Homework #6

p. 197: 3.93, 3.94
p. 246: 4.21(i)

1. Let $K \subseteq L$ be fields. A subset S of L is called algebraically dependent over K if there exists a nonconstant polynomial $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ for some $n \geq 1$ and distinct elements $s_1, \ldots, s_n \in S$ such that $f(s_1, \ldots, s_n) = 0$. The set S is called algebraically independent over K if it is not algebraically dependent.
(a) Show that there exists a maximal algebraically independent (over K) set S contained in L.
(b) Show that the extension $L/K(S)$ is algebraic.
(*Remark:* Such a set S is called a transcendence basis for L/K. It can be shown that any two transcendence bases for L/K have the same cardinality.)

2. Let S be a transcendence basis for $\mathbb{C}/\mathbb{Q}$.
(a) Show that S is infinite (you may use the fact that an algebraic extension of an infinite field has the same cardinality as the field).
(b) Let π be a permutation of S. Show that there is an automorphism σ of $\mathbb{C}$ that gives the permutation π on S. Conclude that $\mathbb{C}$ has infinitely many automorphisms.

3. Let L be a field and let $\mathbb{Q}$ or $\mathbb{F}_p$ (p= prime) be the prime field contained in L. Let σ be an automorphism of L. Show that σ gives the identity map on the prime field. Conclude that the only automorphisms of $\mathbb{Q}$ and of $\mathbb{F}_p$ are trivial.

4. Let σ be an automorphism of $\mathbb{R}$.
(a) Show that σ maps positive reals to positive reals (*Hint:* positive reals are squares).
(b) Show that if $a > b$ then $\sigma(a) > \sigma(b)$.
(c) Show that σ is the identity map on $\mathbb{R}$ (problem 3 is useful here).

5. Let L/K be an extension of degree 2. Show that L/K is normal.

6. Let p be a prime and let ζ be a primitive pth root of unity.
(a) Show that the irreducible polynomial for ζ over $\mathbb{Q}$ is

$$\Phi(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = (X^p - 1)/(X - 1).$$

(b) Show that $\mathbb{Q}(\zeta)$ is the splitting field for $\Phi(X)$.
(c) Let σ be an automorphism of $\mathbb{Q}(\zeta)$. Show that $\sigma(\zeta) = \zeta^r$ for some integer $r \not\equiv 0 \pmod{p}$, and that $r \bmod p$ determines σ.
(d) Show that map $\sigma \mapsto c \in \mathbb{Z}_p^\times$ in part (c) is an injective group homomorphism from $\mathrm{Aut}(\mathbb{Q}(\zeta))$ to $\mathbb{Z}_p^\times$.
(e) Using the fact that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a separable and normal extension, show that $\mathrm{Aut}(\mathbb{Q}(\zeta))$ has order $p - 1$, hence is isomorphic to $\mathbb{Z}_p^\times$.