18.786. (Fall 2011) Notes on splitting primes

Proposition 0.1. *(a variant of Neukirch I.8.3) Let L/K and L'/K be finite extensions of number fields. (One could consider the case where K is the field of fractions of a Dedekind domain and L, L' are finite separable over K.) Show that a prime ideal $\mathfrak{p}$ of K (of $\mathcal{O}_K$, to be precise) is totally split in both L/K and L'/K if and only if it is totally split in the composite extension LL'/K.*

Proof of the "only if" part. Consider the $\mathcal{O}_K$-algebra map

$$\phi : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{L'} \to \mathcal{O}_{LL'}, \qquad a \otimes b \mapsto ab.$$

Let A be the image of ϕ. Note that $\mathcal{O}_L$ and $\mathcal{O}_{L'}$ together generate LL' over K.

In fact it is simpler to argue after localization. Note that $\mathcal{O}_{K,\mathfrak{p}}$ is a PID as $\mathcal{O}_K$ is Dedekind. By localizing all $\mathcal{O}_K$-algebras at $\mathfrak{p}$, we obtain a surjection

$$\phi_{\mathfrak{p}} : \mathcal{O}_{L,\mathfrak{p}} \otimes_{\mathcal{O}_{K,\mathfrak{p}}} \mathcal{O}_{L',\mathfrak{p}} \twoheadrightarrow A_{\mathfrak{p}} \quad (\subset \mathcal{O}_{LL',\mathfrak{p}}).$$

It suffices to show that $\mathcal{O}_{LL',\mathfrak{p}}$ contains at least $[LL' : K]$ prime ideals containing $\mathfrak{p}$ (or equivalently $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$).

Since $\mathcal{O}_{L,\mathfrak{p}}$ and $\mathcal{O}_{L',\mathfrak{p}}$ generate LL' over K, it follows that their image $A_{\mathfrak{p}}$ also generates LL' over K. Then it is easy to see that $A_{\mathfrak{p}}$ is an $\mathcal{O}_{K,\mathfrak{p}}$-algebra which is free of rank $[LL' : K]$ as an $\mathcal{O}_{K,\mathfrak{p}}$-module. ...(∗)

The map $\phi_{\mathfrak{p}}$ modulo $\mathfrak{p}$ is a surjective[1] $\mathcal{O}_K/\mathfrak{p}$-algebra map

$$\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}} \otimes_{\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}} \mathcal{O}_{L',\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L',\mathfrak{p}} \twoheadrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

As $\mathfrak{p}$ splits completely in L and L', the left hand side is isomorphic to $(\mathcal{O}_K/\mathfrak{p})^{[L:K]} \otimes_{\mathcal{O}_K/\mathfrak{p}} (\mathcal{O}_K/\mathfrak{p})^{[L':K]} \simeq (\mathcal{O}_K/\mathfrak{p})^{[L:K][L':K]}$. Therefore the quotient $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is isomorphic to $(\mathcal{O}_K/\mathfrak{p})^m$ for some m. By (∗),

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq (\mathcal{O}_K/\mathfrak{p})^{[LL':K]}$$

as an $\mathcal{O}_K/\mathfrak{p}$-algebra. In particular $A_{\mathfrak{p}}$ contains $[LL' : K]$ maximal ideals, say $\mathfrak{P}_1, ..., \mathfrak{P}_{[LL':K]}$, containing $\mathfrak{p}$.

This together with the fact that $\mathcal{O}_{LL',\mathfrak{p}} \supset A_{\mathfrak{p}}$, implies that $\mathcal{O}_{LL',\mathfrak{p}}$ has at least $[LL' : K]$ maximal ideals containing $\mathfrak{p}$. Indeed, for each i we choose any maximal ideal $\mathfrak{P}'_i$ of $\mathcal{O}_{LL',\mathfrak{p}}$ containing $\mathfrak{P}_i$ (you can check that $\mathfrak{P}_i\mathcal{O}_{LL',\mathfrak{p}} \neq \mathcal{O}_{LL',\mathfrak{p}}$ so such a $\mathfrak{P}'_i$ can be chosen), and it is enough to note that $\mathfrak{P}'_i \neq \mathfrak{P}'_j$ if $i \neq j$. (If $\mathfrak{P}'_i = \mathfrak{P}'_j$ happened, then their intersection with $A_{\mathfrak{p}}$ contains distinct maximal ideals $\mathfrak{P}_i$ and $\mathfrak{P}_j$, which generate the whole $A_{\mathfrak{p}}$. This is absurd.)

