MATH 431 Written Homework 12 Solution **Radford**

04/20/2009

---

1. Page 560, number 4: (**20 points**) set $E = \mathbf{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7})$. Then E is a splitting field of $(x^2-2)(x^2-5)(x^2-7)$ over $\mathbf{Q}$. By the Fundamental Theorem of Galois Theory $K \mapsto \mathrm{Gal}(E/\mathbf{Q})$ describes a bijective correspondence between the subfields of F which contain $\mathbf{Q}$(any subfield of E must contain $\mathbf{Q}$) and $[K : \mathbf{Q}] = [\mathrm{Gal}(E/\mathbf{Q}) : \mathrm{Gal}(E/K)]$. Since $|\mathrm{Gal}(E/\mathbf{Q})| = 8$ we conclude that $4 = [K : \mathbf{Q}]$ if and only if $|\mathrm{Gal}(K/\mathbf{Q})| = 2$ (**10**).

We are given that $\mathrm{Gal}(E/\mathbf{Q} \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. Writing $G = \mathrm{Gal}(E/\mathbf{Q})$ in multiplicative notation we have $a^2 = e$ for all $a \in G$. Therefore there are 7 subgroups of G of order 2 which means there are 7 subfields of E of degree 4 over $\mathbf{Q}$ (**10**).

2. Page 560, number 10: (**20 points**) $E = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ is a splitting field of $(x^2-2)(x^2-5)$ over $\mathbf{Q}$ (**5**). Now $[E : \mathbf{Q}] = 4$ by (C). Therefore $4 = [E : \mathbf{Q}] = |\mathrm{Gal}(E/\mathbf{Q})|$ by the Fundamental Theorem of Galois Theory (**5**).

Note $2 = [\mathbf{Q}(\sqrt{10}) : \mathbf{Q}]$ since $\sqrt{10}$ is a root of $x^2 - 10 \in \mathbf{Q}[x]$ which is irreducible by the Eisenstein Criterion with $p = 2$ or $p = 5$ (**5**). Therefore $2 = [\mathbf{Q}(\sqrt{10}) : \mathbf{Q}] = |\mathrm{Gal}(\mathbf{Q}(\sqrt{10})/\mathbf{Q})|$ by the Fundamental Theorem of Galois Theory (**5**).

3. Page 561, number 12: (**40 points**) $x^3 - 1 = (x-1)(x^2+x+1)$. Let

$$\omega = e^{2\pi\imath/3} = \cos(\frac{2\pi\imath}{3}) + \imath\sin(\frac{2\pi\imath}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}\imath$$

be a primitive 3^{rd} root of unity. Then $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ which means that $\mathbf{Q}(\omega)$ is a splitting field of $x^3 - 1$ over $\mathbf{Q}$ and ω is a root of $(x-\omega)(x-\omega^2) = x^2 + x + 1 \in \mathbf{Q}[x]$. The latter implies that $[\mathbf{Q}(\omega) : \mathbf{Q}] \leq 2$. Since $\omega \notin \mathbf{R}$ it follows that $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$ (**5**).

Let $E = \mathbf{Q}(\omega)$. By definition $\mathrm{Gal}(E/F)$ is the Galois group of $x^3 - 1$ over $\mathbf{Q}$. By the Fundamental Theorem of Galois Theory $|\mathrm{Gal}(E/\mathbf{Q})| = [E : \mathbf{Q}] = 2$ which means $\mathrm{Gal}(E/\mathbf{Q}) \simeq \mathbf{Z}_2$ (**5**).

Observe that $x^3 - 2 = (x - 2^{1/3})(x - \omega 2^{1/3})(x - \omega^2 2^{1/3})$. Therefore a splitting field of $x^3 - 2$ over $\mathbf{Q}$ is $E = \mathbf{Q}(2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}) = \mathbf{Q}(2^{1/3}, \omega)$. The last equation holds since $\omega = (\omega 2^{1/3})(2^{1/3})^{-1} \in E$. By definition the Galois group of $x^3 - 2$ over $\mathbf{Q}$ is $\mathrm{Gal}(E/\mathbf{Q})$.

