Mathematics GU4042 Modern Algebra II
Assignment # 11

Benjamin Church

February 16, 2020

Problem 1.

Let $f(X) = a_n X^n + \cdots + a_1 X + a_0$ be an irreducible polynomial over K. Now,

$$f'(X) = n \cdot a_n X^{n-1} + \cdots a_1$$

If $f' \neq 0$ then f is f is seperable because it will be coprime to f'. Otherwise, because K has characteristic zero, the unique homomorpihsm $\mathbb{Z} \to K$ given by repeated addition is injective so $f' = 0$ implies that $a_n = \cdots = a_1 = 0$. Therefore, $f(X) = a_0$ which is already split in K and has no roots. Thus, f is vacuously seperable.

Page 210.

Problem 2.

Let $f \in \mathbb{R}[X]$ be a degree 3 polynomial. Because f is of odd degree, it must take on both positive and negative values over $\mathbb{R}$. Therefore, by IVT, f has at least one real root. Furthermore, if $f(\alpha) = 0$ then $\overline{f(\alpha)} = f(\overline{\alpha}) = 0$ so $\bar{\alpha}$ is also a root of f. The complex conjugation automorphism can be brought inside f because its coeficients are all real. Thus, if f has a complex root then it has a pair of complex roots. Thus, there are two possibilities, either f has three real roots or f has one real root and two conjugate complex roots. Now, consider the discriminant,

$$\text{Disc}(f) = \Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

If all three roots of f are real then all the differences are real. Thus, $(\alpha_i - \alpha_j)^2 \geq 0$ so $\Delta \geq 0$. Therefore, if $\Delta < 0$ then f has one real root and two complex roots. If $\Delta = 0$ then f has a double root. However, if f had only a single real root then it could not be equal to the other two complex roots which also could not equal eachother because they are complex conjugates and not real. Therefore, if $\Delta = 0$ then f has three real roots. Finally, suppose that $\Delta > 0$. Then, Δ is a square in $\mathbb{R}$ so the Galois group of E, the splitting field of f over $\mathbb{R}$, contains no odd permutations and is thus a subgroup of $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. However, no element of $\mathbb{Z}/3\mathbb{Z}$ has order 2 so complex conjugation cannot be a nontrivial automorphism of E. However, complex conjugation takes a root of f to another root of f and fixes the base field $\mathbb{R}$ so it preserves $E = \mathbb{R}(\alpha_1, \alpha_2, \alpha_3)$ and thus complex conjugation is an automorphism of E. Therefore, E cannot be have complex elements because complex conjugation acts trivially so f must have only real roots. Because $\Delta \neq 0$ we know that f is seperable so it has exactly 3 real roots.

Page 220.

Problem 9. and Problem 10.

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 0.1), 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.

Finally, $[E : K] = [K(\zeta) : K] = \deg \text{Min}(\zeta; K)$ and ζ is a root of $X^n - 1$ so $\text{Min}(\zeta; K) \mid X^n - 1$ and thus $\deg \text{Min}(\zeta; K) \leq n$. Therefore, $[K(\zeta) : K] \leq n$.

Problem 11.

Take the extension $\mathbb{Q}(\zeta_4)$ where $\zeta_4 = e^{\frac{2\pi i}{4}} = i$ generates the group of 4th roots of unity, $\{1, i, -1, -i\}$. However, $\zeta_4 = i$ is a root of $X^2 + 1$ so the simple extension $\mathbb{Q}(\zeta_4)$ is quadratic and therefore, $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2 < 4$.

Lemmas

Lemma 0.1. Let G be cyclic, then $\text{Aut}(G)$ 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 $\sigma \circ \tau = \tau \circ \sigma$. □