□

Remark 0.2. An alternative approach is to use completions at prime ideals, which is conceptually easier. (One of you used this.) One can show that $\mathfrak{p}$ splits (completely) in L if and only if $L \otimes_K K_{\mathfrak{p}}$ is isomorphic to a finite product of $K_{\mathfrak{p}}$'s as a $K_{\mathfrak{p}}$-algebra. (If so, the number of copies must be $[L : K]$ by counting the vector space dimension over $K_{\mathfrak{p}}$.) We will get to this kind of business later in class, so let's take it on faith for the moment. Now suppose that $\mathfrak{p}$ splits in L and L'. It is easy to see that the natural $K_{\mathfrak{p}}$-algebra map

$$(L \otimes_K K_{\mathfrak{p}}) \otimes_{K_{\mathfrak{p}}} (L' \otimes_K K_{\mathfrak{p}}) \to LL' \otimes_K K_{\mathfrak{p}}, \quad (a \otimes b) \otimes (a' \otimes b') \mapsto aa' \otimes bb'$$

is onto. Since the assumption implies that the LHS is a product of $K_{\mathfrak{p}}$'s, it follows that the RHS has the same form. Therefore $\mathfrak{p}$ splits in LL'.

Proposition 0.3. *Let L/K be a finite Galois extension. Let $\mathfrak{P}$ be a prime of L above a prime $\mathfrak{p}$ of K, and denote by $D_{\mathfrak{P}}$ the decomposition group. Write $\mathfrak{P}_D := \mathfrak{P} \cap \mathcal{O}_{L^{D_{\mathfrak{P}}}}$ and $e = e_{\mathfrak{P}/\mathfrak{p}}$, $f = f_{\mathfrak{P}/\mathfrak{p}}$ as usual (which depend only on $\mathfrak{p}$ and not on $\mathfrak{P}$). TFAE. (The Following Are Equivalent.)*

(i) $L^{D_{\mathfrak{P}}}$ is a Galois extension of K.
(ii) $\mathfrak{p}$ splits completely in $L^{D_{\mathfrak{P}}}$.

Proof of (i)⇒(ii). Previously we have shown that $\mathfrak{P}_D$ is non-split in L and that $e_{\mathfrak{P}/\mathfrak{P}_D} = e$, $f_{\mathfrak{P}/\mathfrak{P}_D} = f$ (also $|D_{\mathfrak{P}}| = ef$). Since

$$e = e_{\mathfrak{P}/\mathfrak{P}_D} e_{\mathfrak{P}_D/\mathfrak{p}}, \tag{0.1}$$

we have $e_{\mathfrak{P}_D/\mathfrak{p}} = 1$. Similarly $f_{\mathfrak{P}_D/\mathfrak{p}} = 1$. Now if $L^{D_{\mathfrak{P}}}$ is Galois over K then the Galois group permutes all prime ideals of $L^{D_{\mathfrak{P}}}$ above $\mathfrak{p}$. Hence for every $\mathfrak{q}$ of $L^{D_{\mathfrak{P}}}$ above $\mathfrak{p}$, $e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$. Hence $\mathfrak{p}$ splits in $L^{D_{\mathfrak{P}}}$. □

[1] In a fancy language, tensoring $\otimes_{\mathcal{O}_{K,\mathfrak{p}}} \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is a right exact functor, which preserves surjectivity.

First Proof of $(ii) \Rightarrow (i)$. Let L' be the Galois closure of $L^{D_{\mathfrak{P}}}$ in L. By Proposition 0.1, L' is Galois over L. If $L' \neq L$ then $[L' : K] > [L^{D_{\mathfrak{P}}} : K] = r$. However Proposition 0.1 tells us that $\mathfrak{p}$ splits in L', so $\mathfrak{p}$ splits into at least $r+1$ primes in L' and so also in L. This is a contradiction, as r was the number of primes of L dividing $\mathfrak{p}$. □

Second Proof of $(ii) \Rightarrow (i)$. Let $\mathfrak{Q}$ be any prime of L above $\mathfrak{p}$ and let $\mathfrak{q}$ be the unique prime of $L^{D_{\mathfrak{P}}}$ dividing $\mathfrak{Q}$. By assumption $e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$. Thanks to an identity like (0.1), $e_{\mathfrak{Q}/\mathfrak{q}} = e$ and similarly $f_{\mathfrak{Q}/\mathfrak{q}} = f$. From this we have $[L : L^{D_{\mathfrak{P}}}] = e_{\mathfrak{Q}/\mathfrak{q}} f_{\mathfrak{Q}/\mathfrak{q}}$, and it follows that $\mathfrak{Q}$ is the unique prime above $\mathfrak{q}$ and that $D_{\mathfrak{P}} \subset D_{\mathfrak{Q}}$ (i.e. every element of $D_{\mathfrak{P}}$ fixed $\mathfrak{Q}$). Since $|D_{\mathfrak{P}}| = |D_{\mathfrak{Q}}| = ef$, they are equal.

In particular, for any $\sigma \in G$, applying the above to $\mathfrak{Q} = \sigma(\mathfrak{P})$, we obtain

$$D_{\mathfrak{P}} = D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}.$$

Therefore $D_{\mathfrak{P}}$ is normal in G, which implies that $L^{D_{\mathfrak{P}}}$ is Galois over K.

□