GALOIS THEORY: FUNDAMENTAL THEOREM OF ALGEBRA

A Discussion Exercise to review the Fundamental Theorem of Galois Theory

Fact from group theory: If G is a group of order p^m where p is prime and $m \in \mathbb{Z}_+$, then G has a subgroup H so that $[G : H] = p$.

Goal. Take $f \in \mathbb{R}[t] \setminus \mathbb{R}$ and let $L : \mathbb{C}$ be a splitting field extension for f. Identifying $\mathbb{C}$ with its isomorphic image in L, assume that $\mathbb{R} \subseteq \mathbb{C} \subseteq L$. The goal is to show that $L = \mathbb{C}$.

1. Why is $L : \mathbb{R}$ a splitting field extension for $(t^2 + 1)f$?
2. Is $L : \mathbb{R}$ a finite Galois extension?
3. Set $G = Gal(L : \mathbb{R})$. Is $|G|$ even?
4. Let H be a Sylow 2-subgroup of G. Set $d = [G : H]$. Is d even?
5. Set $M = Fix_L(H)$. What is $[M : \mathbb{R}]$?
6. Is $M : \mathbb{R}$ a simple extension?
7. Take $\gamma \in M$ so that $M = \mathbb{R}(\gamma)$. Is γ algebraic over $\mathbb{R}$?
8. Set $g = m_\gamma(\mathbb{R})$. What is $\deg g$?
9. By Calculus, as $\deg g = d$ is odd [see #4], g has a real root that we call β. How does β relate to γ?
10. What does this tell us about H?
11. As $G = H$ what does this tell us about $|G|$?
12. Take $m \in \mathbb{Z}_+$ so that $|G'| = 2^m$. Set $G' = Gal(L : \mathbb{C})$. What can we say about $|G'|$?
13. We want to show that $m = 1$, and hence $L = \mathbb{C}$. For the sake of contradiction, suppose that $m > 1$. Let H' be a subgroup of G' with $[G' : H'] = 2$, and set $M' = Fix_L(H')$. Is $M' : \mathbb{C}$ a Galois extension?
14. Take $\gamma' \in M'$ so that $M' = \mathbb{C}(\gamma')$, and set $g' = m_{\gamma'}(\mathbb{C})$. Thus $\deg g' = [M' : \mathbb{C}] = |Gal(M' : \mathbb{C})|$. Which integer is $\deg g'$?
15. Write $g' = t^2 - bt - c$ where $b, c \in \mathbb{C}$, and write $b^2 - 4c = r\,\mathrm{e}^{i\theta}$ where $r, \theta \in \mathbb{R}_{\geq 0}$. Does $b^2 - 4c$ have a square root in $\mathbb{C}$?
16. Does this yield a contradiction? What can we conclude?

Note: For $h \in \mathbb{C}[t]\mathbb{C}$, take $f = h\overline{h}$ (where $\overline{h}$ is the complex conjugate of h). So $f \in \mathbb{R}[t]\mathbb{R}$. As f splits over $\mathbb{C}$, so does h.