MATH411 Final Exam

Elliott Hughes

June 23, 2022

Q1

(a)

It is straightforward to show the conjugacy classes of the generators of D_6. First $\rho^q\rho^n\rho^{-q} = \rho^n$ for $n, q \in \mathbb{Z}$ and $\sigma\rho^n\sigma = \rho^{-n}$. Finally $\sigma\rho^q\rho^n\rho^{-q}\sigma = \rho^{-n}$. Since $\rho^q\sigma = \rho^{-q}\sigma$ this is sufficient to demonstrate that ρ^n is conjugate to ρ^{-n} and no other elements.

Furthermore $\sigma\rho^n\sigma\sigma = \rho^{-n}\sigma$, $\rho^q\rho^n\sigma\rho^{-q} = \rho^{2q+n}\sigma$ and $\sigma\rho^q\rho^n\sigma\rho^{-q}\sigma = \sigma\rho^{2q+n}\sigma\sigma = \rho^{-2q-n}\sigma$. By an identical argument as above this limits the possible conjugacy classes to the following set

$$\begin{align} &\{\rho, \rho^5\} \tag{1}\\ &\{\rho^2, \rho^4\} \tag{2}\\ &\{\rho^3\} \tag{3}\\ &\{\sigma, \rho^2\sigma, \rho^4\sigma\} \tag{4}\\ &\{\rho\sigma, \rho^3\sigma, \rho^5\sigma\} \tag{5}\\ &\{e\} \tag{6} \end{align}$$

So the center is simply the set of conjugacy classes of size one, or $Z(D_6) = \{e, \rho^3\}$.

(b)

Consider the set $S = \{e, \sigma\rho^2, \sigma\rho^4, \sigma, \rho^2, \rho^4\}$. The Cayley table of this set is

	e	σ	$\sigma\rho^2$	$\sigma\rho^4$	ρ^2	ρ^4
e	e	σ	$\sigma\rho^2$	$\sigma\rho^4$	ρ^2	ρ^4
σ	σ	e	ρ^2	ρ^4	$\sigma\rho^2$	$\sigma\rho^4$
$\sigma\rho^2$	$\sigma\rho^2$	ρ^4	e	ρ^2	$\sigma\rho^4$	σ
$\sigma\rho^4$	$\sigma\rho^4$	ρ^2	ρ^4	e	σ	$\sigma\rho^2$
ρ^2	ρ^2	$\sigma\rho^4$	σ	$\sigma\rho^2$	ρ^4	e
ρ^4	ρ^4	$\sigma\rho^2$	$\sigma\rho^4$	σ	e	ρ^2

Therefore this set is a subgroup and it is isomorphic to S_3. Since S_3 has size six it has index two in D_6 and is thus normal. Furthermore $Z(D_6)$ is trivially normal in D_6, these sets have trivial intersection and $Z(D_6)S = D_6$ so $D_6 \cong Z(D_6) \times S \cong \mathbb{Z}_2 \times S_3$.

(c)

Clearly any size six subgroup will have to contain a size three subgroup and this size three subgroup must be contained in S_3 so there is only one such subgroup in D_6 ($H_3 \cong A_3 < S_3$). Since this is the only size three subgroup the Sylow theorems imply that it is normal. It follows from the correspondence theorem that the number of index two subgroups (which must contain H_3) must be equal to the number of index two subgroups in D_6/H_3. It is straightforward to find $H_3 = \{e, \rho^2, \rho^4\}$ and so enumerate the elements of D_6/H_3

$$D_6/H_3 = \{H_3, \rho H_3, \sigma H_3, \rho\sigma H_3\}$$

Since three of these elements have order two, there must be three index two subgroups in D_6. So there are three order six subgroups of D_6. In particular there exists $H_\rho = \{e, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$ the subgroup of rotations, $H_\sigma = \{e, \sigma, \rho^2, \rho^4, \sigma\rho^2, \sigma\rho^4\}$ and $H_{\rho\sigma} = \{e, \rho\sigma, \rho^2, \rho^4, \rho^3\sigma, \rho^5\sigma\}$.

Q2

(a)

It is hopefully obvious that $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$. Since the cube root of unity is an element of $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ the polynomial $x^3 - 5$ splits over $\mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$. Straightforward enumeration shows that the maximum possible basis size is $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{-5}) : \mathbb{Q}] \leq 12$ and since both $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ must divide $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{-5}) : \mathbb{Q}]$ it follows that $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{-5}) : \mathbb{Q}] = 12$. This field is the splitting field of $f(x) = (x^2 - 2)(x^2 + 3)(x^3 - 5)$ which is separable and so K is Galois.

The existence of a size 6 subgroup is trivial as $\mathbb{Q}(\sqrt{2})$ is a subfield of K and is a quadratic extension of $\mathbb{Q}$. Therefore there exists H_6 fixing $\mathbb{Q}(\sqrt{2})$ which must be normal. Furthermore since $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ is the splitting field of the separable polynomial $f(x) = (x^2 + 3)(x^3 - 5)$ it is Galois and since $[\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5}) : \mathbb{Q}] = 6$ there exists some size two subgroup which is normal in $H_2 \triangleleft \mathrm{Aut}(K|\mathbb{Q})$.

