Modern Algebra II: Problem Set 13

Nilay Kumar

Last updated: May 4, 2013

Problem 1

Let F be a field of characteristic zero, let $f(x) \in F[x]$ be an irreducible polynomial of degree n, and let E be a splitting field of $f(x)$, with roots $\alpha_1, \ldots, \alpha_n \in E$.

(i) By virtue of being a splitting field, $E = F(\alpha_1, \ldots, \alpha_n)$, and E is a Galois extension of F. Then, the order of $\mathrm{Gal}(E/F)$ is simply the degree $[E : F]$. Consider the sequence of extensions:

$$F \leq F(\alpha_1) \leq E.$$

Since the irreducible polynomial for α_1 over F is $f(x)$, which has degree n, we can compute

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F] = [E : F(\alpha_1)] \cdot n.$$

Hence, n must divide the order of $\mathrm{Gal}(E/F)$.

(ii) Consider $F = \mathbb{Q}$ and $f(x) = x^4 - 10x^2 + 1$. We saw in class that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \{1, \sigma_1, \sigma_2, \sigma_3\}$, where

$$\begin{aligned} \sigma_1(\sqrt{2}) = -\sqrt{2}, \sigma_1(\sqrt{3}) = \sqrt{3} \\ \sigma_2(\sqrt{2}) = \sqrt{2}, \sigma_2(\sqrt{3}) = -\sqrt{3} \\ \sigma_3(\sqrt{2}) = -\sqrt{2}, \sigma_3(\sqrt{3}) = -\sqrt{3} \end{aligned}$$

Note that every element of the Galois group is of order 2, and thus there does not necessarily have to be an element of order 4.

Problem 2

Let A_2 be the element $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$. Note that $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of the splitting field $\mathbb{Q}(\sqrt[3]{2}, \omega)$. Take some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$. If we let

$$\begin{aligned}
A_1 &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \\
A_2 &= a + b\omega\sqrt[3]{2} + c\omega^2(\sqrt[3]{2})^2 \\
A_3 &= a + b\omega^2\sqrt[3]{2} + c\omega(\sqrt[3]{2})^2
\end{aligned}$$

then $\sigma(A_1) = a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{2})^2$. Clearly, all we need to know is what $\sigma(\sqrt[3]{2})$ is – but we know that it can only take on the values $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ because the elements of the Galois group act on the roots. Hence, inserting each possibility into $\sigma(A_1)$ above we find that $\sigma(A_1)$ can only be one of A_1, A_2, A_3. Note that this implies $A_1A_2A_3$ must be fixed by every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/Q)$ because σ can be identified by its action on the indices and because σ is bijective. Furthermore, this means that $A_1A_2A_3 \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})}$, but by the main theorem, this is simply $\mathbb{Q}$. Note that $D = A_1A_2A_3 = 0$ would imply that one of the A_i's must be zero. But because the expressions for A_i's can be seen as linear combinations in a $\mathbb{Q}$-vector space, we see that in this case $a = b = c = 0$ by linear independence.

We can compute $A_1A_2A_3$ now – it is a straightforward but tedious computation, the details of which I will omit in order to spare the grader the enormous burden of grading. Indeed, simply using $\omega^2 + \omega + 1 = 0$ (and the fact that the final answer has to be in $\mathbb{Q}$) results in:

$$D = A_1A_2A_3 = a^3 + 2b^2 + 4c^3 - 6abc.$$

We have seen this expression before in problem 6 of homework 2 Using this, we see that we must have

$$A_1^{-1} = \frac{A_2A_3}{a^3 + 2b^3 + 4c^2 - 6abc}.$$

To be more explicit, one could can multiply out A_2A_3:

$$A_1^{-1} = \frac{(a^2 - 2bc) + (-ab + 2c^2)\sqrt[3]{2} + (b^2 - ac)\sqrt[3]{2}^2}{a^3 + 2b^3 + 4c^2 - 6abc}.$$

Problem 3

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic polynomial with exactly one real root. Let E be the splitting field of $f(x)$.

