MATH411 Assignment 2

Elliott Hughes

June 10, 2022

4.1

1. This polynomial is irreducible, so we can use the technique presented in the notes. Calculating the discriminant we see that $D(f) = -4(-3)^3 - 27(1) = 9^2 \in \mathbb{Q}^2$. Therefore $\text{Gal}(f) = A_3$ and so the action of the automorphisms on the roots is cyclic.

2. Again $f(x)$ is irreducible, so we calculate the discriminant and find that $D(f) = -4(3)^3 - 27(1) = -5(3^3) \notin \mathbb{Q}^2$ so $\text{Gal}(f) = S_3$. So f has two complex and one real root and the action of $\text{Gal}(f)$ can be decomposed into a combination of complex conjugation and/or a cyclic permutation of the roots.

3. Clearly $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ the splitting field of f. This then implies the existence of H_1 and H_2 subgroups of order two in $\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q})$. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ from the definition (an element in this extension field can clearly be written as $\alpha_1 + \alpha_2\sqrt{2} + \alpha_3\sqrt{3} + \alpha_4\sqrt{6}$ for $\alpha_i \in \mathbb{Q}$) proposition 3.5 implies that $\#\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}) \leq 4$. The existence of two distinct subgroups of order 2 then clearly implies that $\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}) \cong C_2 \times C_2$. An element in the automorphism group can be written as a composition of an automorphism that sends $\sqrt{2} \to -\sqrt{2}$ and an automorphism that sends $\sqrt{3} \to -\sqrt{3}$, potentially with one or both of these automorphisms replaced with the identity automorphism.

4. Suppose $E|\mathbb{F}_5$ contains $\alpha \in E$ such that $\alpha^2 = 2$. Then $(2\alpha)^2 = 4\alpha^2 \cong 3 \bmod 5$. Therefore an automorphism which permutes the roots of $x^2 - 2$ will also permute the roots of $x^2 - 3$ in E. Thus $\text{Aut}(E|\mathbb{F}_5) \cong C_2$ and the only non-identity automorphism in this group sends $\sqrt{2} \to -\sqrt{2}$ and $\sqrt{3} \to -\sqrt{3}$.

5. For $f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}(\sqrt{6})[x]$ the splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a quadratic extension of $\mathbb{Q}(\sqrt{6})$ (as $\sqrt{2}\sqrt{3} = \sqrt{6}$, so adding one of these roots is sufficient to add the other). Consequently the automorphism group must be isomorphic to C_2. In particular, the non-identity autmorphism must send $\sqrt{2} \to -\sqrt{2}$ and since $\sqrt{6}$ is fixed it must also send $\sqrt{3} \to -\sqrt{3}$.

4.2

If $f(x) \in \mathbb{Q}[x]$ is irreducible and has degree n, then $\text{Gal}(f) = \text{Aut}(E|\mathbb{Q})$ (where $E|F$ is the splitting field of f) is a transitive subgroup of S_n where $n = \deg(f)$. Since $\mathbb{Q}$ is not characteristic 2 and the extension field contains complex elements, complex conjugation does not fix all elements in $E|\mathbb{Q}$ but does fix all elements in $\mathbb{Q}$. It is also obviously one-to-one and onto and preserves addition and multiplication, so complex conjugation is an automorphism of $E|\mathbb{Q}$.

Furthermore, since $\text{Aut}(E|\mathbb{Q})$ is a transitive subgroup of S_n and f has real and complex roots, for α a real root and β a complex root there must exist σ such that $\sigma(\beta) = \alpha$. Then, letting τ denote the automorphism of complex conjugation, if $\text{Aut}(E|\mathbb{Q})$ is Abelian it follows that $\sigma\tau(\beta) = \tau\sigma(\beta) = \alpha$. However since $\mathbb{Q}$ is of

characteristic zero this violates the requirement that σ be one to one as $\tau(\beta) \neq \beta$. Thus $\mathrm{Aut}(E|\mathbb{Q}) = \mathrm{Gal}(f)$ is not Abelian.

For an non-irreducible polynomial this is trivially false. Consider $f(x) = (x^2+1)(x-1)$. This polynomial has both real and complex roots, but the only element of $\mathrm{Gal}(f)$ is complex conjugation. Therefore $\mathrm{Gal}(f) \cong C_2$ which is Abelian.