Since an automorphism that fixes both the elements in $\mathbb{Q}(\sqrt{2})$ and elements in $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ must fix all elements in K it must be true that $H_2 \cap H_6 = e$. Furthermore $H_2 H_6 = \mathrm{Aut}(K|\mathbb{Q})$ it follows that $H_2 \times H_6 \cong \mathrm{Aut}(K|\mathbb{Q})$. It remains to show that H_6 is isomorphic to S_3. Since H_6 fixes $\mathbb{Q}(\sqrt{2})$ it must permute $\sqrt{-3}$, $-\sqrt{-3}$ and $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$, $\sqrt[3]{5}$. Complex conjugation clearly permutes these roots and fixes $\sqrt{2}$, $-\sqrt{2}$ so it must be an element of H_6. Let τ denote this automorphism with $H' = \{e, \tau\}$ and let σ be an element of size three in H_6. Then for a a not fixed by H_6, $\sigma\tau\sigma^{-1}(a) \neq \bar{a}$ for all a unless $\sigma^{-1}(a) = 5^{1/3}$. So $\sigma H' \sigma^{-1} \neq H'$ and there must be more than one size two subgroup of H_6. The only group with these properties is S_3 so $H_6 \cong S_3$. Therefore $\mathrm{Aut}(K|\mathbb{Q}) \cong \mathbb{Z}_2 \times S_3$ as required.

(b)

Clearly $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. From an identical argument to that above it follows that $[\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}] \mid [E : \mathbb{Q}]$ and $[E : \mathbb{Q}] \leq 28$ so $[E : \mathbb{Q}] = 28$. But $E|\mathbb{Q}$ is normal only if $x^7 - 5$ splits in E. This holds only when the seventh primitive root of unity (denoted here ω) is in E. This would imply that $\mathbb{Q}(\omega) \subseteq E$. But $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$ and $6 \nmid 28$ so $\omega \notin E$. Therefore E is not normal.

Q3

Clearly the roots of the polynomial are given by

$$x = \omega(2 \pm \sqrt{3})^{\frac{1}{3}} \qquad \text{where} \quad \omega^3 = 1, \quad \omega \neq 1$$

Let $\alpha = (2 + \sqrt{3})^{\frac{1}{3}}$ and $\beta = (2 - \sqrt{3})^{\frac{1}{3}}$. The splitting field of this polynomial over $\mathbb{Q}$ is then $E = \mathbb{Q}(\omega, \sqrt{3}, \alpha, \beta)$. It is also useful to note that $\alpha = -1/\beta$. Clearly $[\mathbb{Q}(\omega, \sqrt{3}) : \mathbb{Q}] = 4$ and since α is cube root the minimal polynomial of α must have a degree divisible by three so it follows that $4, 3 | [\mathbb{Q}(\omega, \sqrt{3}, \alpha) : \mathbb{Q}]$ and $[\mathbb{Q}(\omega, \sqrt{3}, \alpha) : \mathbb{Q}] \leq 12$ so $[E : \mathbb{Q}] = 12$ as $\beta \in \mathbb{Q}(\omega, \sqrt{3}, \alpha)$.

The automorphism group must then have size 12. Since $\mathbb{Q}(\omega, \sqrt{3})$ has degree four and is Galois there exists a normal subgroup of size three, $H_3 \cong A_3$. This implies that the number of Sylow three subgroups must be one and so all subgroups of size six must include this subgroup. The correspondence theorem then implies that the structure of the subgroup lattice above H_3 is equivalent to the structure of the subgroup lattice of G/H_3. Since G/H_3 has order four it must be congruent to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, which implies there are either one or three extensions of degree six (as a subgroup with index 2 in G must match a subgroup of index 2 in G/H_3). Since there are at least two subgroups of index 2 in G (as $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\omega)$ are both quadratic extensions of $\mathbb{Q}$ and proper subfields of E) it follows that there must be exactly three such extensions.

Consider $\sigma \in \mathrm{Aut}(E|\mathbb{Q})$. Note furthermore that since σ is an automorphism, the action of σ on β is determined entirely by its action on α. Since σ must permute the roots of $f(x) = x^6 - 4x^3 + 1$ it follows that either $\sigma(\alpha) = \omega^n \alpha$ or $\sigma(\alpha) = \omega^n \beta$ and that $\sigma(\beta) = -\sigma$. Consider then the automorphism τ taking α to β (that this is an automorphism is straightforward to verify) it follows that for γ a root $\sigma\tau\sigma(\gamma) = -\gamma^{-1} = \tau(\gamma)$ and so the set $H_2 = \{e, \tau\}$ is a size two normal subgroup of $\mathrm{Aut}(E|F)$.

