PURDUE UNIVERSITY
Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 4 (Feb 13 – Feb 21)

1 (5+5+15+20) For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
1) $t^4 + 7t^2 + 12$
2) $t^4 + t^2 - 12$
3) $t^{2n} - 2^n$, where $n = 3, 4$.
4) $t^{14} - 1$.

2 (15) Let $K - L - M$ be a field extension and $K - L$, $L - M$ are algebraic extensions. Prove that $K - M$ is also an algebraic extension.

3 (15) Let α be transcendental over a field $K \subset \mathbb{C}$. Show that $K(\alpha)$ is not algebraically closed (hint: consider the polynomial $t^2 - \alpha$).

4 (15) Let $L : K$ be a splitting field extension for a non–constant polynomial $f \in K[t]$. Prove that $[L : K]$ divides $(\deg f)!$ (hint: at the very end look at some binomial coefficients).

Solutions

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

1 (5+5+15+20) For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L:\mathbb{Q}]$.

1) t^4+7t^2+12
2) t^4+t^2-12
3) $t^{2n}-2^n$, where $n=3,4$.
4) $t^{14}-1$.

Solution. 1) We have $t^4+7t^2+12=(t^2+3)(t^2+4)(t+i\sqrt{3})(t-i\sqrt{3})=(t+2i)(t-2i)$. Thus $L=\mathbb{Q}(i,i\sqrt{3})=\mathbb{Q}(i,\sqrt{3})$ is a splitting field of our polynomial. The degree $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$ is two, the degree $[L:\mathbb{Q}(\sqrt{3})]$ is two (since L is a complex field) and therefore by the tower law $[L:\mathbb{Q}]=4$.

2) We have $t^4+t^2-12=(t^2-3)(t^2+4)$. Thus $L=\mathbb{Q}(\sqrt{3},i)$ and the same argument as above shows that $[L:\mathbb{Q}]=4$.

3) We have $t^{2n}-2^n=\prod_{\varepsilon\in\sqrt[2n]{1}}(t-\varepsilon\sqrt{2})$. Thus $L=\mathbb{Q}(\sqrt{2},\varepsilon_{2n})$, where as always $\varepsilon_{2n}=e^{\pi i/n}$ and further $[\mathbb{Q}(\sqrt{2},\mathbb{Q}]=2$. One has $\varepsilon_{2n}+\varepsilon_{2n}^{-1}=2\cos\frac{\pi}{n}$ and $\varepsilon_{2n}\cdot\varepsilon_{2n}^{-1}=1$. Thus by the inverse Vieta theorem ε_{2n} is a root of the following quadratic equation $t^2-2\cos\frac{\pi}{n}\cdot t+1=0$. Compute the coefficient $2\cos\frac{\pi}{n}$ of this quadratic equation. For $n=3$ this is 1 and for $n=4$ this is $\sqrt{2}$. In any case we have a quadratic equation over $\mathbb{Q}(\sqrt{2})$. Thus $[L:\mathbb{Q}(\sqrt{2})]=2$ and by the tower law $[L:\mathbb{Q}]=4$.

4) We have $t^{14}-1=\prod_{\varepsilon\in\sqrt[7]{1}}(t^2-\varepsilon)$. Thus $L=\mathbb{Q}(\sqrt{\varepsilon_7})=\mathbb{Q}(\omega)$, where $\omega=e^{\pi i/7}$. Clearly, $\omega^7=-1$ and $(t^7+1)/(t+1)=t^6-t^5+t^4-t^3+t^2-t+1:=h(t)$. Thus $h(\omega)=0$ and hence $\deg(\mu_\omega^{\mathbb{Q}})\le 6$. Let us prove that $h=\mu_\omega^{\mathbb{Q}}$ and hence $[L:K]=6$. Indeed, other roots of h are $e^{k\pi i/7}$, where $k=1,3,5,9,11,13$. It is easy to see that if $h=h_1h_2$, then $\deg h_1,\deg h_2>2$ (otherwise either the sum or the product of roots of our quadratic equation is not in $\mathbb{Q}$) and hence $\deg h_1=\deg h_2=3$. Finally, by the Vieta formulae, the last case is also impossible.

Another argument. We know (see lectures) that the minimal polynomial of ε_n has degree $\varphi(n)$. Thus $[L:\mathbb{Q}]=\varphi(14)=6$.

2 (15) Let $K-L-M$ be a field extension and $K-L$, $L-M$ are algebraic extensions. Prove that $K-M$ is also an algebraic extension.

Solution. For an arbitrary $m\in M$ there is $f\in L[t]$ such that $f(m)=0$. One has $f=\sum_{j=0}^d l_jt^j$, where $l_j\in L$. Put $L'=K(l_0,l_1,\dots,l_d)$. Since L is algebraic over K and each $l_j\in L$, it follows that $[L':K]<\infty$. Also, $f\in L'[t]$, $f(m)=0$ and therefore m is algebraic over L'. Thus $[L'(m):L']<\infty$. Finally, by the tower law $[L'(m):K]=[L'(m):L'][L':K]<\infty$ and hence m is algebraic over K.

3 (15) Let α be transcendental over a field $K\subset\mathbb{C}$. Show that $K(\alpha)$ is not algebraically closed (hint: consider the polynomial $t^2-\alpha$).

Solution. Put $L=K(\alpha)$, then clearly, $t^2-\alpha\in L[t]$. If L is algebraically closed, then it must be $\beta\in L$ such that $\beta^2=\alpha$. We know that $L=K(\alpha)$ and therefore $\beta=f(\alpha)/h(\alpha)$, where $f,h\in K[t]$. Squaring, we get $f^2(\alpha)=\alpha h^2(\alpha)$ and hence α is a root of the polynomial $f^2(x)-xh^2(x)$. It is easy to check (compare the degrees of $f^2(x)$ and $xh^2(x)$) that this is a non–constant (nonzero) polynomial. We have obtained a contradiction with the assumption that α is transcendental over K.

4 (15) Let $L:K$ be a splitting field extension for a non–constant polynomial $f\in K[t]$. Prove that $[L:K]$ divides $(\deg f)!$ (hint: at the very end look at some binomial coefficients).

Solution. We use induction on the degree d of our polynomial f. We first assume that f is irreducible. Then by the tower law one has $[L:K] = [L:K(\alpha)][K(\alpha):K]$, where $\alpha \in L$ is any root of f. By induction $[L:K(\alpha)]$ divides $(d-1)!$ and $[K(\alpha):K]$ equals exactly d. Thus $[L:K]$ divides $(d-1)!d = d!$.

Now suppose that f is reducible, that is $f = gh$, $\deg g = s$, $\deg h = t$, $s + t = d$, and M be the subfield of L generated by the field K and by the roots of g. In other words, M is a splitting filed for g over K and by induction $[M:K]$ divides $s!$, $[L:M]$ divides $(d-s)!$. Thus by the tower law $[L:K]$ divides $s!t!$. But the binomial coefficient $\binom{d}{s} = \frac{d!}{s!t!}$ is an integer and hence $s!t!$ divides $d!$. It follows that $[L:K]$ divides $d!$.