4.3

Let $E|F$ be a Galois extension of degree 2700, so $\#\mathrm{Aut}(E|F) = 2700$. From the Sylow Theorems it follows that there must exist a subgroup H where $\#H = 27$. Therefore $[\mathrm{Aut}(E|F) : H] = 1000$ and so the corresponding fixed field has degree $[E^H : F] = 1000$ as required.

4.4

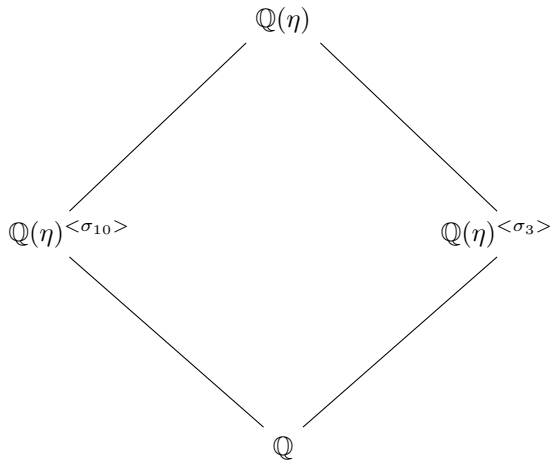
Let $G = \mathrm{Aut}(E|F)$, where $E|F$ Galois and $\#G = 625 = 5^4$. Therefore G is a p-group and so there exists one subgroup of order 5^k for $k = \{1, 2, 3\}$. Consequently there are three intermediate fields M_1, M_2 and M_3 which have degrees 125, 25 and 5 respectively.

4.5

To find the subfields of $\mathbb{Q}(\eta)$ it will be useful to consider the structure of the Galois group. In particular we have

$$\mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q}) \cong \mathbb{Z}_{11}^{\times} \cong C_2 \times C_5$$

Where the last isomorphism follows from the Chinese Remainder Theorem. It is hopefully clear that there are two subgroups of this group, H_2 isomorphic to C_2 and H_5 isomorphic to C_5. One can generate H_2 by choosing any element mapped to an element of order 2 in $\mathbb{Z}_{11}^{\times}$ and since $10^2 \cong 1 \bmod 11$ it follows that $\sigma_{10} : \eta \to \eta^{10}$ generates H_2. By an identical argument we have $< \sigma_3 >= H_5$, $\sigma_3 : \eta \to \eta^3$. It will be useful later to note that this implies $< \sigma_3, \sigma_{10} >= \mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$. The Galois correspondence then implies the following subfield diagram:



So there are two subfields of $\mathbb{Q}(\eta)$ over $\mathbb{Q}$, $\mathbb{Q}(\eta)^{<\sigma_{10}>}$ and $\mathbb{Q}(\eta)^{<\sigma_3>}$. It remains to find the minimal polynomial of a primitive element of each as extensions of $\mathbb{Q}$.

Consider $\mathbb{Q}(\eta)^{<\sigma_{10}>}$. Since the map σ_{10} takes η to $\bar{\eta}$ clearly $\omega = \frac{\eta+\bar{\eta}}{2}$ is fixed under this automorphism. Consider then the orbit of ω under σ_3. It is easy to show that the orbit of ω is

$$\mathcal{O}(\omega) = \left\{ \frac{\eta+\bar{\eta}}{2}, \frac{\eta^3+\bar{\eta}^3}{2}, \frac{\eta^2+\bar{\eta}^2}{2}, \frac{\eta^5+\bar{\eta}^5}{2}, \frac{\eta^4+\bar{\eta}^4}{2} \right\}$$

Note that since these elements are not all equal it follows that ω is not in $\mathbb{Q}$. So the polynomial

$$f(x) = \Pi_{\sigma \in <\sigma_3>}(x - \sigma(\omega)) = \left(x - \frac{\eta+\bar{\eta}}{2}\right)\left(x - \frac{\eta^2+\bar{\eta}^2}{2}\right)\left(x - \frac{\eta^3+\bar{\eta}^3}{2}\right)\left(x - \frac{\eta^4+\bar{\eta}^4}{2}\right)\left(\frac{\eta^5+\bar{\eta}^5}{2}\right)$$

$$\implies f(x) = x^5 + \frac{1}{2}x^4 - x^3 - \frac{3}{8}x^2 + \frac{3}{16}x + \frac{1}{32}$$

Is clearly fixed under every element in $\mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$ and thus $f(x) \in \mathbb{Q}[x]$. The minimal polynomial of ω must thus divide $f(x)$.

