Math 430 Homework 10 Sample solution based on that of Liam Bench

Chapter 32

6. The roots of x^4+1 are $\pm\frac{\sqrt{2}}{2}\pm i\frac{\sqrt{2}}{2}$. So $E=\mathbb{Q}(\sqrt{2},i)$. Because an automorphism must fix $\mathbb{Q}$, an automorphism of E,ϕ, is determined by $\phi(\sqrt{2})$ and $\phi(i)$. Note that $2=\phi(2)=\phi(\sqrt{2}^2)=\phi(\sqrt{2})^2$ and so $\phi(\sqrt{2})=\pm\sqrt{2}$. By a similar argument $\phi(i)=\pm i$. So there are 4 automorphisms in $\text{Gal}(E/\mathbb{Q})$, the identity ε, α where $\alpha\sqrt{2}=-\sqrt{2}$ and $\alpha(i)=i$, β where $\beta(\sqrt{2})=\sqrt{2}$ and $\beta(i)=-i$, and $\alpha\beta$. The subgroups of $\text{Gal}(E/\mathbb{Q})$ are itself, $\{\varepsilon,\alpha\},\{\varepsilon,\beta\}$, $\{\varepsilon,\alpha\beta\}$, and $\{\varepsilon\}$. The corresponding subfields are $\mathbb{Q}$, $\mathbb{Q}(i),\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$, $\mathbb{Q}(\sqrt{2},i)$. In $\text{Gal}(E/\mathbb{Q})$, α has the fixes field $\mathbb{Q}(i)$, β has the fixed field $\mathbb{Q}(\sqrt{2}$, and $\alpha\beta$ has the field $\mathbb{Q}(i\sqrt{2})$. There is no automorphism whose fixed field is $\mathbb{Q}$.

Alternatively Any $\mathbb{Q}$-automorphism of $\mathbb{E}$ will send $w=e^{i2\pi/8}$ to w^3,w^5 or w^7. Thus,

$$\text{Gal}(\mathbb{Q}(w)/\mathbb{Q})\sim\mathbb{Z}_2\oplus\mathbb{Z}_2.$$

8. Let $f(x)\in\mathbb{F}[x]$ and let the zeros of $f(x)$ be $a_1,a_2,...,a_n$. Then $\mathbb{E}=\mathbb{F}(a_1,a_2,...,a_n)$. It suffices to prove that $\text{Gal}(\mathbb{E}/\mathbb{F})$ is isomorphic to a group of permutations of a_i's. Consider one of the roots, a_i. So $f(a_i)=0$. So $0=\alpha(f(a_i))=f(\alpha(a_i))$. So $\alpha(a_i)=a_j$ for some j. The automorphisms are one-to-one so this permutes the a_i's.

10. $\mathbb{E}=\mathbb{Q}(\sqrt{2},\sqrt{5})=\{a_0+a_1\sqrt{2}+a_2\sqrt{5}+a_3\sqrt{2}\sqrt{5}\mid a_i\in\mathbb{Q}\}$. So $|\text{Gal}(\mathbb{E}/\mathbb{Q})|=[\mathbb{E}:\mathbb{Q}]=4$. Also $\mathbb{Q}(\sqrt{10})=\{a_0+a_1\sqrt{10}\mid a_i\in\mathbb{Q}\}$. So $|\text{Gal}(\mathbb{Q}(\sqrt{10})/\mathbb{Q})|=[\mathbb{Q}(\sqrt{10}):\mathbb{Q}]=2$.
Remark In this case, $\text{Gal}(\mathbb{E}/\mathbb{Q})\sim\mathbb{Z}_2\oplus\mathbb{Z}_2$.

12. The zeros of $x^2-10x+21=(x-7)(x-3)$ are $7,3\in\mathbb{Q}$. So the splitting field is $\mathbb{Q}$ and $\text{Gal}(\mathbb{Q}/\mathbb{Q})=\{\varepsilon\}$.

