Mathematics GU4042 Modern Algebra II
Assignment # 8

Benjamin Church

December 21, 2017

Page 196.

Problem 1.

The minimal polynomial of $\sqrt[3]{s}$ is $X^3 - 2$. This must be minimal because any polynomial of lower degree is linear or quadratic which can always be solved by square roots. However, if $\sqrt[3]{2} = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ then $(a + b\sqrt{d})^3 = 2$ so $a^3 + 3a^2 b\sqrt{d} + 3ab^2 d + b^3 d\sqrt{d} \in \mathbb{Q}$ which implies that $\sqrt{d} \in \mathbb{Q}$ so $\sqrt[3]{2} \in \mathbb{Q}$ which is a contradiction. One could also argue that $X^3 - 2$ is irreducible by Eisenstein's criterion because 2 divides every subleadiing term but 4 does not divide the constant term or leading. Thus, $X^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ and we showed on assignment # 7 that the splitting field of $X^3 - 2$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ in which $X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(X - \zeta_3^2\sqrt[3]{2})$ so the conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, and $\zeta_3^2\sqrt[3]{2}$.

Problem 2.

On assignment # 6, I showed that the minimal polynomial of $\sqrt{2} + \sqrt{3}$ is,

$$X^4 - 10X^2 + 1 = (X - (\sqrt{2} + \sqrt{3}))(X + (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X + (\sqrt{2} - \sqrt{3}))$$

with roots: $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, $-\sqrt{2} - \sqrt{3}$ which are the conjugates of $\sqrt{2} + \sqrt{3}$.

Problem 3.

Let F be normal over K and $K \subset E \subset F$. Since F/K is normal, for every $\alpha \in F$ the minimal polynomial $\text{Min}(\alpha; K)$ splints in F. Now, let $q = \text{Min}(\alpha; E)$ then because $K \subset E$ we have $\text{Min}(\alpha; K) \in E[X]$ and has α as a root so $q \mid \text{Min}(\alpha; K)$ in the ring $E[X]$. By unique factorization, since $\text{Min}(\alpha; K)$ splits in F then q splits in F. Therefore, for any $\alpha \in F$ we have $\text{Min}(\alpha; E)$ splits in F so F/E is normal.

Problem 5.

Suppose that K, F, and E are contained in a larger field L. Let E and F be normal over K. Take $\alpha \in E \cap F$ then $\alpha \in E$ and $\alpha \in F$. Because both are normal extensions, the minimal polynomial $q = \text{Min}(\alpha; K)$ splits in both E and F and thus splits in L. Thus, $q(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$ with $\alpha_i \in L$. However, q splits in both F and E and the roots cannot be different because then q would spit in multiple ways inside L which would contradict unqiue factorization. Thus, $\alpha_i \in E$ and $\alpha_i \in F$ so $\alpha_i \in E \cap F$. Thus, all the roots of q are contained in $E \cap F$ so q splits in $E \cap F$. Thus, $E \cap F$ is normal over K.

Page 200.

Problem 1.

Let F_1 and F_2 be intermediate fields of a Galois extension E/K with corresponding subgroups of $Gal(E/K)$ given by H_1 and H_2. Suppose that $F_1 \subset F_2$ then take $\sigma \in H_2$. Now, σ fixes F_2 and therefore fixes $F_1 \subset F_2$. Thus, $\sigma \in H_1$ the subgroup of automorphisms fixing F_1. Thus, $H_2 \subset H_1$. Conversely, suppose that $H_2 \subset H_1$ then take $\alpha \in F_1$. Now, $\forall \sigma \in H_1 : \sigma(\alpha) = \alpha$ and $H_2 \subset H_1$ so $\forall \sigma \in H_2 : \sigma(\alpha) = \alpha$ so $\alpha \in E^{H_2} = F_2$. Thus, $F_1 \subset F_2$.

Problem 2.

