Math 371 / Problem Set 8 (2 pages)

- **Study/read**
  - Ch. 13 of *Abstract Algebra* by Dummit–Foote.
  - Ch. VI, X of *Abstract Algebra* by Fraleigh.

(!) Make sure that you understand the definitions, examples, theorems, etc.

- **Solve the problems below:**

1) Let \( \iota : F \rightarrow E \) be a field isomorphism, and \( \overline{F}/F, \overline{E}/E \) be algebraic closures. For every polynomial \( f(t) = a_n t^n + \cdots + a_0 \in F[t] \), set \( b_i = \iota(a_i) \), and \( g(t) = \iota(f(t)) := b_n t^n + \cdots + b_0 \in E[t] \) be the image of \( f(t) \) under \( \iota \). Prove the following generalizations of assertions proved in the class:

   a) \( \iota : F \rightarrow E \) can be extended to a field morphism \( \overline{\iota} : \overline{F} \rightarrow \overline{E} \).

   b) Every extension \( \overline{\iota} : \overline{F} \rightarrow \overline{E} \) maps the splitting field \( F_f \subset \overline{F} \) of \( f(t) \) isomorphically to the splitting field \( E_g \subset \overline{E} \) of \( g(t) \).

   c) Deduce from this that every extension \( \overline{\iota} : \overline{F} \rightarrow \overline{E} \) is an isomorphism.

2) Find the degree, a basis of \( F' \mid F \), and a generator, in the following cases:

   a) \( F = \mathbb{Q} \) and
     i) \( F' = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \); respectively \( F' = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) \).
     ii) \( F' = \mathbb{Q}(\zeta_8, \zeta_{12}) \); respectively \( F' = \mathbb{Q}(\sqrt{5}, \zeta_5) \), where \( \zeta_n := e^{2\pi i n} \) denotes the first \( n \)th root of unity.

   b) Same questions over the field \( F = \mathbb{R} \).

   c) \( F = \mathbb{F}_5 \), and \( F' = \mathbb{F}(\sqrt{-1}, \sqrt{3}) \).

3) Give concrete descriptions of the splitting fields of the following polynomials (i) \( f(t) = t^3 - 6 \); (ii) \( f(t) = t^4 + t^2 + 1 \); (iii) \( f(t) = t^n - 2 \) over each of the fields: a) \( F = \mathbb{Q} \); b) \( F = \mathbb{F}_2 \); c) \( F = \mathbb{R} \).

4) **Frobenius endomorphism.** For an arbitrary field \( F \) prove:

   a) If \( F \) has characteristic \( \text{Char}(F) = p > 0 \), then \( \text{Frob}_p : F \rightarrow F, x \mapsto x^p \) is a field morphism, called the **Frobenius endomorphism**.

   b) For \( n > 1 \), define \( \varphi_n : F \rightarrow F \) by \( x \mapsto x^n \). Then \( \varphi_n \) is a field morphism iff \( n = p^e \) is some \( e \in \mathbb{N} \) and \( p = \text{Char}(F) \); equivalently, \( \varphi_n = \text{Frob}^e \).

**Definition.** A field \( F \) is called **perfect**, if either \( \text{Char}(F) = 0 \), or \( \text{Char}(F) = p > 0 \), and \( \text{Frob}_p : F \rightarrow F \) is an isomorphism.
Cyclotomic field extensions. Recall that given a field $F$, and $n > 0$, an element $a \in F$ is called a (primitive) $n$th root of unity, if $a^n = 1$ (and $n > 0$ is minimal with that property). For instance, $-1 \in \mathbb{C}$ is a 4th root of unity, but is not a primitive one, whereas $i := e^{2\pi i/4}$ is a primitive 4th root of unity in $\mathbb{C}$.

5) Let $F$ be an arbitrary field, $F'|F$ an algebraic extension of $F$, and $n > 0$ a natural number. Prove in all detail the assertions from the class:
   a) $\mu_{F,n} := \{a \in F | a^n = 1\}$ is a cyclic subgroup of $F^\times$ of order dividing $n$.
   b) If $p = \text{Char}(F) > 0$, and $n = n'p^e$ with $\gcd(p, n') = 1$, then $\mu_{F,n} = \mu_{F,n'}$.
   c) Let $F_n \subset F$ be the splitting field of $t^n - 1 \in F[t]$. Then $F_n = F(\mu_{F,n})$.

Terminology. The above $F_n$ is called the $n$th cyclotomic extension of $F$.

Finite fields. Let $F$ be a finite field. Then $\text{Char}(F) = p > 0$ iff $\mathbb{F}_p$ is the prime field of $F$ (WHY), and if so, $F|\mathbb{F}_p$ is a finite extension (WHY).

6) Let $F|\mathbb{F}_p$ be a finite field extension, and $m := [F : \mathbb{F}_p]$. Prove the following:
   a) $F^\times$ consists of roots of unity.
      • Precisely, $F^\times = \mu_{F,n}$, where $n = p^m - 1$.
   b) Hence $F$ is the splitting field of $t^{p^m} - t \in \mathbb{F}_p[t]$, and therefore all finite extension of $\mathbb{F}_p$ of degree $m$ are isomorphic.
   c) Finally, the splitting field of $t^{p^m} - t \in \mathbb{F}_p[t]$ is a finite extension of $\mathbb{F}_p$ of degree $m$.

Notation: The typical finite extension of $\mathbb{F}_p$ of degree $m$ is denoted $\mathbb{F}_{p^m}$, and is called the finite field with $p^m$ elements.

Note: $\mathbb{Z}/p^m\mathbb{Z}$ is a ring with $p^m$ elements, but for $m > 1$, this is not a field!

7) Give a list of rings $R$ having either 4 or 9 elements, such that any ring $R'$ with either 4 or 9 elements is isomorphic to one precisely one $R$ on the list.