Math 562/662 **Spring 2019**
Homework 1 **Drew Armstrong**

---

1. Degree of a Field Extension. Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension.

(a) There is an obvious "multiplication function" $\mathbb{F} \times \mathbb{E} \to \mathbb{E}$ defined by the rule $(a, b) \mapsto ab$. Verify that this multiplication makes $\mathbb{E}$ into a **vector space** over $\mathbb{F}$. We will denote this vector space by $\mathbb{E}/\mathbb{F}$. Its dimension is called the *degree* of the extension:

$$[\mathbb{E} : \mathbb{F}] := \dim(\mathbb{E}/\mathbb{F}).$$

(b) **Dedekind's Tower Law.** Now let $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$ be any intermediate field. Prove that the degrees of the three extensions satisfy

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}].$$

[Hint: Let $\{\alpha_i\}_i$ be a basis for $\mathbb{K}/\mathbb{F}$ and let $\{\beta_j\}_j$ be a basis for $\mathbb{E}/\mathbb{K}$. Prove that the set $\{\alpha_i\beta_j\}_{i,j}$ is a basis for $\mathbb{E}/\mathbb{F}$.] Does this remind you of Lagrange's Theorem?

2. Definition of the Galois Group. In this problem you will show that the hypothesis of invertibility is redundant in the definition of the Galois group. Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension and let $\sigma : \mathbb{E} \to \mathbb{E}$ be any function satisfying

$$\sigma(a + b) = \sigma(a) + \sigma(b) \quad \text{and} \quad \sigma(ab) = \sigma(a)\sigma(b) \quad \text{for all } a, b \in \mathbb{E}.$$

(a) Prove that σ is necessarily injective.
(b) If $\sigma(a) = a$ for all $a \in \mathbb{F}$, prove that $\sigma : \mathbb{E}/\mathbb{F} \to \mathbb{E}/\mathbb{F}$ is a linear function.
(c) If $\sigma(a) = a$ for all $a \in \mathbb{F}$ and if $[\mathbb{E} : \mathbb{F}] < \infty$,[1] combine parts (a) and (b) to prove that σ is necessarily bijective. [Hint: Use the Rank-Nullity Theorem.]

3. Adjoining a Subset to a Subfield. Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension and let $S \subseteq \mathbb{E}$ be any subset. We let $\mathbb{F}(S) \subseteq \mathbb{E}$ denote the smallest subfield of $\mathbb{E}$ that contains the set $\mathbb{F} \cup S$.

(a) Prove that $\mathbb{F}(S) = \mathbb{F}(S - \mathbb{F})$.
(b) For any two subsets $S, T \subseteq \mathbb{F}$ prove that $\mathbb{F}(S)(T) = \mathbb{F}(T)(S) = \mathbb{F}(S \cup T)$.
(c) If $\mathbb{K} \subseteq \mathbb{E}$ is a subfield, prove that $\mathbb{F}(\mathbb{K}) = \mathbb{K}(\mathbb{F}) = \mathbb{F} \vee \mathbb{K}$ is the join operation in the lattice of subfields. We also call this the *compositum* of subfields:

$$\mathbb{F}\mathbb{K} := \mathbb{F}(\mathbb{K}).$$

4. Quadratic Field Extensions. Let $\mathbb{E} \supseteq \mathbb{F}$ be a field extension and let $\alpha \in \mathbb{E}$ be any element such that $\alpha \notin \mathbb{F}$ and $\alpha^2 \in \mathbb{F}$. Consider the subfield $\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{E}$ generated by α.

(a) Prove that the set $\{1, \alpha\} \subseteq \mathbb{F}(\alpha)/\mathbb{F}$ is linearly independent.
(b) Prove that $\{1, \alpha\} \subseteq \mathbb{F}(\alpha)/\mathbb{F}$ is a spanning set. [Hint: Prove that $\{a+b\alpha : a, b \in \mathbb{F}\} \subseteq \mathbb{E}$ is a subfield by "rationalizing the denominator."] It follows that $\{1, \alpha\}$ is a basis for $\mathbb{F}(\alpha)/\mathbb{F}$ and hence $[\mathbb{F}(\alpha) : \mathbb{F}] = 2$.
(c) Use Dedekind's Tower Law to prove that there **does not exist** any intermediate field:

$$\mathbb{F} \subsetneq \mathbb{K} \subsetneq \mathbb{F}(\alpha).$$

(d) Prove that the function $\sigma : \mathbb{F}(\alpha) \to \mathbb{F}(\alpha)$ defined by $\sigma(a + b\alpha) := a - b\alpha$ is a field automorphism. We call this operation *conjugation*.

---

[1] This will be true if $\mathbb{E}$ is the splitting field of a polynomial over $\mathbb{F}$.

5. Square Roots are Irrational. Let $D \in \mathbb{N}$ be a positive integer and let $\sqrt{D} \in \mathbb{R}$ be any real square root. In this problem you will show that

$$\sqrt{D} \notin \mathbb{Z} \quad \Longrightarrow \quad \sqrt{D} \notin \mathbb{Q}.$$

(a) Consider the set $S = \{n \in \mathbb{N} : n\sqrt{D} \in \mathbb{Z}\} \subseteq \mathbb{N}$. Observe that

$$S = \emptyset \quad \Longleftrightarrow \quad \sqrt{D} \notin \mathbb{Q}.$$

(b) Assuming that $\sqrt{D} \notin \mathbb{Z}$, use Well-Ordering to prove that there exists $a \in \mathbb{Z}$ such that

$$a < \sqrt{D} < a + 1.$$

(c) Suppose in addition that $\sqrt{D} \in \mathbb{Q}$. By part (a) and Well-Ordering, this means that the set S has a smallest element, say $m \in S$. Now use part (b) to obtain a contradiction. [Hint: Consider the number $m(\sqrt{D} - a)$.]

6. An Interesting Example. Let $\sqrt{2}, \sqrt{3} \in \mathbb{R}$ be some specific square roots of 2 and 3, and consider the subfields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$. We saw in class that the union $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ is **not** a subfield. So instead we will consider the join/compositum subfield:

$$\mathbb{Q}(\sqrt{2}) \vee \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{R}.$$

(a) **A Basis.** Prove that elements of this field have the following explicit form:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}.$$

[Hint: It's quite tricky to prove directly that the set on the right is a field. Use Dedekind's Tower Law for an indirect proof.]

(b) **The Galois Group.** Let $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ be any field automorphism. Prove that σ necessarily fixes the prime subfield $\mathbb{Q}$, and hence that σ is uniquely determined by the two values $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Write down all of the possibilities and observe that you get a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) **A Primitive Element.** Define the number $\alpha := \sqrt{2} + \sqrt{3}$ and prove that

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha).$$

[Hint: One inclusion is easy. For the other inclusion, expand α^3 to show that $\sqrt{2}$ and $\sqrt{3}$ are in the field $\mathbb{Q}(\alpha)$.] You know from part (a) that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. It follows that the five elements $1, \alpha, \alpha^2, \alpha^3, \alpha^4 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ are **not** linearly independent over $\mathbb{Q}$, hence α must satisfy a quartic equation of the form

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 = 0 \quad \text{for some nontrivial } a, b, c, d, e \in \mathbb{Q}.$$

Find this equation. [Hint: Expand α^4 and work down.] If $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is any field automorphism, prove that $\sigma(\alpha)$ is another solution of the same equation. Finally, use part (b) to obtain all four roots of the equation.