PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 10 (Apr 11 – Apr 18)

1 (10+10+5+5) Let $K, E, F \subseteq L$ be fields, $E : K$, $F : K$ be finite extensions. Prove:

a) if $E : K$ is separable, then $EF : F$ is separable;

b) if $E : K$ and $F : K$ are both separable, then $EF : K$ and $E \cap F : K$ are both separable;

c) if $E : K$ is Galois, then $EF : F$ is Galois;

d) if $E : K$ and $F : K$ are both Galois, then $EF : K$ and $E \cap F : K$ are both Galois.

2 (5+5+10) *a*) Find the splitting field L of the polynomial $f(t) = t^4 - 4t^2 + 5$.

b) Prove that $[L : \mathbb{Q}]$ is either 4 or 8.

c) Find 10 intermediate fields of the extension $L : \mathbb{Q}$ and their degrees.

d) (for enthusiasts) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(f)$.

3 (30) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(t^6 + 3)$. *Hint*: Use the calculations (and the notation, if you like) from Lecture 18.

Solutions

General remark. If there is a typo in any task, then the maximum score will be awarded for that task.

1 (10+10+5+5) Let $K, E, F \subseteq L$ be fields, $E : K$, $F : K$ be finite extensions. Prove:

a) if $E : K$ is separable, then $EF : F$ is separable;

b) if $E : K$ and $F : K$ are both separable, then $EF : K$ and $E \cap F : K$ are both separable;

c) if $E : K$ is Galois, then $EF : F$ is Galois;

d) if $E : K$ and $F : K$ are both Galois, then $EF : K$ and $E \cap F : K$ are both Galois.

Solution. *a*) By assumption $E : K$ is separable hence using the primitive element theorem, we see that $E = K(\theta)$, where $\theta \in E$ is separable over K. In particular, θ is separable over F. Further, we have $EF = F(\theta)$ (see lectures) and by the main result on separability (Theorems 1,1' of Lecture 14) $F(\theta) : F$ is separable.

b) By assumption $F : K$ is separable and by the first part we know that $EF : F$ is separable. Hence $EF : K$ is also separable (Theorems 1,1' of Lecture 14). As for the second part, consider the extension $K - E \cap F - E$ and by assumption $K - E$ is separable. Then $K - E \cap F$ is also separable (Theorems 1,1' of Lecture 14).

Finally, to obtain c, d) combine a, b) and parts 3,4 of the first lemma of Lecture 22.

2 (5+5+10) *a*) Find the splitting field L of the polynomial $f(t) = t^4 - 4t^2 + 5$.

b) Prove that $[L : \mathbb{Q}]$ is either 4 or 8.

c) Find 10 intermediate fields of the extension $L : \mathbb{Q}$ and their degrees.

d) (for enthusiasts) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(f)$.

Solution. *a*), *b*). One has $f(t) = t^4 - 4t^2 + 5 = (t^2 - 2)^2 + 1$ and hence the splitting field of f is $L = \mathbb{Q}(\alpha_1, \alpha_2)$, where $\alpha_1 = \sqrt{2+i}$ and $\alpha_2 = \sqrt{2-i}$. Also, $\alpha_1\alpha_2 = \sqrt{5}$ therefore $L = \mathbb{Q}(\alpha_1, \sqrt{5})$. Thus $[L : \mathbb{Q}]$ is either 4 or 8.

c) Clearly, L contains three distinct quadratic subfields $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\alpha_1^2) = \mathbb{Q}(i)$ and hence $\mathbb{Q}(i\sqrt{5})$. Also, the composite field $\mathbb{Q}(i, \sqrt{5})$ contains all these fields and obviously the degree $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}]$ is 4. Other fields of degree four are $\mathbb{Q}(\alpha_1), \mathbb{Q}(\alpha_2)$ (they both contain $\mathbb{Q}(i)$) and $\mathbb{Q}(\alpha_1 + \alpha_2), \mathbb{Q}(\alpha_1 - \alpha_2)$ (they both contain $\mathbb{Q}(\sqrt{5})$, consider $(\alpha_1 + \alpha_2)^2$ and $(\alpha_1 - \alpha_2)^2$). Of course, it remains to be proven that all these intermediate fields are distinct, but full score goes to just pointing out the above fields.