Consider furthermore the subfield $\mathbb{Q}(\sqrt{3})$. Since $\tau(2 + \sqrt{3}) = (\alpha^3) = \beta^3 = 2 - \sqrt{3}$ it follows that τ does not fix this subfield, so the size six subgroup $H_{\sqrt{3}}$ fixing this field (which has index two and is thus normal) and H_2 have trivial intersection. Therefore since together they compose the whole set it follows that $\mathrm{Aut}(E|F) \cong H_2 \times H_{\sqrt{3}}$.

It is also useful to note that f is irreducible (as while $(\alpha\beta)^n \in \mathbb{Q}$ for all n, $\alpha^n + \beta^n \in \mathbb{Q}$ only for $n = 3$). Therefore, using the result from problem 4.2 of the final assignment, G cannot be Abelian. It thus follows that $H_{\sqrt{3}}$ must be a non-Abelian group of order 6, of which S_3 is the only possible choice. Thus $\mathrm{Aut}(E|F) \cong \mathbb{Z}_2 \times S_3 \cong D_6$.

Q4

Since $E|F$ is Galois with $\mathrm{Aut}(E|F) \cong S_3$ the characterisation of Galois extensions implies that there exists some $g(x)$ seperable which splits over $E|F$. Let $g(x) = h_1(x)h_2(x)\dots h_n(x)$ where each $h_i(x) \in F[x]$ is an irreducible factor. It is clear that there exists $g^*(x)$ a separable polynomial with no roots in F (as any linear h_i can be eliminated from $g(x)$ and it will still split only over $E|F$). Then if g^* is not irreducible there exists some $h_1(x), h_2(x), \dots h_n(x) \in F[x]$ which are irreducible and seperable polynomials. If any h_i split only in $E|F$ then we have obtained the desired result.

If however, all $h_1, h_2, \dots, h_n$ split in proper subfields of $E|F$ then there must exist h_k, h_j which split only in distinct subfields (as otherwise the splitting field of $g(x)$ would be the proper subfield rather than $E|F$). Then since h_k and h_j are separable the splitting fields of these two polynomials are themselves Galois extensions and so this implies the existence of two distinct normal subgroups of S_3 by the Galois correspondence. However, S_3 has only one normal subgroup A_3 and so this is a contradiction. Thus there must exist an irreducible polynomial that splits in $E|F$ as required.

Q5

(a)

Clearly σ, τ fix K and for $f(x) \in K(x)$ it is clear that $\sigma(f), \tau(f) \in K(x)$. These functions are their own inverses and thus these inverses are well-defined everywhere the functions are defined, so they must be one-to-one and onto. Thus $\sigma, \tau \in \mathrm{Aut}(K(x))$.

(b)

Note that $\sigma\tau\sigma(x) = 1 - \frac{1}{1-x}$ is also an order two automorphism. From this it is easy although tedious to compute the following Cayley Table:

	e	σ	τ	$\sigma\tau\sigma$	$\sigma\tau$	$\tau\sigma$
e	e	σ	τ	$\sigma\tau\sigma$	$\sigma\tau$	$\tau\sigma$
σ	σ	e	$\sigma\tau$	$\tau\sigma$	τ	$\sigma\tau\sigma$
τ	τ	$\tau\sigma$	e	$\sigma\tau$	$\sigma\tau\sigma$	σ
$\sigma\tau\sigma$	$\sigma\tau\sigma$	$\sigma\tau$	$\tau\sigma$	e	σ	τ
$\sigma\tau$	$\sigma\tau$	$\sigma\tau\sigma$	σ	τ	$\tau\sigma$	e
$\tau\sigma$	$\tau\sigma$	τ	$\sigma\tau\sigma$	σ	e	$\sigma\tau$

So this group G is isomorphic to S_3.

(c)

It is possible although tedious to show $\sigma(u) = u$ and $\tau(u) = \tau$, so $K(u) \subset E^G$. Consider the polynomial $f(y) \in K(u)[y]$,

$$f(y) = (y^2 + u)(y^4 - 2y^3 + y^2) - y^5 - y^4 + 5y^3 - 3y + 1$$

When $y = x$ this polynomial becomes the zero polynomial (in x), so x is a root of $f(y)$. Since any polynomial in x that has x indeterminate as a root must be the zero polynomial, any polynomial $f(y) \in K(u)[y]$ that has $y = x$ as a solution and is not the zero polynomial in $K(u)[y]$ must include a power of u as a coefficient. Since we furthermore require that $f(x)$ be a polynomial this implies that the minimum degree must be the largest degree in the numerator of u (as since the numerator also includes a constant term one cannot divide by a non-constant rational function and obtain a polynomial in x). Therefore $[K(x) : K(u)] = 6$.

Artin's lemma then implies that $[E : E^G] \leq 6$ and since $[E : K(u)] = 6$ it follows that $[E^G : K(u)] = 1$ and so $E^G = K(u)$.