MATH 468
EXERCISE SET 4

A. ZEYTİN

(1) Verify the Galois correspondence for the following extensions
 i. $\mathbf{Q}(\sqrt{p}, \sqrt{q})/\mathbf{Q}$ where p and q are distinct prime numbers.
 ii. $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbf{Q}$
 iii. $\mathbf{Q}(\zeta_7)/\mathbf{Q}$.

(2) For relatively prime m and n in $\mathbf{Z}_{>0}$ let ζ_1 be any primitive n^{th} root of unity and ζ_2 be any primitive m^{th} root of unity. Show that $\zeta_1\zeta_2$ is a primitive mn^{th} root of unity.

(3) Let n be a postive odd integer. Prove that if a field contains a primitive n^{th} root of unity, then is also contains a primitive $(2n)^{\text{th}}$ root of unity, too!

(4) Show that if K/k is a finite extension then K may contain at most finitely many roots of unity.

(5) Let $n > 1$ be an odd integer and let Φ_n denote the n^{th} cyclotomic polynomial. Show that

$$\Phi_{2n}(X) = \Phi_n(-X).$$

(6) Prove that there are infinitely many prime numbers, p, with

$$p \equiv 1 \bmod n.$$

(Hint: Consider the group μ_n.)

Questions 7 - 9 are aimed at reminding you the structure of abelian groups. If you feel comfortable you may skip them.

(7) Let p be an odd prime and let $n \in \mathbf{Z}_{>0}$.
 i. Show that $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$ but $(1+p)^{p^{n-2}} \equiv 1 \bmod p^n$
 ii. Using (i.) conclude that $(1+p)$ is an element of order p^{n-1} in $(\mathbf{Z}/p^n\mathbf{Z})^{\times}$.

(8) Let $n \in \mathbf{Z}_{>2}$.
 i. Show that $(1+2^2)^{2^{n-2}} \equiv 1 \bmod p^n$ but $(1+2^2)^{2^{n-3}} \equiv 1 \bmod p^n$
 ii. Using (i.) conclude that 5 is an element of order 2^{n-2} in $(\mathbf{Z}/2^n\mathbf{Z})^{\times}$ for any $n \geq 3$.

(9) Show that $(\mathbf{Z}/2^n\mathbf{Z})^{\times}$ is not cyclic(i.e. generated by a single element) for any $n \geq 3$.
(Hint: Find two distinct subgroups of order 2. Why is this enough?)

(10) Recall that $\sigma_a \colon \mathbf{Q}(\zeta_n) \longrightarrow \mathbf{Q}(\zeta_n)$ is defined as $\sigma_a(\zeta_n) = (\zeta_n)^a$. Let ζ be any *primitive* n^{th} root of unity. Show that $\sigma_a(\zeta) = \zeta$.

(11) Let p be a prime number and $\zeta_1, \cdots, \zeta_{p-1}$ denote primitive p^{th} roots of unity. Define

$$\varepsilon_n = \zeta_1^n + \cdots + \zeta_{p-1}^n.$$

Prove that:
 i. $\varepsilon_n = -1$ if $p \nmid n$
 ii. $\varepsilon_n = p - 1$ if $p \mid n$
(Hint: Show that ε_n is a conjugate of ε_1 for p not dividing n. What is ε_1?)

(12) Prove that $\mathbf{Q}(\sqrt[3]{2})$ is not a subfield of *any* cyclotomic field $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$.

(13) Let $K = \mathbf{Q}(\zeta_n)$ and $k = \mathbf{Q}$ and consider the extension K/k.
 i. Show that complex conjugation $\bar{\cdot}\colon \mathbf{C} \longrightarrow \mathbf{C}$(Exercise Set 3, Problem 10) restricts to $\sigma_{-1} \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$; where σ_{-1} is defined as in Problem 10 of this exercise set.

ii. Show that the field $K^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$ is contained in $\mathbf{R} \cap K$, i.e. imaginary parts of elements of K^+ are 0! K^+ is called the maximal real subfield of K.

Let now $n = 2^{n+2}$ and consider $K_n = \mathbf{Q}(\zeta_n)$ for $n \geq 0$ and $\alpha_n = \zeta_n + \zeta_n^{-1}$.

iii. Show that for any $n \geq 0$

a. $[K_n : \mathbf{Q}] = 2^{n+1}$

b. $[K_n : K_n^+] = 2$

c. $[K_n^+ : \mathbf{Q}] = 2^n$

d. $[K_{n+1}^+ : K_n^+] = 2$

iv. Determine the equation satisfied by ζ_n over K_n^+ in terms of α_n

v. Show that $\alpha_{n+1}^2 = 2 + \alpha$

vi. Show that

$$\alpha_n = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}\,(\,n \text{ times}).$$

vii. Prove that K_n^+ is a cyclic extension (i.e. the automorphism group is cyclic) of $\mathbf{Q}$ of degree 2^n. (Hint: Show that $(\mathbf{Z}/2^{n+2}\mathbf{Z})^\times \cong (\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2^n\mathbf{Z})$.)

(14) Determine explicitly the multiplication table for $\mathbb{F}_8$ and $\mathbb{F}_9$.

(15) Set $q = p^m$ and consider $\mathbb{F}_q = \mathbb{F}_{p^m}$. Define $\sigma_q \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ as $\sigma_q(\alpha) = \alpha^q$. This exercise will prove the analogous results we prove in class for $\mathbb{F}_p$. Show that

i. σ_q fixes $\mathbb{F}_q$.

ii. every finite extension of $\mathbb{F}_q$ of degree n is the splitting field of $X^{q^n} - X$ over $\mathbb{F}_q$. Deduce that this extension is unique.

iii. every finite extension K of $\mathbb{F}_q$ of degree n is cyclic with σ_q as a generator of the group $\mathrm{Gal}(K/\mathbb{F}_q)$.

iv. there is a one to one correspondence between subfield of the unique extension K of $\mathbb{F}_q$ of degree n and divisors d of n.

(16) Prove that $n \mid \varphi(p^n - 1)$. (Hint: Show that $\varphi(p^n - 1) = \left|\left(\mathbf{Z}/(p^n - 1)\mathbf{Z}\right)^\times\right|$.)