(i) By the fundamental theorem of algebra we know that $f(x)$ must have 3 complex roots. Thus, since it has one real root, it must have 2 complex roots. We know that complex roots always occur in conjugates; indeed, it is easy to check that permuting these two conjugates is an automorphism, and thus σ, the conjugation automorphism, is an element of $\mathrm{Gal}(E/\mathbb{Q})$. Clearly σ is an element of order 2, and hence it is impossible for $\mathrm{Gal}(E/\mathbb{Q})$ to be equal to A_3, as all elements of A_3 have order one or three (by Lagrange's theorem, since the order of A_3 is 3).

(ii) Since E is the splitting field for $f(x)$ over $\mathbb{Q}$, we know that the order of the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is equal to $[E:\mathbb{Q}]$. We also know that this is divisible by 3 and that this must divide $3! = 6$ (first problem). We can write:

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 3[E:\mathbb{Q}(\alpha)].$$

Hence, $[E:\mathbb{Q}(\alpha)]$ is either 1 or 2. It cannot be 1, as that would imply that $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$ over $\mathbb{Q}$. This is a contradiction, as $f(x)$ is irreducible in $\mathbb{Q}[x]$ and cannot be factored into linear factors. Thus we have that $[E:\mathbb{Q}(\alpha)] = 2$. Consequently $[E:\mathbb{Q}] = 6$, i.e. E has degree 6 over $\mathbb{Q}$.

Problem 4

Let F be a field of characteristic zero and let E be a normal extension of F with Galois group isomorphic to S_3. Since E is a Galois extension of F we may invoke the main theorem of Galois theory: $[E:F] = 6$. Note that there are no order 2 normal subgroups of S_3, and thus, by the main theorem, there exists an intermediate field K, not normal over F, such that $[K:F] = 3$. K must be a simple extension of F (by the usual divisibility arguments since 3 is prime). Hence, $K = F(\alpha)$ where $\alpha \in E$ is the root of some polynomial $f(x) \in F[x]$ irreducible in $F[x]$. Note that $K = F(\alpha)$ is not normal, and therefore cannot be a splitting field for F. E, however, is a normal extension of F, and since we know that $f(x)$ is an irreducible polynomial in $F[x]$ with a root in E, $f(x)$ must factor into a product of linear factor in $E[x]$. Thus, there must be a splitting field for $f(x)$, call it L, such that $F(\alpha) \leq L \leq E$. We know that:

$$\begin{aligned}[E:F] &= [E:F(\alpha)][F(\alpha):F] = 6\\ [E:F(\alpha)] &= 2\end{aligned}$$

and hence,

$$[E : F(\alpha)] = [E : L][L : F(\alpha)] = 2$$

but since $[L : F(\alpha)] > 1$, we must have that $[L : F(\alpha)] = 2$ and thus $[E : L] = 1$, i.e. $E = L$. By construction, L is a splitting field for $f(x)$, and thus E must be as well.

Problem 5

Let F be a field of characteristic zero containing all the cube roots of unity and let ω be a generator of this group. Suppose that E is a normal extension of F whose Galois group is cyclic of order 3, and let σ be a generator for $\mathrm{Gal}(E/F)$. Suppose that $\beta \in E$ is nonzero and that $\sigma(\beta) = \omega\beta$. First note that $\beta \notin F$, obviously, as otherwise it would be fixed by β. Furthermore,

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

i.e. σ fixes β^3. Since this is true of the generator σ of $\mathrm{Gal}(E/F)$, every element in the Galois group must fix β^3. Hence, β^3 must actually be in F, by the main theorem (as in problem 2). Finally, note that $x^3 - \beta^3 \in F[x]$ is irreducible, because its roots are $\beta, \omega\beta, \omega^2\beta$, none of which are in F (as they are not fixed by σ: $\sigma(\beta) = \omega\beta, \sigma(\omega\beta) = \omega^2\beta, \sigma(\omega^2\beta) = \beta$ using the fact that $\omega \in F$ is fixed). Consequently, we have that

$$[E : F] = [E : F(\beta)][F(\beta) : F] = 3[E : F(\beta)]$$

since $x^3 - \beta^3 = \mathrm{irr}(\beta, F, x)$ has degree 3 but since $[E : F] = 3$ we must have that $[E : F(\beta)] = 1$, and hence, $E = F(\beta)$. Thus, assuming that we can find a $\beta \neq 0$ such that $\sigma(\beta) = \omega\beta$, E is obtained from F by adding a cube root.