We have shown that $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$. Now $[\mathbf{Q}(2^{1/3}) : \mathbf{Q}] = 3$ since $2^{1/3}$ is a root of $x^3 - 2 \in \mathbf{Q}[x]$ and the latter is irreducible by the Eisenstein Criterion with $p = 2$. Therefore $[E : \mathbf{Q}] = [\mathbf{Q}(\omega, 2^{1/3}) : \mathbf{Q}] = 6$ by (D). By the Fundamental Theorem of Galois Theory $|\mathrm{Gal}(E/\mathbf{Q})| = [E : \mathbf{Q}] = 6$ (**5**).

Let $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$. Then $\sigma(2^{1/3}) \in \{2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}\} = R_1$, the set of roots of $x^3 - 2$ in E, by (A). Likewise $\sigma(\omega) \in \{\omega, \omega^2\} = R_2$, the set of roots of $x^2 + x + 1$ in E. Thus there are $|R_1||R_2| = 3 \times 2 = 6$ possible choices for the pair $(\sigma(2^{1/3}), \sigma(\omega))$. Since $\mathrm{Gal}(E/\mathbf{Q})| = 6$, given $r_1 \in R_1$ and $r_2 \in R_2$ there exists a $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$ such that $\sigma(2^{1/3}) = r_1$ and $\sigma(\omega) = r_2$ by (B).

Let $\tau, \sigma \in \mathrm{Gal}(E/\mathbf{Q})$ satisfy

$$\tau(\omega) = \omega^2 \text{ and } \tau(2^{1/3}) = 2^{1/3} \quad (\mathbf{5})$$

and

$$\sigma(\omega) = \omega \;\text{ and }\; \sigma(2^{1/3}) = \omega 2^{1/3} \quad (\mathbf{5}).$$

Then $\tau, \sigma \neq \mathrm{Id}$. Note

$$\tau^2(\omega) = \tau(\tau(\omega)) = \tau(\omega^2) = \tau(\omega)^2 = (\omega^2)^2 = \omega^4 = \omega,$$

as $\omega^3 = 1$, and

$$\tau^2(2^{1/3}) = \tau(\tau(2^{1/3})) = \tau(2^{1/3}) = 2^{1/3}.$$

Therefore $\tau^2 = \mathrm{Id}$ by (B) which means τ has order 2.

Likewise

$$\sigma^3(\omega) = \omega$$

and, since by induction $\sigma^n(2^{1/3}) = \omega^n 2^{1/3}$ for all $n \geq 0$, we have

$$\sigma^3(2^{1/3}) = \omega^3 2^{1/3} = 2^{1/3}.$$

Therefore $\sigma^3 = \mathrm{Id}$ by (B) again and thus has order 3. Since $\tau^{-1} = \tau$,

$$\tau\sigma\tau^{-1}(\omega) = \tau(\sigma(\tau(\omega))) = \tau(\sigma(\omega^2)) = \tau(\sigma(\omega)^2) = \tau(\omega^2) = \tau(\omega)^2 = (\omega^2)^2 = \omega^4 = \omega = \sigma^{-1}(\omega),$$

as $\sigma(\omega) = \omega$ implies $\omega = \sigma^{-1}(\omega)$, and

$$\tau\sigma\tau^{-1}(2^{1/3}) = \tau(\sigma(\tau(2^{1/3}))) = \tau(\sigma(2^{1/3})) = \tau(\omega 2^{1/3}) = \tau(\omega)\tau(2^{1/3}) = \omega^2 2^{1/3} = \sigma^2(2^{1/3}).$$

Therefore $\tau\sigma\tau^{-1} = \sigma^2$ by (B) again, and thus $\tau\sigma\tau^{-1} = \sigma^{-1}$ as σ has order 3 (**5**). Thus $\mathrm{Gal}(E/\mathbf{Q}) \simeq \mathrm{D}_3$ (**5**).

4. Page 561, number 16: (**20 points**) By the Fundamental Theorem of Galois Theory $|\mathrm{Gal}(E/F)| = [E : F]$ is finite and the subgroups of $G = \mathrm{Gal}(E/F)$ are in one-one correspondence with the subfields of E which contain F (**10**). Since G is finite it has only finitely subgroups; thus E has only finitely many subfields K which contain F (**10**).