Let F_1, F_2, and F_3 be intermediate fields of a Galois extension E/K with corresponding subgroups of $Gal(E/K)$ given by H_1, H_2, and H_3. Suppose that $F_1 = F_2 F_3$ then $F_2, F_3 \subset F_1$ so $H_2, H_3 \supset H_1$ so $H_1 \subset H_2 \cap H_3$. Now, the subgroup $H' = H_1 \cap H_2 \subset H_2, H_3$ so $E^{H'} \supset F_2$ and $E^{H'} \supset F_3$. Therefore, $E^{H'} \supset F_2 F_3 = F_1$ and thus $H' \subset H_1$ so $H_1 = H_2 \cap H_3$.

Conversely, let $H_1 = H_2 \cap H_3$. Then, $H_1 \subset H_2, H_3$ so $F_2, F_3 \subset F_1$ and thus $F_2 F_3 \subset F_1$. Now, take $L = F_2 F_3$ which satisfies $L \supset F_2$ and $L \supset F_3$ so $H_L = Gal(E/L)$ satisfies $H_L \subset H_2$ and $H_L \subset H_3$ so $H_L \subset H_2 \cap H_3 = H_1$ so $L \supset F_1$ and thus $F_1 = F_2 F_3$.

Problem 3.

Let F_1, F_2, and F_3 be intermediate fields of a Galois extension E/K with corresponding subgroups of $Gal(E/K)$ given by H_1, H_2, and H_3. Suppose that $F_1 = F_2 \cap F_3$ then $F_1 \subset F_2, F_3$ so $H_1 \supset H_2, H_3$ so $H_1 \supset \langle H_2 \cup H_3 \rangle$. Now, the subgroup $H' = \langle H_2 \cup H_3 \rangle \supset H_2, H_3$ so $E^{H'} \subset F_2$ and $E^{H'} \subset F_3$. Therefore, $E^{H'} \subset F_2 \cap F_3 = F_1$ and thus $H' \supset H_1$ so $H_1 = \langle H_2 \cup H_3 \rangle$.

Conversely, let $H_1 = \langle H_2 \cup H_3 \rangle$. Then, $H_1 \supset H_2, H_3$ so $F_1 \subset F_2, F_3$ and thus $F_1 \subset F_2 \cap F_3$. Now, take $L = F_2 \cap F_3$ which satisfies $L \subset F_2$ and $L \subset F_3$ so $H_L = Gal(E/L)$ satisfies $H_L \supset H_2$ and $H_L \supset H_3$ so $H_l \supset \langle H_2 \cup H_3 \rangle = H_1$ so $L \subset F_1$ and thus $F_1 = F_2 \cap F_3$.

Problem 5.

The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is normal because $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. consider the Frobenius map, $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $\sigma : x \mapsto x^p$. Because $\mathbb{F}_{p^n}$ has characteristic p, this is a field homomorphism and therefore is injective. However, because the field is finite, the map is also surjective and thus an automorphism. The extension is seperable because $\mathbb{F}_p$ is perfect since the Frobenius is surjective. Thus, the extension is Galois so $|Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. However, by Lagrange, $\forall x \in \mathbb{F}_p^\times : x^{p-1} = 1$ so $x^p = x$. This equation is also satisfied by $x = 0$ so for any $x \in \mathbb{F}_p$ we have $\sigma(x) = x$. Thus, $\sigma \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Suppose that $\sigma^k = \text{id}$. Then, $\forall x \in \mathbb{F}_{p^n} : \sigma^k(x) = x^{p^k} = x$. Therefore, every element of $\mathbb{F}_{p^n}$ is a root of $X^{p^k} - X$. However, in any field, this polynomial has at most p^k roots. Thus, $p^n \leq p^k$ so $n \leq k$. Therefore, the order of σ is at least n. However, the order of $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is n so σ must be a generator of the group and therefore the Galois group is cyclic with order n.