However any polynomial $g(x) \in \mathbb{Q}[x]$ that divides $f(x)$ must include one root ω' of $f(x)$. Since this polynomial is in $\mathbb{Q}[x]$ it must be fixed under every automorphism in $\mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$ and so every element in $\mathcal{O}(\omega')$ must be a root of $g(x)$. It is hopefully obvious that $\mathcal{O}(\omega') = \mathcal{O}(\omega)$ and thus the roots of $g(x)$ must include every element in $\mathcal{O}(\omega)$ (e.g. $f(x)|g(x)$).

Therefore $g(x)|f(x) \implies g(x) = f(x)$ and so $f(x)$ is the minimal polynomial of ω. Since $\mathbb{Q}(\eta)^{<\sigma_{10}>}$ has degree five from the Galois correspondence, $\mathbb{Q}(\omega)$ has degree five and the above clearly implies $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\eta)^{<\sigma_{10}>}$ we have that $\mathbb{Q}(\omega) = \mathbb{Q}(\eta)^{<\sigma_{10}>}$. Thus the minimal polynomial of a primitive element $\omega \in \mathbb{Q}(\eta)^{<\sigma_{10}>}$ is $f(x)$.

Considering the second subfield, $\mathbb{Q}(\eta)^{<\sigma_3>}$ it is easy to see that $\gamma = \eta + \eta^3 + \eta^4 + \eta^5 + \eta^9$ is fixed under σ_3 and that the orbit of γ under $\mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$ is simply

$$\mathcal{O}(\gamma) = \left\{\eta + \eta^3 + \eta^4 + \eta^5 + \eta^9, \eta^2 + \eta^6 + \eta^7 + \eta^8 + \eta^{10}\right\} = \{\gamma, \bar{\gamma}\}$$

Note $\gamma \neq \bar{\gamma}$ and it also follows that the polynomial

$$g(x) = (x - \gamma)(x - \bar{\gamma})$$

is fixed under all $\sigma \in \mathrm{Aut}(\mathbb{Q}(\eta)|\mathbb{Q})$ and from an identical argument to that above is thus the minimal polynomial of $\mathbb{Q}(\gamma)$. Furthermore the Galois correspondence implies that $\mathbb{Q}(\eta)^{<\sigma_3>}$ is a quadratic extension and since $\mathbb{Q}(\gamma)$ is also of degree two we have $\mathbb{Q}(\eta)^{<\sigma_3>} = \mathbb{Q}(\gamma)$. Therefore $g(x)$ is the minimal polynomial of a primitive element γ in $\mathbb{Q}(\eta)^{<\sigma_3>}$.

4.6

Consider $g(x) = x^4 + x^3 + x^2 + x + 1$. Clearly this polynomial splits over $\mathbb{Q}(\eta)$ where $\eta^5 = 1$, $\eta \neq 1$ and $\mathrm{Gal}(g) \cong C_4$. Then let $h(x) = x^2 - 2$, so $\mathrm{Gal}(h) \cong C_2$. Finally, let $f(x) = g(x)h(x) \in \mathbb{Q}[x]$. It is clear that the splitting field of $f(x)$ will be $\mathbb{Q}(\eta, \sqrt{2})$. We claim that that $\mathrm{Aut}(\mathbb{Q}(\eta, \sqrt{2})|\mathbb{Q}) \cong C_2 \times C_4$, so it remains to show this is the case. First, we wish to find the size of the associated automorphism group $\mathrm{Aut}(\mathbb{Q}(\eta, \sqrt{2})|\mathbb{Q})$.

