

Homework 7

Proofs and explanations should always be written using complete English sentences. You should always explain and justify each of the steps in your solution, unless otherwise noted. Write your name and "Math 114" on the top right of the first page.

1. Let $L : K$ be a finite normal field extension. By Theorem 8.4 there exists $f \in K[t]$ such that L is a splitting field for f . Let $n = \deg(f)$. Prove that the Galois group $\Gamma(L : K)$ is isomorphic to a subgroup of the symmetric group S_n . (Proceed as in Stewart's exercise 7.5, i.e. show that $\Gamma(L : K)$ is isomorphic to a subgroup of the group of permutations of the roots of f .) What can you say about $\Gamma(L : K)$ if f is reducible? What can you say about $\Gamma(L : K)$ if f is inseparable?

Solution:

Let $A = \{\alpha_1, \dots, \alpha_r\}$ be the zeros of f in L . Then $L = K(\alpha_1, \dots, \alpha_r)$. The minimal polynomial of α_i over K is an irreducible factor of f , so the other roots of the minimal polynomial of α_i are some of the α_j . If $\gamma \in \Gamma(L : K)$, then $\gamma(\alpha_i)$ has the same minimal polynomial as α_i , so $\gamma(\alpha_i) = \alpha_j$ for some j . (The proof of exercise 7.5 carries over.) Then γ induces a map from A to A , which is injective, so bijective since A is finite (see proof for exercise 7.5). We get a group homomorphism from the Galois group to the group S_A of all permutations of A (since in both groups the operation is composition of maps). Since A has $r \leq n$ elements, S_A is isomorphic to S_r , which is isomorphic to a subgroup of S_n , so every subgroup of S_A is isomorphic to a subgroup of S_n . It remains to show that the homomorphism $\Gamma(L : K) \rightarrow S_A$ is injective (so that $\Gamma(L : K)$ is isomorphic to a subgroup of S_A). But let γ be an element of the kernel of this homomorphism. Then γ is a K -automorphism of $K(\alpha_1, \dots, \alpha_r)$, which also maps every α_i to itself. It follows that γ also maps every rational expression in $\alpha_1, \dots, \alpha_r$ to itself, so γ is the identity map of L . So the kernel is trivial and we have an injective homomorphism.

If f is reducible, then not all permutations are possible: $\gamma(\alpha_i) = \alpha_j$ for some j which is a zero of the same irreducible factor. So if $f = f_1 \cdot \dots \cdot f_k$ is a decomposition into irreducible factors, $\deg(f_i) = n_i$, then $\Gamma(L : K)$ is isomorphic to a subgroup of $S_{n_1} \times \dots \times S_{n_k}$.

If f is inseparable, then $r < n$, so $\Gamma(L : K)$ is isomorphic to a subgroup of S_r with $r < n$. (If f is irreducible and inseparable, one can show that $r \leq \frac{n}{\text{char}(K)}$.)

2. Let $\Sigma \subset \mathbb{C}$ be the splitting field for $t^3 - 2 \in \mathbb{Q}[t]$. Show that the Galois group $\Gamma(\Sigma : \mathbb{Q})$ is isomorphic to the symmetric group S_3 . (Use the previous exercise, and two results from chapter 10.) Describe the elements of this Galois group, determine the subgroups of $\Gamma(\Sigma : \mathbb{Q})$ and find the corresponding fixed fields.

Solution:

By the previous exercise $\Gamma(\Sigma : \mathbb{Q})$ is isomorphic to a subgroup of the group of the permutations of the three zeros $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = e^{\frac{2\pi i}{3}} \sqrt[3]{2}$, $\alpha_3 = (e^{\frac{2\pi i}{3}})^2 \sqrt[3]{2} \in \Sigma$ of $t^3 - 2$. The extension is finite,

separable, normal, and of degree 6. (Recall that the polynomial does not split over $\mathbb{Q}(\sqrt[3]{2})$ which is of degree 3 over \mathbb{Q} , so one has to adjoin another zero which results in Σ having degree 6 over \mathbb{Q} .) Corollary 10.7 implies that $\Gamma(\Sigma : \mathbb{Q})$ has 6 elements, so it is isomorphic to S_3 . So every element of the Galois group corresponds bijectively to a permutation of $\alpha_1, \alpha_2, \alpha_3$. We have a subgroup corresponding to the trivial subgroup of S_3 with fixed field Σ , we have the subgroup $\Gamma(\Sigma : \mathbb{Q})$ of $\Gamma(\Sigma : \mathbb{Q})$, with fixed field \mathbb{Q} by Thm 10.8. We have three subgroups corresponding to the subgroups generated by transpositions in S_3 . By Corollary 9.5 their fixed fields are of degree $\frac{[\Sigma:\mathbb{Q}]}{2}=3$ over \mathbb{Q} , so we get the subfields

$\mathbb{Q}(\alpha_1) = \mathbb{Q}(\sqrt[3]{2})$ for the transposition which exchanges α_2 with α_3 ,

$\mathbb{Q}(\alpha_2) = \mathbb{Q}(e^{\frac{2\pi i}{3}} \sqrt[3]{2})$ for the transposition which exchanges α_1 with α_3 ,

$\mathbb{Q}(\alpha_3) = \mathbb{Q}((e^{\frac{2\pi i}{3}})^2 \sqrt[3]{2})$ for the transposition which exchanges α_1 with α_2 .

