Mathematics GU4042 Modern Algebra II
Assignment # 8

Benjamin Church

February 16, 2020

Page 200. Problem 6.

Let ζ be a primitive n^{th} root of unity in a field extension E/K. That is, ζ is a root of $X^n - 1$ and not of $X^k - 1$ for any $k < n$. Consider $G \subset E$, the set of all roots of the polynomial $X^n - 1$. Now, if $\alpha, \beta \in G$ then $(\alpha\beta)^n - 1 = \alpha^n\beta^n - 1 = 0$ because $\alpha^n = \beta^n = 1$. Furthermore, $\alpha \neq 0$ (since $0^n = 0 \neq 1$) so $\alpha^{-1} \in E$ and $(\alpha^{-1})^n = (\alpha^n)^{-1} = 1^{-1} = 1$ so $\alpha^{-1} \in E$. Therefore, $(G, \cdot)$ is a group and because each element satisfies $X^n - 1$ which has at most n roots in E then $|G| \leq n$ so G is finite. Therefore, as a finite multiplicative subgroup of a field, G is cyclic. Suppose that $\zeta^i = \zeta^j$ with $i > j$, then $\zeta^{i-j} = 1$ but because ζ is primitive, $i - j > n$. Therefore, for $0 \leq i, j < n$, the n powers of ζ are all distinct meaning that the entire group is only powers of ζ. Thus, ζ is a generator of G.

Consider the extension $K(\zeta)/K$. Because $G = \langle\zeta\rangle$ and $K(\zeta)$ is a subfield of E, then $G \subset K(\zeta)$ so $K(\zeta)$ contains all the roots of $X^n - 1$. Furthermore, $K(\zeta) = K(G)$ because $\zeta \in G$ and $G \subset K(\zeta)$. Therefore, $K(\zeta)$ is the splitting field of $X^n - 1$ over K. Therefore, $K(\zeta)/K$ is a normal extension. The extension is also seperable because K has characteristic zero. Therefore, $K(\zeta)/K$ is a Galois extension. Finally, consider $\text{Gal}\,(K(\zeta)/K)$ which is embedded in S_n because $\deg(X^n - 1) = n$. Any Galois automorphism restricted to G is a group automorphism of G because it is multiplicative and permutes roots. Because the group of automorphisms of any cyclic group is abelian (see Lemma **??**), for any $\sigma, \tau \in \text{Gal}\,(K(\zeta)/K)$ then $\sigma|_G \circ \tau|_G = \tau|_G \circ \sigma|_G$. However, the map from $\text{Gal}\,(E/K)$ into S_n given by the action of $\text{Gal}\,(E/K)$ on G (the roots of $X^n - 1$) is injective since $E = K(G)$ so if σ fixes G and K then it is the idenitity on E. Because $\sigma \circ \tau$ and $\tau \circ \sigma$ acts indentically on G by injectivity $\sigma \circ \tau = \tau \circ \sigma$. Therefore $\text{Gal}\,(E/K)$ is abelian.

Probelm 2.

Let E be the splitting field of $X^3 - 2$ over $\mathbb{Q}$. Take $\alpha = \sqrt[3]{2}$ and $\zeta = \frac{-1+\sqrt{-3}}{2}$. The Galois group $\text{Gal}\,(E/\mathbb{Q})$ is isomorphic to $S_3 = \langle\sigma, \tau\rangle$ with automorphisms acting as follows,

$$\sigma : \zeta^i\alpha \mapsto \zeta^{i+1}\alpha$$
$$\tau : x \mapsto \bar{x}$$

which permute the roots of $X^3 - 2$. Now, we consider the element $AB \in E$ where $A = \alpha = \sqrt[3]{2}$ and $B = \sqrt{-3} = 2\zeta + 1$. The six elements of S_3 are presented as $\sigma^i\tau^j$ for $0 \leq i \leq 2$ and $0 \leq j \leq 1$. Therefore, we can calculate the conjugtes of AB by acting on the element $AB = (2\zeta + 1)\alpha$ with the

elements of the Galois group:

$$\sigma^0\tau^0((2\zeta+1)\alpha) = \mathrm{id}((2\zeta+1)\alpha) = (2\zeta+1)\alpha = \sqrt{-3}\cdot\sqrt[3]{2}$$
$$\sigma^0\tau^1((2\zeta+1)\alpha) = \tau((2\zeta+1)\alpha) = (2\bar{\zeta}+1)\alpha = -\sqrt{-3}\cdot\sqrt[3]{2}$$
$$\sigma^1\tau^0((2\zeta+1)\alpha) = \sigma((2\zeta+1)\alpha) = (2\zeta+1)\zeta\alpha = \zeta\sqrt{-3}\cdot\sqrt[3]{2}$$
$$\sigma^1\tau^1((2\zeta+1)\alpha) = \sigma((2\bar{\zeta}+1)\alpha) = (2\bar{\zeta}+1)\zeta\alpha = -\zeta\sqrt{-3}\cdot\sqrt[3]{2}$$
$$\sigma^2\tau^0((2\zeta+1)\alpha) = \sigma^2((2\zeta+1)\alpha) = (2\zeta+1)\zeta^2\alpha = \zeta^2\sqrt{-3}\cdot\sqrt[3]{2}$$
$$\sigma^2\tau^1((2\zeta+1)\alpha) = \sigma((2\bar{\zeta}+1)\alpha) = (2\bar{\zeta}+1)\zeta^2\alpha = -\zeta^2\sqrt{-3}\cdot\sqrt[3]{2}$$

Lemmas

Lemma 0.1. Let G be cyclic, then $\mathrm{Aut}(G)$ is abelian.

Proof. Take a generator $g \in G$. Now, let $\sigma, \tau : G \to G$ be automorphisms. Then $\sigma(g) = g^{k_\sigma}$ and $\tau(g) = g^{k_\tau}$ because every element in G is a power of g. Thus, for any element $g^r \in G$,

$$\sigma\circ\tau(g^r) = \sigma(\tau(g)^r) = \sigma(g^{k_\tau r}) = \sigma(g)^{k_\tau r} = (g^{k_\sigma})^{k_\tau r} = g^{k_\sigma k_\tau r}$$

$$\tau\circ\sigma(g^r) = \tau(\sigma(g)^r) = \tau(g^{k_\sigma r}) = \tau(g)^{k_\sigma r} = (g^{k_\tau})^{k_\sigma r} = g^{k_\tau k_\sigma r}$$

However, $k_\sigma k_\tau = k_\tau k_\sigma$ because integer multiplication is commutative. Therefore, $\sigma\circ\tau(g^r) = \tau\circ\sigma(g^r)$. However, every element of G is of the form g^r so $\sigma\circ\tau = \tau\circ\sigma$. □