Obviously $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. To find the degree of this extension we must also find $[\mathbb{Q}(\sqrt{2}, \eta) : \mathbb{Q}(\eta)]$. Since the minimal polynomial of η in $\mathbb{Q}$ is $g(x)$, the minimal polynomial of η in $\mathbb{Q}(\sqrt{2})$ must divide $g(x)$. Therefore it must be a product of the monic linear factors, $x - \eta^k$, $k \in \{1, 2, 3, 4\}$. Since we require that all coefficients must be in $\mathbb{Q}(\sqrt{2})$ it must be the case that the constant term is η^{5m} for some $m > 0$. Suppose minimal polynomial is a quadratic. Then the above condition restricts our choice of polynomials to two possibilities

$$(x-\eta)(x-\bar{\eta}) = x^2 - \frac{1}{2}(\sqrt{5}-1)x + 1 \in \mathbb{Q}(\sqrt{5})[x]$$
$$(x-\eta^2)(x-\bar{\eta}^2) = x^2 + \frac{1}{2}(\sqrt{5}+1)x + 1 \in \mathbb{Q}(\sqrt{5})[x]$$

Since $\mathbb{Q}(\sqrt{5}) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$ these polynomials are not in $\mathbb{Q}(\sqrt{2})[x]$. Furthermore the divisor cannot be a cubic as the sum of any three elements from $\{1,2,3,4\}$ is not a divisible by 5. Therefore $g(x)$ is irreducible over $\mathbb{Q}(\sqrt{2})$ so it is the minimal polynomial of η over this field. Thus $[\mathbb{Q}(\eta,\sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 4$. Therefore $[\mathbb{Q}(\eta,\sqrt{2}) : \mathbb{Q}] = 8$ and so $\#\mathrm{Aut}(\mathbb{Q}(\eta,\sqrt{2})|\mathbb{Q}) = 8$.

Since $\mathbb{Q}(\eta)$ and $\mathbb{Q}(\sqrt{2})$ are subfields of the splitting field of f there are obviously two subgroups of $H_\eta, H_{\sqrt{2}} < \mathrm{Aut}(\mathbb{Q}(\eta,\sqrt{2})|\mathbb{Q}(\sqrt{2}))$ where H_η fixes $\mathbb{Q}(\eta)$ and $\mathbb{Q}(\sqrt{2})$ is fixed by $H_{\sqrt{2}}$. Since $\mathbb{Q}(\eta)$ is the splitting field of $g(x)$ which is irreducible in $\mathbb{Q}[x]$ and $\mathbb{Q}(\sqrt{2})$ is the splitting field of $h(x)$ which is also irreducible in $\mathbb{Q}[x]$ the Galois correspondence implies both subgroups are normal. In addition $\phi \in H_{\sqrt{2}}$ fixes $\sqrt{2}$ and permutes roots of $g(x)$, so it is hopefully obvious that valid automorphisms will send η to powers of η and that $\phi : \eta \to \eta^2$ is sufficient to generate the whole group of automorphisms which must be isomorphic to C_4.

Clearly H_η acts only on the roots of $h(x)$ and has size two. Therefore the only non-identity element must send $\sqrt{2} \to -\sqrt{2}$. Thus $H_\eta \cong C_2$. Since H_η and $H_{\sqrt{2}}$ have trivial intersection (as an automorphism which fixes both η and $\sqrt{2}$ must clearly be the identity automorphism) and $\#H_\eta \# H_{\sqrt{2}} = \#\mathrm{Aut}(\mathbb{Q}(\eta,\sqrt{2})|\mathbb{Q})$ it follows that $\mathrm{Aut}(\mathbb{Q}(\eta,\sqrt{2})|\mathbb{Q}) \cong H_{\sqrt{2}} \times H_\eta \cong C_2 \times C_4$ as required.

4.7

Consider $x^{256} - x$. This polynomial has 256 roots, corresponding to each element of $\mathbb{F}_{256}$. If $g(x)$ is an irreducible monic factor of $x^{256} - x$ it clearly must be of the form

$$g(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n), \qquad \alpha_i \in \mathbb{F}_{256}, \quad \alpha_i \neq \alpha_j \quad \forall i \neq j$$