Problem 6

Let $\zeta = \zeta_5$ be the fifth root of unity $e^{2\pi i/5}$, and consider the field $\mathbb{Q}(\zeta)$.

(i) We know that $\Phi_5(x) = x^4+x^3+x^2+x+1$ is an irreducible polynomial in $\mathbb{Q}[x]$ of degree four of which ζ_5 is a root. It follows that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

(ii) Take $\alpha = \zeta + \zeta^{-1}$. Then we have that:

$$\begin{aligned}(\zeta + \zeta^{-1})^2 + \zeta + \zeta^{-1} - 1 &= \zeta^2 + \zeta^{-2} + 2 + \zeta + \zeta^{-1} - 1 \\ &= \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0\end{aligned}$$

By the quadratic formula, then, we must have that

$$\alpha = \left(-1 \pm \sqrt{5}\right)/2.$$

Let us take

$$\zeta = e^{2\pi i/5} = \cos\left(2\pi/5\right) + \sin\left(2\pi/5\right).$$

Then,

$$\zeta^{-1} = e^{-2\pi i/5} = \cos\left(2\pi/5\right) - \sin\left(2\pi/5\right)$$

and thus $\alpha = 2\cos\left(2\pi/5\right)$. It's clear, since $2\pi/5 < \pi/2$ that $\alpha > 0$, and hence we must choose:

$$\alpha = \left(-1 + \sqrt{5}\right)/2.$$

(iii) We now have

$$\zeta^2 - \alpha\zeta + 1 = \zeta^2 - \left(\zeta + \zeta^{-1}\right)\zeta + 1 = \zeta^2 - \zeta^2 - \zeta^5 + 1 = 0.$$

Hence, by the quadratic formula, we have that:

$$\begin{aligned}\zeta &= \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2} \\ &= \frac{\left(-1+\sqrt{5}\right)/2 \pm \sqrt{\frac{-5-\sqrt{5}}{2}}}{2} \\ &= \frac{-1+\sqrt{5}}{4} + \left(\frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}\right) i\end{aligned}$$

Note that the sign must be positive, as we know that both the real and imaginary parts must be positive.

(iv) Now let $\zeta = \zeta_7$ be the seventh root of unity, $e^{2\pi i/7}$, and consider the field $\mathbb{Q}(\zeta)$. Let $\alpha = \zeta + \zeta^2 + \zeta^4$. Then,

$$\begin{aligned}\alpha^2 + \alpha + 2 &= (\zeta + \zeta^2 + \zeta^4)^2 + \zeta + \zeta^2 + \zeta^4 + 2 \\ &= 2\zeta^2 + 2\zeta^3 + 2\zeta^5 + 2\zeta^4 + 2\zeta^6 + \zeta^8 + \zeta + 2 \\ &= 2\Phi_7(\zeta) = 0\end{aligned}$$

By the quadratic formula, then, we see that

$$\alpha = \frac{-1 \pm \sqrt{-7}}{2}.$$

Next let $\beta = \zeta + \zeta^{-1}$:

$$\begin{aligned}
\beta^2 &= \zeta^2 + \zeta^{-2} = \zeta^2 + \zeta^5 + 2 \\
\beta^2 - 2 &= \zeta^2 + \zeta^5 \\
(\beta^2 - 2)\beta &= \left(\zeta^2 + \zeta^5\right)\left(\zeta + \zeta^6\right) \\
&= \zeta^3 + \zeta + \zeta^6 + \zeta^4
\end{aligned}$$

Hence, we see that

$$(\beta^2 - 2)\beta + \left(\beta^2 - 2\right) + 1 = \Phi_7(\zeta) = 0$$

and hence β is the root of $(x^2-2)x+(x^2-2)+1 = (x^2-2)(x+1)+1 = x^3 + x^2 - 2x - 1$.