MATH411 Assignment 2

Elliott Hughes

May 20, 2022

3.1

Let $E|F$ be a Galois extension of a field F and let $f(x) \in F[x]$ irreducible over F. Then $f(x)$ can be factored into a product of some scalar and a set of monic polynomials irreducible over $E|F$, $f(x) = af_1(x)f_2(x)\dots f_n(x)$, $a \in F$. For some $\sigma \in \mathrm{Gal}(E|F)$ it follows that

$$a\sigma(f_1(x))\sigma(f_2(x))\dots\sigma(f_n(x)) = af_1(x)f_2(x)\dots f_n(x)$$

Since f has a unique factorization up to order in E and σ must map monic polynomials to monic polynomials it follows that $\sigma(f_i) = f_j$ for some f_i, f_j in the factorization. It remains to show that this groups acts transitively on these irreducible factors.

Consider the action $\mathrm{Aut}(E|F) \circlearrowleft \{f_j\}$, where $\{f_j\}$ is the set of irreducible factors. Then for f_j in this set, denote the product of irreducible factors in this orbit as $p(x)$. Cearly $p(x)|f(x)$ and, furthermore, note that for $\phi \in \mathrm{Aut}(E|F)$, $\phi(p(x)) = p(x)$ by the definition of orbits. Since this implies that each coefficient in $p(x)$ is fixed for all $\phi \in \mathrm{Aut}(E|F)$ it follows from the fact that $E|F$ is Galois that $p(x) \in F[x]$. Then since $f(x)$ is irreducible this implies that $f(x) = ap(x)$ and therefore that $\mathrm{Aut}(E|F)$ acts transitively on the irreducible factors of $f(x)$ in E.

3.2

Let $E|F$ be an extension of F and let H be a subgroup of $\mathrm{Aut}(E|F)$. The set E^H is non-empty as clearly $F \subseteq E^H$. Then for $a, b \in E^H$ and $\phi \in H$ we have $\phi(a-b) = \phi(a) - \phi(b) = a - b$ so $a - b \in E^H$. Furthermore, for $a \in E^H$, $b \in E^H \backslash \{0\}$ we have $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = ab^{-1}$ so E^H is a subfield of $E|F$ and consequently a field.

3.3

Let $E|F$ be an algebraic extension, $\theta \in E$ and $g(x) \in F[x]$ the minimal polynomial of θ over F. For $\sigma \in \mathrm{Aut}(E|F)$ we have $\sigma(g(\theta)) = \sigma(g)(\sigma(\theta)) = g(\sigma(\theta)) = \sigma(0) = 0$ and so $\sigma(\theta)$ is a root of g.

For $f \in F[x]$, $E|F$ splitting f it follows that there exists a finite set of roots in $E|F$, $R = \{\theta_0, \theta_1, \dots, \theta_n\}$. Since for any $\sigma \in \mathrm{Gal}(f)$ and for any $\theta \in R$ it must be true that $\sigma(\theta) \in R$ we can define the action $\sigma \star \theta = \sigma(\theta)$. It remains to show that this fulfills the definition of a group action. Since the identity automorphism is clearly the identity of $\mathrm{Gal}(f)$ the first requirement is straightforwardly fulfilled. The second restriction that for $\sigma_1, \sigma_2 \in \mathrm{Gal}(E|F)$ and $\theta \in R$, $\sigma_1 \star \sigma_2 \star \theta = \sigma_1\sigma_2 \star \theta$ is clearly fulfilled by the properties of automorphism groups. Therefore this action is a valid group action.

3.4

Let $f \in F[x]$ and $E|F$ be the splitting field of f, with the set of roots $R = \{\theta_1, \theta_2, \dots, \theta_n\}$. From 3.3 and the requirement that for any $\sigma \in \text{Aut}(E|F)$, $\sigma(f) = f$ it follows that each σ defines a permutation on R. Therefore $\text{Aut}(E|F) \cong H \leq \text{Sym}(R)$.

Assume that this homomorphism is not injective. This implies that the kernel is non-trivial and thus that there exists a non identity $\sigma \in \text{Aut}(E|F)$ such that $\sigma(\theta) = \theta$ for all $\theta \in R$. However since $E = F(\theta_1, \theta_2, \dots, \theta_n)$, if $\sigma(\theta) = \theta$ for all $\theta \in R$ then since every element can be written as a sum and/or product of elements fixed by σ it follows that $\sigma(x) = x$ for all $x \in E$ which contradicts our assumption. Therefore this homomorphism is injective.

3.5

Clearly, $\phi(\theta) = \phi(\eta^3\theta) = \eta\theta$ and $\phi(\eta\theta) = \eta^2\theta$ which implies $\phi(\eta) = \phi(\eta\theta\theta^{-1}) = \phi(\eta\theta)\phi(\theta^{-1}) = \eta^2\theta(\eta\theta)^{-1} = \eta$. From the actions on these two elements and the fact that ϕ fixes any element in F we can construct the matrix that gives the action of ϕ on elements of the vector space of E over $\mathbb{Q}$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

The corresponding 1-eigenspace is comprised of the first and fourth columns, or $\mathbb{Q}(\eta)$. This agrees with our initial computation that $\phi(\eta) = \eta$.

3.6

Clearly the roots of this polynomial are products of η, ζ where η is one of the fifth roots of unity and $\zeta = 2^{1/5}$. The splitting field can then be straightforwardly written as $\mathbb{Q}(\eta, \zeta)$. To compute the degree of this extension, it is convenient to consider the degrees of constituent subfields. In particular, consider $\mathbb{Q}(\eta)$. This is the cyclotomic extension of $\mathbb{Q}$ corresponding to the fifth root of unity. Therefore $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$ by theorem 5.1.

