Due: Monday, Dec 10, 2018

Math 371 / Problem Set 9 (2 pages)

- **Study/read**

  - Ch. 13, 14 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:**

Let $F'|F$ be an algebraic field extension, $\overline{F}\,|F$ be a fixed algebraic extension, and $\mathcal{S}_{F'|F}$ be the set of all the field F-embeddings $\sigma : F' \to \overline{F}$, i.e., field morphisms $\sigma : F' \to F$ s.t. $\sigma(a) = a$ for all $a \in F$.

1) Let $F'|F$ be a finite extension. Then the following are equivalent:

i) $F'|F$ is separable, i.e., the minimal polynomial $p_\alpha(t) \in F[t]$ of each $\alpha \in F'$ is separable.

ii) $|\mathcal{S}_{F'|F}| = [F' : F\,]$.

[**Hint**: Proof by induction on $d := [F' : F]$, etc.]

2) Let $p(t) \in F[t]$ be an irreducible non-constant polynomial. Prove:

a) If $\mathrm{Char}(F) = 0$, then $p(t)$ is separable.

b) If $\mathrm{Char}(F) = p > 0$, the following are equivalent:

(i) $p(t)$ is separable; (ii) $p'(t) \neq 0$; (iii) $\exists\, p_1(t) \in F[t]$ s.t. $p(t) = p_1(t^p)$.

c) Moreover, in the context of b), there exists $e \geq 0$ and a separable irreducible polynomial $p_0(t) \in F[t]$ such that $p(t) = p_0(t^{p^e})$.

3) Find the Galois group and all the subfields of $F'|F$ in the following cases:

a) $F = \mathbb{Q}$ and

i) $F' = F(\sqrt{2}, \sqrt{3})$; respectively $F' = F(\sqrt{2}, \sqrt{3}, \sqrt{6})$.

ii) $F' = F(\zeta_8, \zeta_{12})$; respectively $F' = F(\sqrt{5}, \zeta_5)$, wehre $\zeta_n := e^{\frac{2\pi i}{n}}$.

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

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

4) Give concrete descriptions of the Galois groups of the 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) $F = \mathbb{R}$.

Cyclotomic field extensions. Recall that he cyclotomic polynomials $\Phi_n(t)$ are defined inductively on n implicitly as to satisfy $X^n - 1 = \prod_{d|n} \Phi_d(t)$.

5) Answer/prove the following:

a) Write down $\Phi_d(t)$ for $d = 1, 2, 3, 4, 5, 6, 7$.

b) What is the relationship between $\Phi_p(t)$ and $\Phi_{p^e}(t)$?

c) Show that $\deg \Phi_n(t) = \varphi(n)$, where $\varphi(n)$ is the Euler function Google it!

6) Knowing that $\Phi_d(t) \in \mathbb{Q}[t]$ is irreducible, prove that the map

$$\chi_n : \mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \to (\mathbb{Z}/n)^\times, \quad \zeta \mapsto \zeta^m, \quad (n, m) = 1$$

is an isomorphism.

7) What happens if one replaces $\mathbb{Q}$ by $\mathbb{F}_p$?