

Homework 6

D. Zack Garza

October 23, 2019

Contents

1 Homework Problems	1
1.1 Problem 1	1
1.2 Problem 2	1
1.3 Problem 3	2
1.3.1 Part 1	2
1.3.2 Part 2	2
1.4 Problem 4	3
1.5 Problem 5	3
1.6 Problem 6	3
2 Qual Problems	3
2.1 Problem 1	3
2.2 Problem 2	3
2.3 Problem 3	3

1 Homework Problems

1.1 Problem 1

Todo

1.2 Problem 2

We can note that since f has 4 roots, the Galois group G of its splitting field will be a subgroup of S_4 . Moreover, G must be a *transitive subgroup* of S_4 , i.e. the action of G on the roots of f should be transitive. This reduces the possibilities to $G \cong S^4, A^4, D^4, \mathbb{Z}_4, \mathbb{Z}_2^2$.

Since f has exactly 2 real roots and thus a pair of roots that are complex conjugates, the automorphism given by complex conjugation is an element of G . But this corresponds to a 2-cycle $\tau = (ab)$, and we can then make the following conclusions:

- Not A_4 : A_4 contains only even cycles, and τ is odd.
- Not \mathbb{Z}_4 : This subgroup is generated by a single 4-cycle σ , which up to conjugacy is (1234) , and σ^n is not a 2-cycle for any n .

- Not \mathbb{Z}_2^2 : In order to be transitive, this subgroup must be $\{e, (12)(34), (13)(24), (14)(23)\}$, which does not contain τ .

The only remaining possibilities are S^4 and D^4 . \square

1.3 Problem 3

1.3.1 Part 1

To see that $\phi(n)$ is even for all $n > 2$, we can take a prime factorization of n and write

$$\phi(n) = \phi\left(\prod_{i=1}^m p_i^{k_i}\right) = \prod_{i=1}^m \phi(p_i^{k_i}) = \prod_{i=1}^m p_i^{k_i-1}(p_i - 1) = \prod_{i=1}^m p_i^{k_i-1} \prod_{i=1}^m (p_i - 1)$$

where each $k_i \geq 1 \implies k_i - 1 \geq 0$. But every prime power is odd, and a product of odd numbers is odd, so the first product is odd. It is also true that $p - 1$ is even for every prime p , and the second term is a product of even terms and thus even. So $\phi(n)$ is the product of an even and an odd number, which is always even.

1.3.2 Part 2

Suppose $\phi(n) = 2$. Take a prime factorization of n , so we have

$$2 = \phi(n) = \prod_{i=1}^m \phi(p_i^{k_i})$$

Since the only factors of 2 are 1 and 2, we must have $\phi(p_i^{k_i}) = 2$ for exactly one i , and the rest must be equal to 1.

Consider the term that equals 2. We have $\phi(p_i^{k_i}) = p_i^{k_i-1}(p_i - 1) = 2$, so we must have either

- Case 1: $p - 1 = 2$ and $p^{k_i-1} = 1$, so $p = 3$ and $k_i = 1$. So $3 \mid n$, but 3^ℓ does *not* divide n for any $\ell > 1$.
- Case 2: $p^{k_i-1} = 2$ and $(p - 1) = 1$, so $p = 2$ and $k_i = 2$. Thus 2^2 divides n but 2^ℓ does not for any $\ell > 2$.

In either case, it remains to check are whether the other factors where $\phi(p_j^{k_j}) = 1$ can contribute any other distinct divisors to n . We can note that $\phi(p_j^{k_j}) = 1$ iff $p_j^{k_j-1}(p_j - 1) = 1$, so this forces $p = 2$ and $k_j = 1$. So n may or may not contain a single factor of 2, but by uniqueness of prime factorization, this can only happen in case 1. Note that this also forces $2 \mid n$ but 2^2 does not divide n .

In summary, we've found that $\phi(n) = 2$ implies that

- $3 \mid n$, 9 does not divide n , and
 - $2 \mid n$, 4 does not divide n
 - 2 does not divide n
- $2^2 \mid n$, 2^3 does not divide n .

This reduces the possibilities to the finite set $n \in \{6, 3, 4\}$, and $\phi(6) = \phi(3) = \phi(4) = 2$. \square

1.4 Problem 4

Note that since $\zeta(\zeta + \zeta^{-1}) = \zeta^2 + 1$, we have the relation $\zeta^2 - (\zeta + \zeta^{-1})\zeta + 1 = 0$. But then

$$f(x) = x^2 - (\zeta + \zeta^{-1})x + 1$$

is a polynomial in $\mathbb{Q}(\zeta + \zeta^{-1})$ for which $f(\zeta) = 0$. Thus $g = \min(\zeta, \mathbb{Q}(\zeta + \zeta^{-1}))$ divides f , but since $\deg f = 2$ and $\mathbb{Q}(\zeta + \zeta^{-1})$ is totally real, $\zeta \notin \mathbb{Q}(\zeta + \zeta^{-1})$. This means that g can not be linear and must have degree at least 2, but the above argument shows that g has degree at *most* 2, so it must be 2. Letting $m = [\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}]$, we have

$$\begin{aligned} [\mathbb{Q}(\zeta) : \mathbb{Q}] &= [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})][\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] \\ \implies \phi(n) &= 2m, \end{aligned}$$

and so $m = \phi(n)/2$ as desired.

1.5 Problem 5

Suppose $F = K[\alpha_1, \dots, \alpha_n]$ where $\alpha_1^{n_1} \in K$ for some n_1 and }or each i we have $\alpha_i^{n_i} \in K[\alpha_1, \dots, \alpha_{i-1}]$ for some powers n_i . We want to show that $F = E[\beta_1, \dots, \beta_m]$ where each β_i satisfy a similar condition.

Let $A = \{\alpha_i \ni \alpha_i \notin E\}$, then it is since $E \hookrightarrow F$, adjoining all elements of A to E will yield exactly F . Using the order of α_i given by the definition of F as a radical extension, let β_1 be the $\alpha_i \in A$ with the smallest index i . Then by assumption, there is some m_1 such that $\beta_1^{m_1} \in K[\alpha_1, \dots, \alpha_{i-1}] \subset F$, so we can construct $F_1 := E[\beta_1]$ which will be a radical extension.

Inductively letting $A_2 = A \setminus \{\beta_1\}$ and repeating this process to construct L_2 will yield radical extensions at every step, and since A is finite, there is some n such that $L_n = L$. But then L is a radical extension over E as desired.

1.6 Problem 6

2 Qual Problems

2.1 Problem 1

2.2 Problem 2

2.3 Problem 3