MATH 571: Higher Algebra I, Winter 2005

Solutions to Assignment 7

Chapter V, Section 3, #2: Obvious, because since F is generated by K and roots of polynomials from S then clearly F is generated by E and roots of polynomials from $S \subseteq K[\overline{x}] \subseteq E[\overline{x}]$.

Chapter V, Section 3, #16: (a) $\mathbb{Q}(X) \subseteq E$ is clear because every $\sqrt{p} \in X$ is a root of a polynomial $x^2 + p \in S$ which splits over E. On the other hand for every $a \in \mathbb{Q}$ its square root $\sqrt{a}$ can be expressed as

$$\sqrt{a} = \sqrt{\pm 1}\frac{\prod_{i=1}^{k(a)}(\sqrt{p_i})^{n_i}}{\prod_{j=1}^{m(a)}(\sqrt{q_j})^{s_j}},$$

where $\sqrt{p_i},\ \sqrt{q_j} \in X$. Thus, every element of E can expressed via $\mathbb{Q}$ and X and it follows that $E \subseteq \mathbb{Q}(X)$.

(b) σ is completely defined by its action on X. Moreover, if $u, v \in X$ then $\sigma u = v$ only if u and v are roots of the same irreducible polynomial which by the choice of X has the form $x^2 - p$, where either $p = -1$ or p is a prime integer. Hence, u, v are equal to $\pm\sqrt{p}$ and $\sigma : \sqrt{p} \to \pm\sqrt{p}$ for every prime p or $p = -1$. Thus $\sigma^2 = 1_E$.

(c) Using the hint provided in the textbook for each $Y \subseteq X$ one can define a map

$$\sigma : \begin{array}{ll} q \to q, & \forall\ q \in \mathbb{Q} \\ \sqrt{p} \to -\sqrt{p}, & \text{if } \sqrt{p} \in Y \\ \sqrt{p} \to \sqrt{p}, & \text{if } \sqrt{p} \in X - Y \end{array}$$

σ can be easily checked to be a homomorphism of fields, and automatically it's injective. Surjectivity is also straightforward since $\sigma^2 = 1_E$ by **(b)** and it follows that $\sigma^{-1} = \sigma$.

Chapter V, Section 3, #23: Since $[F : K] = 2$ it follows that F is algebraic over K and there exists $u \in F$ such that $F = K(u)$. Moreover, the irreducible polynomial of u is of degree 2 and every element of F has a form $au + b,\ a, b \in K$. If $f(x) = ax^2 + bx + c$ then it has roots

$$u = \frac{-b + \sqrt{b^2 - 4ac}}{2a},\ v = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

and it's easy to see that $v = -\frac{b}{a} - u \in F$. Hence, $f(x)$ splits over F and F is generated by the roots of f over K. Thus, F is a splitting field of f over K and by Theorem 3.14, F is normal.

Chapter V, Section 4, #3: By Corollary 4.6, $K(\Delta)$ corresponds to $S_3 \cap A_3 = A_3$. Also, if $i \in [1,3]$ then $[K(u_i) : K]$ can be only 2 or 3. If 2 then a minimal inrreducible polynomial for u_i is of degree 2 and it divides f which is impossible. Thus, $[K(u_i) : K] = 3$ and the subgroup corresponding to $K(u_i)$ is a cyclic of order 2.

Chapter V, Section 4, #8: We have $[K(u) : K] = 4$, hence the intermediate field E can be only of dimension 2 over K. Denote $G = Aut_K F,\ H = Aut_{K(u)} F, H_0 = Aut_E F$, so $|G : H| = 4,\ |G : H_0| = 2$. By Proposition 4.11 G is one of the groups from the list

$$S_4, A_4, D_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4.$$

The last two groups from the list have order 4 and both have a subgroup of index 2. D_4 has order 8 and we have $D_4 > \mathbb{Z}_2 \times \mathbb{Z}_2 > \mathbb{Z}_2$, where $|D_4 : \mathbb{Z}_2| = 4,\ |D_4 : (\mathbb{Z}_2 \times \mathbb{Z}_2)| = 2$. Hence, we have shown that when G is $D_4, \mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$ then one can find a field properly between K and $K(u)$.

Now let $G = A_4$, then $|G| = 12$ and the subgroup of index 4 is $\mathbb{Z}_3$. But there exists no subgroup between A_4 and $\mathbb{Z}_3$ because it should have order 6 and a group of order 6 can be either $\mathbb{Z}_6$ or S_3 which are not in A_4.

Finally, let $G = S_4$. Hence, H has order 6, and then H is either $\mathbb{Z}_6$ or S_3. The subgroup between G and H should have order 12 which is possible only if it's A_4. But A_4 contains neither $\mathbb{Z}_6$ nor S_3.

Chapter V, Section 4, #10(a): 1. over $\mathbb{Q}$

x^4-5 is irreducible and separable, its resolvant is $x^3+20x = x(x+2\sqrt{5}i)(x-2\sqrt{5}i)$. Hence, $[\mathbb{Q}(\alpha,\beta,\gamma) : \mathbb{Q}] = 2$ and by Proposition 4.11 either $G \simeq D_4$ or $G \simeq \mathbb{Z}_4$. Finally, observe that $x^4 - 5$ is irreducible over $\mathbb{Q}(2\sqrt{5}i)$ hence $G \simeq D_4$.

2. over $\mathbb{Q}(\sqrt{5})$

$x^4 - 5 = (x^2 - \sqrt{5})(x^2 + \sqrt{5})$ over $\mathbb{Q}(\sqrt{5})$. We have the splitting field F of $x^4 - 5$ is $\mathbb{Q}(\sqrt[4]{5}, \sqrt[4]{5}i)$. Since $x^2 + \sqrt{5}$ is irreducible over $\mathbb{Q}(\sqrt[4]{5})$ then $[F : \mathbb{Q}(\sqrt{5})] = 4$ and $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}(\sqrt{5})] = 2$. Thus, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. over $\mathbb{Q}(\sqrt{5}i)$

x^4-5 is irreducible over $\mathbb{Q}(\sqrt{5}i)$ and its resolvant is x^3+20x. Hence $[\mathbb{Q}(\sqrt{5}i)(\alpha,\beta,\gamma) : \mathbb{Q}(\sqrt{5}i)] = 1$ and by Proposition 4.11 $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

(d),(i) can be done similarly to **(a)**.