In particular, $g(x) \in \mathbb{F}_2[x]$ must be of the form

$$g(x) = \Pi_{\alpha_i \in \mathcal{O}(\alpha)}(x-\alpha_i)$$

For some $\alpha \in \mathbb{F}_{256}$. Otherwise, if $\alpha_* \in \mathcal{O}(\alpha)$ and α_* is not a root of the polynomial then there exists an automorphism which sends one root of the polynomial to α_* so the resulting polynomial is not fixed under this automorphism and thus not in $\mathbb{F}_2[x]$. The above also implies that if $\beta \notin \mathcal{O}(\alpha)$ is a root of $g(x)$ then the entire orbit of β must also be included so $g(x)$ can be written as

$$g(x) = h_\alpha(x)h_\beta(x) = \Pi_{\alpha_i \in \mathcal{O}(\alpha)}(x-\alpha_i)\Pi_{\beta_i \in \mathcal{O}(\beta)}(x-\beta_i)$$

and this polynomial is not irreducible as both $h_\alpha(x)$ and $h_\beta(x)$ are in $\mathbb{F}_2[x]$. Since the set of orbits of elements in $\mathbb{F}_{256}$ under $\mathrm{Aut}(\mathbb{F}_{256}|\mathbb{F}_2)$ forms a partition of $\mathbb{F}_{256}$ the number of monic irreducible factors is thus the number of distinct orbits in $\mathbb{F}_{256}$.

Next it is useful to consider the possible size of orbits for elements in each of the subfields of $\mathbb{F}_{256}$. If $\alpha \in \mathbb{F}_2$ then clearly $\#\mathcal{O}(\alpha) = 1$ as this field is fixed by the definition of the automorphism group. Elements in $\mathbb{F}_4 \backslash \mathbb{F}_2$ are in a degree two extension, so the maximal subgroup that fixes these is elements is a subgroup of index two in $\mathrm{Aut}(\mathbb{F}_{256}|\mathbb{F}_2)$. Since $\mathrm{Aut}(\mathbb{F}_{256}|\mathbb{F}_2)$ has size eight, this implies the subgroup has size four. Therefore the stabilizer of $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2$ has size four and the orbit has size two. By an identical argument the stabilizer of $\alpha \in \mathbb{F}_{16} \backslash \mathbb{F}_4$ has size two and so $\#\mathcal{O}(\alpha) = 4$. Finally if $\alpha \in \mathbb{F}_{256} \backslash \mathbb{F}_{16}$ the stabilizer is trivial and $\#\mathcal{O}(\alpha) = 8$.

Since there are two elements in $\mathbb{F}_2$ both these elements have an orbit of size one. There are two elements in $\mathbb{F}_4 \backslash \mathbb{F}_2$ and each of these elements belongs in an orbit of size two, so there is one orbit of size two. There are twelve elements in $\mathbb{F}_{16} \backslash \mathbb{F}_4$ and each of these belong in an orbit of size four, so there are three orbits of size four. Finally there are 240 elements in $\mathbb{F}_{256} \backslash \mathbb{F}_{16}$ each of which belong to orbits of size eight so there are 30 orbits of size eight.

Consequently there are 36 monic irreducible factors of $x^{256} - x$. However, one of these is x which is clearly not a factor of $x^{255} - 1 = (x^{256} - x)/x$. Consequently there are 35 irreducible monic factors of $x^{255} - 1$, one of which is linear, one is quadratic, three are quartic and 30 have degree eight.

4.8

If $f(x) \in \mathbb{Q}[x]$ and has degree less than 4, then $\mathrm{Gal}(f)$ is a subgroup of S_4. Galois' theorem states that f is solvable in radicals if and only if $G = \mathrm{Gal}(f)$ is solvable. Since G is a subgroup of S_4, its order must divide S_4 and thus $\#G = 2^n 3^k$ for $n \in \{0, 1, 2, 3\}$, $k = \{0, 1\}$. Clearly if n and/or k equal zero then the resulting group is either a two group or a three group. All subgroups of such groups are normal and for any two or three group each of order 2^r or 3^r there exists subgroups of that group for each $r - 1, r - 2, \ldots, 0$. This implies the existence of a Jordan-Hölder series where each Jordan-Hölder factor is either C_2 or C_3 and consequently they must be solvable.

Clearly if both n and k are greater than zero, then G must have order 6, 12 or 24 and so it is hopefully obvious that G must be one of S_3, A_4 or S_4. In assignment 2 we demonstrated that S_4 was solvable and since this composition series passed through A_4 this is sufficient to demonstrate that A_4 is also solvable. Finally $S_3 \triangleright A_3 \triangleright \{1\}$ and it is clear from this that the Jordan-Hölder series contains only C_3 and C_2 so S_3 is solvable. Thus all polynomials in $\mathbb{Q}[x]$ of degree four or less are solvable in radicals.