Finally we have the subgroup corresponding to A_3 with a fixed field of degree 2 over \mathbb{Q} , and its fixed field is $\mathbb{Q}(e^{\frac{2\pi i}{3}})$.

3. Stewart, exercise 11.5.

Hints: Find the other (complex) zeros of the minimal polynomial for γ , then use $\sqrt{2 - \sqrt{2}} = \frac{(\sqrt{2+\sqrt{2}})^2 - 2}{\sqrt{2+\sqrt{2}}}$. In order to compute the Galois group use again the first exercise (and two results from chapter 10): determine for every element of the Galois group the corresponding permutation of the set of roots of the minimal polynomial of γ . Finally determine the real and imaginary part of ϕ .

Solution:

Since the minimal polynomial for γ over \mathbb{Q} is $m = t^4 - 4t^2 + 2$ which involves only even powers, also $-\gamma$ is a root of m . The other two roots are $\pm\sqrt{2 - \sqrt{2}}$, which are also contained in $\mathbb{Q}(\gamma)$, since $\sqrt{2 - \sqrt{2}} = \frac{\gamma^2 - 2}{\gamma}$. So $\mathbb{Q}(\gamma) : \mathbb{Q}$ is a splitting field extension, hence finite, normal (and separable). By Corollary 10.7 the Galois group has 4 elements (the degree of m). By Proposition 10.2 the four elements ϕ_1, \dots, ϕ_4 of the Galois group can be numbered so that $\phi_1(\gamma) = \gamma$, $\phi_2(\gamma) = -\gamma$, $\phi_3(\gamma) = \frac{\gamma^2 - 2}{\gamma}$, $\phi_4(\gamma) = -\frac{\gamma^2 - 2}{\gamma}$. From the formula $-\sqrt{2 + \sqrt{2}} = \frac{(\sqrt{2 - \sqrt{2}})^2 - 2}{\sqrt{2 - \sqrt{2}}}$ it follows that ϕ_3 has order 4, so the Galois group is isomorphic to \mathbb{Z}_4 .

Finally $\phi = \frac{1 + \sqrt{2 + i}}{\sqrt{2}\sqrt{2 + \sqrt{2}}}$, $\phi^2 = \frac{1 + i}{\sqrt{2}}$, $\phi^4 = i$, $\phi^8 = -1$, so ϕ has a minimal polynomial over \mathbb{Q} of degree at most 8, and $\mathbb{Q}(\phi)$ contains i , so it contains $\sqrt{2}$, so it contains γ , so it contains $\mathbb{Q}(\gamma, i)$ which is of degree 8 over \mathbb{Q} since $i \notin \mathbb{Q}(\gamma)$. So we must have $\mathbb{Q}(\phi) = \mathbb{Q}(\gamma, i)$.

4. Stewart, exercise 12.1 (a), 12.2 (a) and 12.3(a).

Solution:

The extension is finite, separable and normal (it is the splitting field extension for $(t^2 - 2)(t^2 - 5)$). Since $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$, the extension has degree 4. The four elements of the Galois group are described by

$$\gamma_1(\sqrt{2}) = \sqrt{2}, \gamma_1(\sqrt{5}) = \sqrt{5},$$

$$\gamma_2(\sqrt{2}) = \sqrt{2}, \gamma_2(\sqrt{5}) = -\sqrt{5},$$

$$\gamma_3(\sqrt{2}) = -\sqrt{2}, \gamma_3(\sqrt{5}) = \sqrt{5},$$

$$\gamma_4(\sqrt{2}) = -\sqrt{2}, \gamma_4(\sqrt{5}) = -\sqrt{5}.$$

All maps have order 2, so the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. The subgroups are the trivial

subgroup with fixed field $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, the whole group with fixed field \mathbb{Q} by theorem 10.8,
 $\{\gamma_1, \gamma_2\}$ with fixed field of degree 2 over \mathbb{Q} by corollary 9.5, so the fixed field is $\mathbb{Q}(\sqrt{2})$,
 $\{\gamma_1, \gamma_3\}$ with fixed field of degree 2 over \mathbb{Q} by corollary 9.5, so the fixed field is $\mathbb{Q}(\sqrt{5})$,
 $\{\gamma_1, \gamma_4\}$ with fixed field of degree 2 over \mathbb{Q} by corollary 9.5, so the fixed field is $\mathbb{Q}(\sqrt{10})$.