Let K be a number field and let $L = K(\alpha)$ be a finite extension. Let $\mathfrak{p}$ be a prime of K, and let $f(t) \in K[t]$ be the minimal polynomial of α. Recall that we proved the following in lectures (Proposition 58, and later again in the Remark following Proposition 93):

Proposition. *There is a canonical bijection between the irreducible factors of $f(t)$ in $K_{\mathfrak{p}}[t]$ and the primes in L above $\mathfrak{p}$.*

Remark. I don't think I emphasized this enough in the course, but in my opinion the most natural proof of this Proposition is the second one we gave, in the Remark following Proposition 93 (using places/embeddings). That doesn't mean that the first proof isn't important; it is important to understand the bijection between the primes in L above $\mathfrak{p}$ and the double coset space

$$Gal(M/L)\backslash Gal(M/K)/D_{\mathfrak{P}/\mathfrak{p}},$$

with notation as below (this was Proposition 57).

The purpose of this note, however, is to make some remarks about the Proposition above and to illustrate these remarks with an example. The bijection was given explicitly by the following recipe: Let M/K be the Galois closure of L/K, with Galois group $G = Gal(M/K)$. Choose a prime $\mathfrak{P}$ in M above $\mathfrak{p}$. If $g[t] \in K_{\mathfrak{p}}[t]$ is an irreducible factor of $f(t)$, choose $\sigma \in G$ such that $\sigma(\alpha)$ is a root of $g(t)$ *in* $M_{\mathfrak{P}}$. Then the recipe is

$$g(t) \mapsto \mathcal{O}_L \cap \sigma^{-1}(\mathfrak{P}).$$

This *is* independent of the choice of $\mathfrak{P}$ and σ, and a proof of this was given in lectures. However, in the course of doing this, I failed to point out something that (at least I think) is somewhat subtle. This is the condition, emphasized above, that $\sigma(\alpha)$ is a root of $g(t)$ in $M_{\mathfrak{P}}$, where we think of $\sigma(\alpha)$, which is an element of M, as an element of $M_{\mathfrak{P}}$ via the natural embedding $M \hookrightarrow M_{\mathfrak{P}}$.

If $\mathfrak{P}'$ is different choice of prime in M above $\mathfrak{p}$, then we have canonical embeddings $M \hookrightarrow M_{\mathfrak{P}}$ and $M \hookrightarrow M_{\mathfrak{P}'}$ as well as $K_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{P}}$ and $K_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{P}'}$, so it might be tempting to think that the subfields M and $K_{\mathfrak{p}}$ interact in the same way inside $M_{\mathfrak{P}}$ and $M_{\mathfrak{P}'}$. In other words, it might seem that the choice of σ above is independent of the choice of $\mathfrak{P}$. But this is not true. Let us illustrate this in the simplest possible example.

Example. Let $K = \mathbb{Q}$ and let $L = M = \mathbb{Q}(i)$; then $f(t) = t^2 + 1$. We look at the prime 5 in $\mathbb{Q}$, it splits as $5 = (2+i)(2-i)$ in L. Now consider $\mathbb{Q}_5$. In $\mathbb{F}_5$, -1 has square roots ± 2, which we can lift by Hensel's Lemma. So let $\theta \in \mathbb{Z}_5$ be the unique element with $\theta^2 = -1$ and $\theta \equiv 2$ modulo 5, then the lift of -2 is $-\theta$. We have two completions

$$L_{(2+i)}, L_{(2-i)}$$

which are both (canonically) isomorphic to $\mathbb{Q}_5$. But, in identifying these with $\mathbb{Q}_5$, the embeddings $L \hookrightarrow \mathbb{Q}_5$ change. $2+i$ is a uniformizer in $L_{(2+i)}$, so in identifying $L_{(2+i)} \cong \mathbb{Q}_5$ the image of $2+i$ must land inside $5\mathbb{Z}_5$. Since any embedding $L \hookrightarrow \mathbb{Q}_5$ has to send i to either θ or $-\theta$, we conclude that the image of $2+i$ must be $2-\theta$, since

$$2 - \theta \in 5\mathbb{Z}_5$$

but $2+\theta \notin 5\mathbb{Z}_5$, as $\theta \equiv 2$ modulo 5. In summary, after identifying $L_{(2+i)}$ with $\mathbb{Q}_5$, the embedding $L \hookrightarrow L_{(2+i)}$ becomes

$$L \hookrightarrow \mathbb{Q}_5;$$
$$a+bi \mapsto a-b\theta,$$

where $a, b \in \mathbb{Q}$. Similarly, after identifying $L_{(2-i)}$ with $\mathbb{Q}_5$, the embedding $L \hookrightarrow L_{(2-i)}$ becomes

$$L \hookrightarrow \mathbb{Q}_5;$$
$$a+bi \mapsto a+b\theta.$$

You should compare this with Proposition 93, where we talked about the equivalence between places and embeddings. Let us now work out the recipe for the bijection for the factor $t-\theta$ of t^2+1 in $\mathbb{Q}_5[t]$. Let $G = Gal(L/\mathbb{Q})$ and let τ be the non-trivial element. The element i is what we wrote as α in the general discussion above.

First, we need a choice of prime $\mathfrak{P}$ in $M = L$ above 5. Let's take $(2+i)$. Now, we need $\sigma \in G$ such that $\sigma(i)$ is a root of $t-\theta$ in $L_{(2+i)}$. From our discussion above, upon identifying $L_{(2+i)}$ with $\mathbb{Q}_5$, i maps to $-\theta$, which is not a root of $t-\theta$. So we are forced to choose $\sigma = \tau$, since then $\tau(i) = -i$ which maps to θ, the root of $t-\theta$. We then plug this in to our recipe above to get

$$t-\theta \mapsto \tau^{-1}((2+i)) = (2-i).$$

(since $L = M$, we don't need to intersect with $\mathcal{O}_L$). If we had instead chosen $\mathfrak{P} = (2-i)$, then we would have been forced to choose $\sigma = id$ (the identity), and so the recipe gives

$$t-\theta \mapsto id^{-1}((2-i)) = (2-i).$$

So we have verified the indepence in this particular case, and (hopefully) got a feel for why it holds in general.