14. First I show there are exactly three subgroups of D_6 of order 6. Let G be one of these subgroups. So G contains an element of order 2 and an element of order 3. The only elements of order 3 in D_6 are R_{120} and R_{240}. So a subgroup of order 6 contains $\{R_0,R_{120},R_{240}\}$. If it contains R_{60},R_{180}, or R_{300}, then the subgroup is $\langle R_{60}\rangle$. If the subgroup contains one of the three flips through a pair of vertices, V_i, then it contains 6 elements (and contain no more) and is $\langle R_{120},V_1\rangle$. If it contains one of the three flips through a side, S_i, then it contains 6 elements and is $\langle R_{120},S_1\rangle$. We have exhausted all of the possible elements to add and these are the only order 6 subgroups. Each of these corresponds to a subfield of E, call it L, with $[E:L]=6$.

18. Note that $x^3-1=(x-1)(x^2+x+1)$ and the zeros are $1,\frac{-1\pm i\sqrt{3}}{2}$. So the splitting field is $\mathbb{E}=\mathbb{Q}(i\sqrt{3})$. So the automorphisms are determined by $\phi(i\sqrt{3})$. Well $i\sqrt{3}\to\pm i\sqrt{3}$ by the same reasoning in number 6. Let α be the automorphism such that $\alpha(i\sqrt{3})=-i\sqrt{3}$. So $\text{Gal}(\mathbb{E}/\mathbb{Q})=\{\varepsilon,\alpha\}$.

Note that the zeros of x^3-2 are $2^{\frac{1}{3}}, \frac{-2^{\frac{1}{3}} \pm 2^{\frac{1}{3}} i\sqrt{3}}{2}$. So the extension field $E = \mathbb{Q}(2^{\frac{1}{3}}, i\sqrt{3})$. So $|\mathrm{Gal}(\mathbb{Q}(2^{\frac{1}{3}}, i\sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(2^{\frac{1}{3}}, i\sqrt{3}) : \mathbb{Q})] = 6$. By problem 7, the Galois group is isomorphic to a group of permutations of the zeros of x^3-2. The Galois group has 6 elements so has all permutations of the 3 zeros. So each permutation corresponds to an element of the Galois group where if a zero, a_1, is sent to another zero, a_2, in the permutation, then $\phi(a_1) = a_2$.

22. If $[\mathbb{E} : \mathbb{F}]$ is finite then $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})|$ is finite. So the power set of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is finite. The set of subgroups is a subset of the power set of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ so there are a finite number of subgroups. There is a one-to-one correspondence between the subgroups of $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and the fields between $\mathbb{E}$ and $\mathbb{F}$. So there are a finite number of fields between $\mathbb{E}$ and $\mathbb{F}$.

24. First note that $\mathbb{Q}(\omega) = \{a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 : a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$ because ω is a zero of the irreducible $x^4+x^3+x^2+x+1$. Thus, $a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 = \phi(a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3) = a_0 + a_1\omega^4 + a_2\omega^3 + a_3\omega^2 = a_0 + a_1(-1-\omega-\omega^2-\omega^3) + a_2\omega^3 + a_3\omega^2$ if and only if $a_0 = a_0 - a_1, a_1 = -a_1, a_2 = a_1 + a_3, a_3 = a_2$, i.e., $a_1 = 0, a_2 = a_3$. By the Fundamental Theorem of Galois Theory $\{a_0 + a_2(\omega^2+\omega^3) : a_0, a_2 \in \mathbb{Q}\}$ is the fixed field of $\langle \phi \rangle$.

Remark Actually, $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})) \sim \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

34. $GF(p) \approx \mathbb{Z}_p$. Note that $\phi(1) = 1$ and 1 generates $\mathbb{Z}_p$ and therefore it generates $GF(p)$. Let $m \in \mathbb{Z}_p$. So $\phi(m) = \phi(1_1 + 1_2 + ... + 1_m) = m\phi(1) = m$. So this corresponds to the automorphism acting on $GF(p)$. So ϕ must act as the identity on $GF(p)$.