (R, P, K) is quasilocal. Let $f \in K[x]$ be the image of F modulo $PR[x]$. Then f factors uniquely, except for the order of the terms, as $g_1 \cdots g_r$ where the g_i are monic and are powers of mutually distinct monic irreducible polynomials. Thus, g_i and g_j generate the unit ideal in $K[x]$ if $i \neq j$. We claim that $S = R[x]/(F)$ decomposes if and only if the factorization $f = g_1 \cdots g_r$ lifts to a factorization $F = G_1 \cdots, G_r$ over $R[x]$, where every G_j is monic and $G_j \equiv g_j \mod PR[x]$. Suppose one has the lifted factorization. Then the principal ideals G_jS are pairwise comaximal: since PS is in every maximal ideal of S, it suffices to see this working over $R[x]/PR[x] \cong K[x]$, and in this ring the G_j map to the g_j. It follows from the Chinese remainder theorem that $S \cong \prod_j S/G_jS$, and this shows that S decomposes.

For the converse, suppose that $S = \prod S_j$ decomposes, where $S_j/PS_j \cong K[x]/(g_j)$. Let $d_j = \deg(g_j)$. By Nakayama's lemma, the images of $1, x, \ldots, x^{d_j-1}$ generate S_j as an R-module, since their images in $S_j/PS_j \cong K[x]/(g_j)$ generate that ring as K-vector space, and PS_j is in the Jacobson radical. Therefore, the image of x_j^d is in the R-span of the images of $1, x, \ldots, x^{d_j-1}$ in S_j, and this means that we can choose a monic polynomial $G_j \in R[x]$ of degree d_j such that $G_j(x)$ maps to 0 in S_j. This implies that the image of G_j in $K[x]$ is divisible by g_j. Since they have the same degree, g_j is the image of G_j mod $PR[x]$. Let $G = \prod_j G_j$. Then $\deg(G) = \sum_j \deg(G_j) = \sum_j \deg(g_j) = \deg(f) = \deg(F)$. Now, x satisfies $G(x) = 0$ in S: since S is the product of the S_j, it is enough to check that this is true in every S_j, and that follows because G_j divides G. Since $S = R[x]/F$, it follows that F divides G. Since they are monic of the same degree, they are equal.

Note that if (R, P, K) is Henselian, a factorization of the image f of $F \in R[x]$ over $k[x]$, say $f = g_1 \cdots, g_r$, where the g_i, g_j are relatively prime in pairs, lifts to such a factorization into monic polynomials over $R[x]$. When $r = 2$ it is the definition of Henselian, and one may prove the result in general by induction on r: if $r \geq 3$, since $g^* = g_1 \cdots g_{r-1}$ and g_r are relatively prime, we may lift the factorization $g = g^* g_r$ to a factorization $G = G^* G_r$, and then apply the induction hypothesis to G^* and the factorization $g^* = g_1 \cdots g_{r-1}$.

We are now ready to prove the equivalence of the first four conditions in the statement of the Theorem from the previous lecture.

Proof of the equivalence of (1), (2), (3), and (4). The remarks above show that (1) $\Leftrightarrow$ (4), while (2) $\Rightarrow$ (3) $\Rightarrow$ (4) is clear. We can therefore complete the proof by showing that (4) $\Rightarrow$ (2). Let $R \subseteq S$ be module finite and let Q be a maximal ideal of R. Let e_0 be the corresponding idempotent in S/PS, so that e_0 is in Q/PS and not in any other maximal ideal. It suffices to show that e_0 lifts to S. Choose any lifting c of e_0 to S: of course, c need not be idempotent, but c is not in Q and and is in every other maximal ideal of S. Of course, c satisfies some monic polynomial $F \in R[x]$. Let $T = R[x]/(F)$. We have an R-algebra map $T \to S$ that sends the image of x in T to $c \in S$. Let q be the inverse image of Q in T, which is a maximal ideal of T. Since T decomposes it contains an idempotent e_0 that is not in q but is in every other maximal ideal of T. The image e of e_0 is an idempotent of S that is evidently not in Q. It will suffice to show that e is in every maximal ideal Q' of S other than Q, for then e must lift e_0. It suffices to show that if $Q' \neq Q$ then Q' does not lie over q, for e_0 will then be in the contraction of Q' to T, and so e will be in Q'. But if Q' lies over q then T/q injects into S/Q'. The image of x is sent to the image of c under this map, and so is sent to 0. Hence, the image of x in T is in q, and so is sent to 0 under the injection $T/q \to S/Q$. But $c \notin Q$, a contradiction. $\square$