Galois theory - Problem Set 4

To be solved on Thursday 21.03

Chapter 17.1

Problem 1. (Exercise 17.1.1 in the book.) Let $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be an extension field of $\mathbb{Q}$, where $\omega^3 = 1$, $\omega \neq 1$. For each of the following subgroups S_i of the group $G(E/\mathbb{Q})$ find E_{S_i}.

(a) $S_1 = \{1, \sigma_2\}$, where σ_2 is defined by $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$ and $\sigma_2(\omega) = \omega^2$.

(b) $S_2 = \{1, \sigma_3\}$, where σ_3 is defined by $\sigma_3(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ and $\sigma_3(\omega) = \omega^2$.

(c) $S_3 = \{1, \sigma_4\}$, where σ_4 is defined by $\sigma_4(\sqrt[3]{2}) = \sqrt[3]{2}$ and $\sigma_4(\omega) = \omega^2$.

(d) $S_4 = \{1, \sigma_5, \sigma_6\}$ where σ_5 is defined by $\sigma_5(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ and $\sigma_5(\omega) = \omega$ and σ_6 is defined by $\sigma_6(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$ and $\sigma_6(\omega) = \omega$.

Problem 2. (Exam June 2015, Problem 5.) Let $E = F(\alpha_1, \alpha_2)$ be a Galois extension of a field F, and let $K_1 = F(\alpha_1)$ and $K_2 = F(\alpha_2)$. Consider the subgroups $H_1 = G(E/K_1)$ and $H_2 = G(E/K_2)$ of the Galois group $G(E/F)$.

(a) Show that $H_1 \cap H_2 = \{e\}$, that is, the intersection of H_1 with H_2 is the trivial subgroup of $G(E/F)$.

(b) Suppose that each element $g_1 \in H_1$ maps K_2 to K_2, and that each element $g_2 \in H_2$ maps K_1 to K_1. Show that $g_1 g_2 = g_2 g_1$ for all $g_1 \in H_1$, $g_2 \in H_2$.

Chapter 17.2

Problem 3. (Exercise 17.2.1 in the book.) Find the Galois groups $G(K/\mathbb{Q})$ of the following extensions K of $\mathbb{Q}$:

(a) $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(b) $K = \mathbb{Q}(\alpha)$, where $\alpha = \cos 2\pi/3 + i \sin 2\pi/3$.

(c) K is the splitting field of $x^4 - 3x^2 + 4 \in \mathbb{Q}[x]$.

Problem 4. (Exam May 2017, Problem 3(c)-(e).) Let E be the splitting field of $f(x) = x^{17} - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$, that is $E = \mathbb{Q}(\omega, \sqrt[17]{2})$ where $\omega = e^{\frac{2\pi i}{17}}$. (see Problem 7 in Problem Set 3).

(a) Let $G = \mathrm{Gal}(E/\mathbb{Q})$ be the Galois group of E over $\mathbb{Q}$. Show that there exists an intermediate field L, $\mathbb{Q} \subseteq L \subseteq E$, such that L corresponds by the Galois correspondence to a normal subgroup H of G of order 17. Explain your argument.

(b) Show that there exists an intermediate field M, $\mathbb{Q} \subseteq M \subseteq E$, such that $[M : \mathbb{Q}] = 34$. [*Hint*: Use Sylov's Theorem.]

(c) Show that G is non-abelian. [*Hint*: G abelian implies that all subgroups are normal.]

Problem 5. (Exam June 2015, Problem 7.) Let $f(x) = x^5 - x - 1 \in \mathbb{Z}_5[x]$ and $E = \mathbb{Z}_5(\beta)$, where β is a root of $f(x)$.

(a) Show that $\beta+1$, $\beta+2$, $\beta+3$, $\beta+4$ are also roots of $f(x)$. Deduce that $\beta \notin \mathbb{Z}_5$.

(b) Define $\sigma \in G(E/\mathbb{Z}_5)$ by $\sigma(\beta) = \beta + 1$. Find the order of σ in $G(E/\mathbb{Z}_5)$, and describe the action of σ on the roots of $f(x)$.

(c) Use the above and the FTGT to deduce that $f(x)$ is irreducible, and that $[E : \mathbb{Z}_5] = 5$.

Problem 6. (Exam June 2015, Problem 6.) Let $F \subseteq E$ be a Galois extension of degree $[E : F]$.

(a) Is it possible that $[E : F] = 4$ and that there are precisely two proper intermediate fields between E and F?

(b) Suppose that $[E : F] = 6$ and that E is the splitting field of a polynomial of degree 3 (and a Galois extension of F.) How many proper intermediate fields are there between E and F?

Problem 7. (Exam May 2017, Problem 5, Exam May 2013, Problem 6.) Let N be a Galois extension of K such that $G(N/K)$ is abelian. Let $\alpha \in N$ and let $p(x) \in K[x]$ be the minimal polynomial of α over K. Show that all roots of $p(x)$ lie in $K(\alpha)$.

Problem 8. (Exercise 17.2.3 in the book.) Let $u \in \mathbb{R}$ and let $\mathbb{Q}(u)$ be a normal extension of $\mathbb{Q}$ such that $[\mathbb{Q}(u) : \mathbb{Q}] = 2^m$, where $m \geq 0$. Show that there exist intermediate fields K_i such that

$$K_0 = \mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = \mathbb{Q}(u),$$

where $[K_i : K_{i-1}] = 2$. (Hint: Sylow's first theorem.)

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 9. (Chapter 17.2) (For those with a background on category theory, for example MA3204) Let $F \subseteq E$ be a field extension. Define two categories $\mathcal{F}$ and $\mathcal{G}$ by

$$\mathrm{Obj}(\mathcal{F}) = \{\text{intermediate fields } F \subseteq K \subseteq E\} \text{ and } \mathrm{Obj}(\mathcal{G}) = \{\text{subgroups } H < G(E/F)\},$$

and morphisms given by inclusion in both $\mathcal{F}$ and $\mathcal{G}$. Let $E_- : \mathcal{G} \to \mathcal{F}$ be the contravariant functor given by $E_-(H) = E_H$, and let $G(E/-) : \mathcal{F} \to \mathcal{G}$ be the contravariant functor given by $G(E/-)(K) = G(E/K)$.

(a) Show that the functors E_- and $G(E/-)$ are well-defined.

(b) Show that $(G(E/-), E_-)$ form an adjoint pair between $\mathcal{F}$ and $\mathcal{G}^{\mathrm{op}}$.

(c) Show that if $F \subseteq E$ is a Galois extension, then E_- is an isomorphism of categories with inverse given by $G(E/-)$.

Remark: This is an example of a special type of adjunction between poset categories called *Galois connection.*

Problem 10. (Chapter 17.2) Let F be a field and $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Let E be the splitting field of $f(x)$. Show that $[E : F]$ divides $n!$.

Problem 11. (Chapter 17.2) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 3. Let E be the splitting field of $f(x)$. What are the possible values of $[E : \mathbb{Q}]$? Provide an explicit example for each such possible value.