Answer to the problem 9.3.1 [1]

Let L/K be a finite Galois extension of number fields. Let $\mathfrak{P}$ be a maximal ideal of O_L, $\mathfrak{p} := O_K \cap \mathfrak{P}$. Any $\sigma \in Gal(L/K)$ induces an automorphism of the O_K-algebra O_L. Let $D_{\mathfrak{P}}$ be the subgroup of $Gal(L/K)$ consisting of elements which send $\mathfrak{P}$ to itself via the induced automorphism of O_L. If $\sigma \in D_{\mathfrak{P}}$, then σ induces an automorphism of the field $\kappa(\mathfrak{P}) := O_L/\mathfrak{P}$ and this automorphism fixes the subfield $\kappa(p) := O_K/\mathfrak{p} \subseteq O_L/\mathfrak{P} = \kappa(\mathfrak{P})$. Let $I_{\mathfrak{P}}$ be the subgroup of $D_{\mathfrak{P}}$ consisting of elements which induces the identity field automorphism of $\kappa(\mathfrak{P})$. Now, we want to show that that there is an exact sequence of groups:

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \to 1$$

Proof: Set $G_{\mathfrak{P}}$ to be the decomposition group of $\mathfrak{P}$, then if $\mathfrak{P}_1 = \mathfrak{P}$ and $\mathfrak{p} = {\mathfrak{P}_1}^e \cdots {\mathfrak{P}_g}^e$ is the factorization of $\mathfrak{p}$ in O_L, then as we know g is the index of $G_{\mathfrak{P}}$ in G. So, since $|G| = efg$ we get $ef = |G_{\mathfrak{P}}|$. Now, notice that if F is the fixed field of $G_{\mathfrak{P}}$ and $\mathfrak{P}'$ is $\mathfrak{P} \cap F$, then $\mathfrak{P}$ is the only prime above $\mathfrak{P}'$ in L, since L/F is Galois, because the prime above $\mathfrak{P}'$ are all $\sigma(\mathfrak{P})$ where $\sigma \in Gal(L/F)$. But, $Gal(L/F) = G_{\mathfrak{P}}$, so for every $\sigma \in Gal(L/F)$, $\sigma(\mathfrak{P}) = \mathfrak{P}$. Now, if e' and f', e'' and f'' are respectively the ramification indexes of L/F and F/K, then $ef = e'f'$ since $\mathfrak{P}$ is the only prime of L above $\mathfrak{P}'$ we have $[L : F] = e'f'$; here notice F/K is not necessarily Galois and e'' is the ramification of $\mathfrak{P}'$ over $\mathfrak{p}$. But the ramification index and residue index are both multiplicative we have $e = e'$ and $f = f'$. Therefore, $\kappa(\mathfrak{P}') = \kappa(\mathfrak{p})$ and the map $G_{\mathfrak{P}/\mathfrak{p}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ coming from the extension L/K is the same as the map $G_{\mathfrak{P}/\mathfrak{P}'} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}'))$ coming from L/F.

Hence, from the beginning we can assume that there is only one prime above $\mathfrak{p}$, so $G_{\mathfrak{P}} = G$ and we should prove that the map $G \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is surjective.

Now take $\tau \in Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ and $\bar{\theta}$ any primitive element in the extension $Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, note that this extension is Galois, primitive element exists. If θ is any lifting of $\bar{\theta}$ to O_L, and $f := \min(\theta, K), g = \min(\bar{\theta}, \kappa\mathfrak{p})$, then since $\bar{f}(\bar{\theta}) = \overline{f(\theta)} = 0$, we have $g|\bar{f}$. So, since $g(\tau(\bar{\theta})) = 0$, $\bar{f}(\tau(\bar{\theta})) = 0$. Hence since the roots of f are exactly $\sigma(\theta)$ where $\sigma \in G$, there exists $\sigma \in G$ such that $\overline{\sigma(\theta)} = \bar{\sigma}(\bar{\theta}) = \tau(\bar{\theta})$. But $\bar{\theta}$ is a primitive element of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ so any non-trivial element of $Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ does not fix $\bar{\theta}$. Therefore $\bar{\sigma} = \tau$ and we are done.

[1] Questions and comments to siinarezazadeh@gmail.com.