Name: ____________________

Read Section 23.1, focusing on the *examples*, particularly Examples 23.4 and 23.9 (which harken back to Example 21.20), and the *statements* of results, rather than the proofs.

Reading Questions

1. **Galois Groups.** Make sure you know the definition of the Galois group of a field extension and the Galois group of a polynomial and the statements of the main results (Proposition 23.5, Proposition 23.6, and Theorem 23.7).

2. **Separable Extensions.** The defining condition for a separable extension is not easily verified, but, while there are some (pathological) exceptions, "most" field extensions are separable. In particular, in characteristic zero, *all extensions* are separable, so all extensions of $\mathbb{Q}$ are separable. And in characteristic p, all *finite* extensions of *finite* fields are separable.

   (a) A finite extension $F(\alpha)$ is separable if and only if the minimal polynomial of α over F has no repeated factors.

   (b) A finite extension $F(\alpha_1, \ldots \alpha_n)$ is separable if and only if each of the intermediate extensions $F(\alpha_1)/F$, $F(\alpha_1, \alpha_2)/F(\alpha_1)$, $\ldots F(\alpha_1, \ldots, \alpha_n)/F(\alpha_1, \ldots, \alpha_{n-1})$ is separable.

3. **Primitive Element Theorem.** Every finite separable extension has a *primitive element*: if E/F is a finite separable extension, then there is an element α in E such that $E = F(\alpha)$.

4. Consider the extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \mu\}$ be the Galois group of the extension, as in Examples 23.4 and 23.9.

   (a) Recall that the extension field is a four-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$, so every element in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ can be written uniquely in the form $a_0 + a_1\sqrt{3} + a_2\sqrt{5} + a_3\sqrt{15}$, where $a_i \in \mathbb{Q}$ for all i. Describe each element of G explicitly by computing its effect on an arbitrary element $a_0 + a_1\sqrt{3} + a_2\sqrt{5} + a_3\sqrt{15}$ of the extension field.

   (b) Which elements of G are also elements of the Galois group $H_1 = \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3}))$ of the intermediate extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3})$? (These should be automorphisms of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ that fix $\mathbb{Q}(\sqrt{3})$.)

(c) Which elements of G are also elements of the Galois group $H_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{5}))$ of the intermediate extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{5})$?

(d) What is the Galois group of $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3}, \sqrt{5})$?

(e) Is $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ a finite separable extension of $\mathbb{Q}$? (Explain.)

(f) What is a primitive element for $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$?

5. What struck you in this reading? What is still unclear? What remaining questions do you have?