PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 9 (Apr 4 – Apr 11)

1 (10+5) *a*) Let L be the splitting field of the polynomial $t^{13}-1$. Find all subgroups of $\mathrm{Gal}_{\mathbb{Q}}(L)$.
b) How many intermediate subfields are there in the extension $L:\mathbb{Q}$?

2 (10) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$. Find orders of all subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$.

3 (10) Prove Artin's theorem: let $[L:K]<\infty$, $G:=\mathrm{Gal}_K(L)$. Then $[L:L^G]$ is a Galois extension.

4 (10) Let $L:K$ be a finite Galois extension, $G:=\mathrm{Gal}_K(L)$. For any $\alpha\in L$ define

$$\mathrm{Tr}(\alpha)=\sum_{g\in G} g(\alpha) \qquad \text{and} \qquad \mathrm{Norm}(\alpha)=\prod_{g\in G} g(\alpha)\,.$$

Prove that for an arbitrary $\alpha\in L$ one has $\mathrm{Tr}(\alpha),\mathrm{Norm}(\alpha)\in K$.

5 (15+15) *a*) Find all of the subfields of $\mathbb{Q}(2^{1/3},e^{2\pi i/3})$.
b) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3},e^{2\pi i/3}))$.

Solutions

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

1 (10+5) *a*) Let L be the splitting field of the polynomial $t^{13}-1$. Find all subgroups of $\mathrm{Gal}_{\mathbb{Q}}(L)$.
b) How many intermediate subfields are there in the extension $L:\mathbb{Q}$?

Solution. *a*) Let $G=\mathrm{Gal}_{\mathbb{Q}}(t^{13}-1)$ and we know (see lectures) that G is isomorphic to the cyclic group $\mathbb{Z}_{12}=\langle g\rangle$. It has four non–trivial subgroups $\langle g^6\rangle$, $\langle g^4\rangle$, $\langle g^3\rangle$, $\langle g^2\rangle$.

b) In total we have 6 subgroups of G and hence 6 intermediate subfields thanks to the fundamental theorem of Galois theory.

2 (10) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$. Find orders of all subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$.

Solution. We have subfields $\mathbb{F}_3-\mathbb{F}_{3^2}-\mathbb{F}_{3^4}-\mathbb{F}_{3^8}$ and $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})\cong\mathbb{Z}_8=\langle\Phi\rangle$, where Φ is the Frobenius automorphism (see lectures). Thus the correspondent subgroups are $\langle\Phi\rangle-\langle\Phi^2\rangle-\langle\Phi^4\rangle-Id$ and their orders are $8,4,2$ and 1.

3 (10) Prove Artin's theorem: let $[L:K]<\infty$, $G:=\mathrm{Gal}_K(L)$. Then $[L:L^G]$ is a Galois extension.

Solution. By Theorem 2 of Lecture 19 we need to check that $\mathrm{Fix}_L(G)=L^G=\mathrm{Fix}_L(\mathrm{Gal}_{L^G}(L))=\mathrm{Fix}_L(G_{L^G})$. But by the 6 part of Theorem 1 of the same lecture (applied to $G=\mathrm{Gal}_K(L)$) we know exactly that $\mathrm{Fix}_L(G)=\mathrm{Fix}_L(\mathrm{Gal}_{L^G}(L))$.

4 (10) Let $L:K$ be a finite Galois extension, $G:=\mathrm{Gal}_K(L)$. For any $\alpha\in L$ define

$$\mathrm{Tr}(\alpha)=\sum_{g\in G}g(\alpha)\qquad\text{and}\qquad\mathrm{Norm}(\alpha)=\prod_{g\in G}g(\alpha)\,.$$

Prove that for an arbitrary $\alpha\in L$ one has $\mathrm{Tr}(\alpha),\mathrm{Norm}(\alpha)\in K$.

Solution. Clearly, for any $g\in G$ one has $g(\mathrm{Tr}(\alpha))=\mathrm{Tr}(\alpha)$, and $g(\mathrm{Norm}(\alpha))=\mathrm{Norm}(\alpha)$. By assumption $L:K$ is Galois and hence the $L^G=K$. Thus $\mathrm{Tr}(\alpha),\mathrm{Norm}(\alpha)\in K$.

5 (15+15) *a*) Find all of the subfields of $\mathbb{Q}(2^{1/3},e^{2\pi i/3})$.
b) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3},e^{2\pi i/3}))$.

Solution. *a*) – *b*) Let $\varepsilon=e^{2\pi i/3}$, $\alpha=2^{1/3}$ and $L=\mathbb{Q}(2^{1/3},e^{2\pi i/3})$. One can think about L as the splitting field of $f(t)=t^3-2$. By the tower law one has $[L:\mathbb{Q}]=[L:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot3=6$ and hence $G:=\mathrm{Gal}_{\mathbb{Q}}(L)\cong S_3$ (see lectures). The subfields are $\mathbb{Q},\mathbb{Q}(\alpha),\mathbb{Q}(\varepsilon),\mathbb{Q}(\alpha\varepsilon),\mathbb{Q}(\alpha\varepsilon^2)$ and $\mathbb{Q}(\alpha,\varepsilon)$ and it is easy to check that they are different. There are no other fields as there are exactly six subgroups of G. Indeed,

$$S_3\cong D_3\cong M_3=\{\sigma_{k,l}\ :\ \varepsilon\to\varepsilon^k,\ \alpha\to\alpha\varepsilon^l,\ k=1,2,\ l=0,1,2\}\,.$$

Let

$$\sigma:=\sigma_{1,1}:\qquad\sigma(\varepsilon)=\varepsilon,\quad\sigma(\alpha)=\alpha\varepsilon \tag{1}$$

be a circle of length three (σ cyclically permutes $\alpha,\alpha\varepsilon,\alpha\varepsilon^2$) and

$$\tau:=\sigma_{2,0}:\qquad\tau(\alpha)=\alpha,\quad\tau(\varepsilon)=\varepsilon^2 \tag{2}$$

be a transposition (it interchanges two of the roots (namely, $\alpha\varepsilon$ and $\alpha\varepsilon^2$), leaving the third root α fixed). Clearly, $S_3=\langle\sigma,\tau\rangle$. Then

$$\mathbb{Q},\mathbb{Q}(\alpha),\mathbb{Q}(\varepsilon),\mathbb{Q}(\alpha\varepsilon),\mathbb{Q}(\alpha\varepsilon^2),\mathbb{Q}(\alpha,\varepsilon)$$

correspond to the subgroups

$$G, \langle\tau\rangle, \langle\sigma\rangle, \langle\sigma^2\tau\rangle, \langle\sigma\tau\rangle, Id$$

(of orders $6, 2, 3, 2, 2$ and 1). Indeed, clearly, $\langle\sigma\rangle$ fixes $\mathbb{Q}(\varepsilon)$ and since $\tau(\alpha) = \alpha$, $\tau(\varepsilon) = \varepsilon^2$ it follows that $\langle\tau\rangle$ fixes $\mathbb{Q}(\alpha)$. Now using (1), (2) one has

$$\sigma^2\tau(\alpha\varepsilon) = \sigma^2(\alpha\varepsilon^2) = \sigma(\alpha) = \alpha\varepsilon\,,$$

and

$$\sigma\tau(\alpha\varepsilon^2) = \sigma(\alpha\varepsilon) = \alpha\varepsilon^2\,.$$

Therefore, $\langle\sigma^2\tau\rangle$ fixes $\mathbb{Q}(\alpha\varepsilon)$ and $\langle\sigma\tau\rangle$ fixes $\mathbb{Q}(\alpha\varepsilon^2)$.