Consider $\mathbb{Q}(\eta, \zeta)|\mathbb{Q}(\eta)$. This extension splits $x^5 - 2$ and every root of this polynomial contains ζ, so any divisor of this polynomial will have a constant term corresponding to some power of ζ (potentially multiplied by some other term). Then $\zeta^n \notin \mathbb{Q}(\eta)$ for $n \in \{1, 2, 3, 4\}$ so this is the minimal polynomial over $\mathbb{Q}(\eta)$. Consequently $[\mathbb{Q}(\eta, \zeta) : \mathbb{Q}(\eta)] = 5$. Therefore the degree of the splitting field of $x^5 - 2$ is $[\mathbb{Q}(\eta, \zeta) : \mathbb{Q}] = 20$ by the Tower Theorem.

Consequently $\text{Aut}(\mathbb{Q}(\eta, \zeta)|\mathbb{Q}) \cong H < S_5$ with $|H| = 20$. A subgroup of order 20 must contain s_2 Sylow-2-Groups and s_5 Sylow-5-Groups. In particular $s_5 \cong 1 \bmod 5$ and $s_5|2$ so $s_5 = 1$ so H contains a single group of order 5.

Furthermore, consider the subgroup $K < \text{Aut}(\mathbb{Q}(\eta, \zeta)|\mathbb{Q})$, where $\phi(\zeta) = \zeta$. This is a subgroup of the automorphism group and it is clearly isomorphic to $\text{Aut}(\mathbb{Q}(\eta)|\mathbb{Q}) \cong \mathbb{Z}_4^+$. Therefore there is a subgroup of the automorphism group (we will denote this subgroup A) and $A \cong \mathbb{Z}_4^+$. Clearly then if $a \in A$ and b is an element of the Sylow-5-Group then H is generated by a and b. Since a group of order 10 cannot contain elements of order four and it must contain b it follows that such a group must be generated by a^2 and b. Furthermore all elements in the Sylow-5-Group are conjugate to some other element in that group, $a^2b^r = b^na^2$ for some $n, r \in \mathbb{N}$. The set generated by a^2 and b is therefore a subgroup of H and since it is the only possible such subgroup of order 10 it follows that there is one subgroup of index 2 in $\text{Aut}(\mathbb{Q}(\eta, \zeta)|\mathbb{Q})$. The Galois correspondence then implies that there is only one quadratic subfield in $\mathbb{Q}(\eta, \zeta)|\mathbb{Q}$.

3.7

The homomorphism $\Phi : \mathrm{Norm}(H) \to \mathrm{Aut}(E^H|F)$ (where $\mathrm{Norm}(H)$ is the normalizer of H) induced by restricting the action of $\phi \in \mathrm{Norm}(H)$ to E^H is well-defined as $\phi(E^H) = E^H$ by the third property of the Galois Correspondence. Then clearly $\ker(\Phi) = H$ and so there is an injective homomorphism between $\mathrm{Norm}(H)/H$ and $\mathrm{Aut}(E|F)$.

Consider ϕ an injective homomorphism from a subfield K to E and write $E = K(\alpha_1, \alpha_2, \ldots, \alpha_l)$ (note that E is finite so the set of elements that must be adjoined is finite). Clearly E is algebraic over K as E is the splitting field of some polynomial in $f(x) \in F[x] \subset K[x]$. Thus for α_1 the minimal polynomial of α_1 in K exists, is irreducible and has at least one root in E, so there is at least one extension of ϕ which is an injective homomorphism from $K(\alpha_1)$ to E that agrees on K by Lemma 3.4.

Let $K_0 = E^H$. Then from above we can write $E = K_0(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Consider a sequence of subfields K_i, $i = 1, 2, \ldots, n$ with $K_1 = E^H(\alpha_1)$, $K_{i+1} = K_i(\alpha_{i+1})$. Then for $\phi \in \mathrm{Aut}(E^H|F)$ define ϕ_1 as the injective homomorphism from $K_1 \to E$ which agrees with ϕ on E^H. From the argument above, we can inductively define a sequence of injective homomorphisms from $K_i \to E$ which agree with ϕ on E^H. In particular there exists ϕ_n an injective isomorphism from $K_n = E$ to E which agrees with ϕ on E^H.

We wish to show that this is an automorphism of $E|F$, so it remains to show that it is surjective. Since ϕ_n agrees with ϕ on E^H it follows that $\phi_n(0) = 0$. Then for $a \in E$, $a \neq 0$ and $\phi_n(a) \neq 0$ as ϕ_n is injective. Furthermore if $\phi_n(a) = b$ then the injectivity of ϕ_n implies $\phi_n^{-1}(b) = a$ and so $\phi_n(b^{-1}) = a$. Since b^{-1} is well-defined it follows that ϕ_n is surjective and so ϕ_n is an automorphism (F is trivially fixed as ϕ_n agrees with $\phi \in \mathrm{Aut}(E^H|F)$ on F).

Thus for $\phi \in \mathrm{Aut}(E|F)$ and the map $\phi \to \phi_n$ is clearly injective as the action of any two elements of $\mathrm{Aut}(E^H|F)$ differs on E^H so it will differ on E. Trivially $\phi(E^H) = E^H$ and so $\phi_n \in \mathrm{Norm}(H)$. As their action differs on E^H each ϕ_n belongs to a different coset of $\mathrm{Norm}(H)/H$ and so there is an injective homomorphism between $\mathrm{Aut}(E|F)$ and $\mathrm{Norm}(H)/H$. Therefore these groups are isomorphic.