d) We claim that $[L : \mathbb{Q}] = 8$ and that above we have found the complete list of intermediate fields of L (plus $\mathbb{Q}$ and L, of course). To prove this we need to determine the structure of $G := \mathrm{Gal}_{\mathbb{Q}}(f)$. We will look at this later in class *(time permitting)* but the fact that $[L : \mathbb{Q}] = 8$ is not so hard to see. Indeed, if $|G| = [L : \mathbb{Q}] = 4$, then all fields of degree 4 coincide with $\mathbb{Q}(i, \sqrt{5})$ and this field has the Galois group V_4 (see lectures). Namely, put $\alpha_1' = -\alpha_1$, $\alpha_2' = -\alpha_2$ and $\rho_1(i) = -i$, $\rho_2(\sqrt{5}) = -\sqrt{5}$, then $\rho_1^2 = \rho_2^2 = Id$ and $G = \langle \rho_1, \rho_2 \rangle = V_4$. Moreover, $\rho_1(\alpha_1) = \alpha_1'$, $\rho_1(\alpha_2) = \alpha_2'$ and for G to be transitive we must either swap α_1, α_2, swap α_1, α_2', or swap α_2, α_1' using ρ_2. All these possibilities are impossible. Indeed, let us take, say, the pair α_1, α_2 (the reasoning for α_1, α_2' and for α_2, α_1' is similar). Then we have $\alpha_1\alpha_2 = \sqrt{5}$ and therefore

$$\rho_2(\alpha_1)\rho_2(\alpha_2) = \rho_2(\sqrt{5}) = -\sqrt{5} = -\alpha_1\alpha_2 \,.$$

If $\rho_2(\alpha_1) = \alpha_2$ and $\rho_2(\alpha_2) = \alpha_1$, then we obtain a contradiction. Thus $|G| = [L : \mathbb{Q}] = 8$ (and above we found the complete list of intermediate fields of L).

3 (30) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(t^6 + 3)$. *Hint*: Use the calculations (and the notation, if you like) from Lecture 18.

Solution. By Lecture 18 we know that $G := \mathrm{Gal}_{\mathbb{Q}}(t^6 + 3) \cong D_3 \cong S_3$. This group contains $A_3 \cong \mathbb{Z}_3$ and three groups generated by transpositions τ_1, τ_2 and τ_3. None of these groups are contained in the other. We know that the splitting field L is $\mathbb{Q}(r,\varepsilon) = \mathbb{Q}(i3^{1/6})$, where $r = i3^{1/6}$, $\varepsilon = \varepsilon_6 = (1+i\sqrt{3})/2$ and as we have seen in lectures (or one can easily check) $r^3 = -i\sqrt{3}$. Clearly, L corresponds to $\{e\}$ and $\mathbb{Q}$ corresponds to the whole Galois group G. Also, we know that G is generated by the rotation ρ^2 which moves $r \to r\varepsilon^2$ and $\varepsilon \to \varepsilon$ and by the symmetry σ, where $\sigma(r) = r\varepsilon$, $\sigma(\varepsilon) = \varepsilon^{-1}$. Now $A_3 \cong \langle \rho^2 \rangle$ corresponds to $\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\varepsilon)$ (notice that $i\sqrt{3} = -r^3$ and clearly ρ^2 fixes $\varepsilon = (1+i\sqrt{3})/2$). The remaining subgroups $\langle \tau_1 \rangle, \langle \tau_2 \rangle, \langle \tau_3 \rangle$ can be alternatively denoted as $\langle \sigma \rangle, \langle \sigma\rho^2 \rangle, \langle \rho^2\sigma \rangle$, it is easy to see that these groups of order two. Now

$$\sigma(r + r\varepsilon) = r\varepsilon + r\varepsilon\varepsilon^{-1} = r + r\varepsilon\,,$$

and

$$\sigma\rho^2(r + r\varepsilon^{-1}) = \sigma(r\varepsilon^2 + r\varepsilon) = r\varepsilon\varepsilon^{-2} + r\varepsilon\varepsilon^{-1} = r + r\varepsilon^{-1}\,.$$

Thus $\langle \sigma \rangle$ fixes $\mathbb{Q}(r(1+\varepsilon))$ and $\langle \sigma\rho^2 \rangle$ fixes $\mathbb{Q}(r + r\varepsilon^{-1})$. Finally, clearly, $\rho^2\sigma(\varepsilon) = \varepsilon^{-1} = \overline{\varepsilon}$ and

$$\rho^2\sigma(r) = \rho^2 r\varepsilon = r\varepsilon^3 = -r\,.$$

Thus $\rho^2\sigma$ is just the complex conjugation and hence $\langle \rho^2\sigma \rangle$ preserves $\mathbb{Q}(r^2) = \mathbb{Q}(3^{1/3})$.