PURDUE UNIVERSITY
Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 6 (Feb 28 – Mar 7)

1 (5+10+10) Find Galois groups for the following polynomials f over $\mathbb{Q}$:
1) $(t^2-3)(t^2+1)$
2) t^4-t^2+1
3) t^4-2

2 (10+10) 1) Find $\mathrm{Gal}_{\mathbb{F}_3(t^2)}(\mathbb{F}_3(t))$.
2) Find $\mathrm{Gal}_{\mathbb{F}_2(t^2)}(\mathbb{F}_2(t))$.

3 (10+5) (a) Let $K-M-L$ be a field extension and $L:K$ is a normal extension. Prove that $L:M$ is also a normal extension.
(b) Give an example of three fields K,M,L such that $[L:K]=4$ and $[M:K]=[L:M]=2$ (hence $K-M$ and $M-L$ are normal extensions) but $L:K$ is not a normal extension.

4 (10) Let $L:K$ be a splitting field extension for a non–constant polynomial $f\in K[t]$. Prove that $|\mathrm{Gal}_L(K)|$ divides $(\deg f)!$.

5 (15+20) $a)$ Let $f=t^3+t+1\in\mathbb{F}_2[t]$. Prove that $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$.
$b)$ Let $f=t^3+t^2+1\in\mathbb{F}_2[t]$. Prove that $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$.

Solutions

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

1 Find Galois groups for the following polynomials f over $\mathbb{Q}$:
1) $(t^2-3)(t^2+1)$
2) t^4-t^2+1
3) t^4-2

Solution. 1) The splitting field is $\mathbb{Q}(\sqrt{3},i)$ hence $\mathrm{Gal}_{\mathbb{Q}}(f)\cong \mathbb{Z}_2\oplus\mathbb{Z}_2$ (see lectures).

2) The roots of f are $e^{\pm\pi i/6}, e^{\pm 7\pi i/6}$, so the splitting field is $\mathbb{Q}(\sqrt{3},i)$ and thus we have $\mathrm{Gal}_{\mathbb{Q}}(f)\cong \mathbb{Z}_2\oplus\mathbb{Z}_2$ again.

3) The splitting field is $\mathbb{Q}(2^{1/4},i)$ and the degree $[\mathbb{Q}(2^{1/4},i):\mathbb{Q}]=8$. Thus $\mathrm{Gal}_{\mathbb{Q}}(f)\cong D_4$ (see lectures).

2 1) Find $\mathrm{Gal}_{\mathbb{F}_3(t^2)}(\mathbb{F}_3(t))$.
2) Find $\mathrm{Gal}_{\mathbb{F}_2(t^2)}(\mathbb{F}_2(t))$.

Solution. 1) We have the following extension $L:K$, where $K=\mathbb{F}_3(t^2)$ and $L=\mathbb{F}_3(t)$. One has $f(x):=x^2-t^2\in K[t]$ and $f(t)=0$. Thus t is algebraic over K. Clearly, $f(x)$ is irreducible over K and hence $[L:K]=2$. All roots of f are t and $-t$, where $t\neq -t$. Thus $\mathrm{Gal}_{\mathbb{F}_3(t^2)}(\mathbb{F}_3(t))\cong\mathbb{Z}_2$.

2) We have the following extension $L:K$, where $K=\mathbb{F}_2(t^2)$ and $L=\mathbb{F}_2(t)$. One has $f(x):=x^2-t^2\in K[t]$ and $f(t)=0$. Thus t is algebraic over K. Clearly, $f(x)$ is irreducible over K and hence $[L:K]=2$. But $x^2-t^2=(x-t)^2$ and therefore $\mathrm{Gal}_{\mathbb{F}_2(t^2)}(\mathbb{F}_2(t))\cong\{Id\}$.

3 (a) Let $K-M-L$ be a field extension and $L:K$ is a normal extension. Prove that $L:M$ is also a normal extension.
(b) Give an example of three fields K,M,L such that $[L:K]=4$ and $[M:K]=[L:M]=2$ (hence $K-M$ and $M-L$ are normal extensions) but $L:K$ is not a normal extension.

Solution. (a) Take any irreducible $f\in M[t]\setminus M$ and let $\alpha\in L$ be a root of f. We know that $\mu_\alpha^M|\mu_\alpha^K$ and that $f=c\mu_\alpha^M$, where $c\in M$. By assumption $L:K$ is normal and therefore μ_α^K splits over L. It follows that μ_α^M splits over L and thus $L:M$ is a normal extension.

(b) Take $f=t^4-2$, say, and put $M=\mathbb{Q}(\sqrt{2})$, $L=\mathbb{Q}(2^{1/4})$. Then $[M:K]=[L:M]=2$ but $L:K$ is not a normal extension as L contains $\pm i2^{1/4}$.

4 Let $L:K$ be a splitting field extension for a non–constant polynomial $f\in K[t]$. Prove that $|\mathrm{Gal}_L(K)|$ divides $(\deg f)!$.

Solution. We know that any $\tau\in\mathrm{Gal}_L(K)$ acts as a permutation on the distinct roots of f. Thus by the Lagrange theorem $|\mathrm{Gal}_L(K)|$ divides $n!$, where n is the number of distinct roots of f. Clearly, $n!$ divides $(\deg f)!$.

5 $a)$ Let $f=t^3+t+1\in\mathbb{F}_2[t]$. Prove that $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$.
$b)$ Let $f=t^3+t^2+1\in\mathbb{F}_2[t]$. Prove that $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$.

Solution. $a)$ Clearly, f is irreducible over $\mathbb{F}_2$ and if $f(\alpha)=0$, then

$$f(t)=(t+\alpha)(t^2+\alpha t+1+\alpha^2)=(t+\alpha)(t+\alpha^2)(t+\alpha+\alpha^2)\,.$$

Thus the splitting field $L=\mathbb{F}_2(\alpha)$, therefore $[L:\mathbb{F}_2]=3$ and hence $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$.

$b)$ Clearly, f is irreducible over $\mathbb{F}_2$ and if $f(\alpha)=0$, then

$$f(t)=(t+\alpha)(t^2+(1+\alpha)t+\alpha+\alpha^2)\,.$$

One can check that α^2 is another root of f and hence $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$ as above.

Another solution: $(t+1)^3 + (t+1) + 1 = t^3 + t + 1$ and we can use 5.a.

It was a misprint in 5.b (S_3 instead of $\mathbb{Z}_3$), so try either to get $\mathrm{Gal}_{\mathbb{F}_2}(f) \cong \mathbb{Z}_3$ or to disprove that $\mathrm{Gal}_{\mathbb{F}_2}(f) \cong S_3$. Both solutions deserve a full credit.