MAT 612 **HW #7** Name SOLUTIONS
04/17/10, due Friday 04/23/10, 5 pm
25 points

For these problems, use the Fundamental Theorem of Galois Theory (which we are in the midst of proving in class): if E is Galois over F with $|E:F| < \infty$, then subgroups of $G = \mathrm{Gal}(E,F)$ are in one-to-one correspondence with fields K with $F \subseteq K \subseteq E$, and $|E:K| = |\mathrm{Gal}(E,K)|$. Moreover, $H = \mathrm{Gal}(E,K)$ is normal in G if and only if K is Galois over F, in which case $G/H \cong \mathrm{Gal}(K,F)$.
In addition, you may use the following results (which will be proved in the course of proving the "FTGT"): if $\mathrm{char}(F) = 0$ then E is Galois over F if and only if E is a splitting field of some polynomial in $F[x]$. In this case, every irreducible $f \in F[x]$ splits over E, and G acts transitively on its roots.

1. Find a splitting field $E \subseteq \mathbb{C}$ of the polynomial $f(x) = x^4 - 4$ over $\mathbb{Q}$. Identify the Galois group, and find $\alpha \in E$ such that $E = \mathbb{Q}[\alpha]$. (α is called a *primitive element* for the extension.)

2. Let $\omega = e^{2\pi i/n}$.

   (a) Show that $E = \mathbb{Q}[\omega]$ is a splitting field for the polynomial $f(x) = x^n - 1$, hence E is Galois over $\mathbb{Q}$.

   (b) Show that $\mathbb{Q}[\omega^k] = \mathbb{Q}[\omega]$ if $(k,n) = 1$, use this to prove that $\mathrm{Gal}(E,\mathbb{Q})$ is isomorphic to the group $U(\mathbb{Z}_n)$ of units in $\mathbb{Z}_n$. Stipulation: $\prod_{(k,n)=1}(x-\omega^k)$ is irreducible over $\mathbb{Q}$.

   (c) By analyzing the group $U(\mathbb{Z}_{17})$, show that $e^{2\pi i/17}$ is constructible by compass and straightedge. (Hence the 17-gon is constructible; the same is true for any prime number of the form $n = 2^m + 1$; if $2^m + 1$ is prime, m must be a power of 2.)

   (d) By analyzing the group $U(\mathbb{Z}_{18})$, prove that $e^{2\pi i/18}$ is not constructible by compass and straightedge. (Since $e^{2\pi i/6}$ is constructible, this shows that angles cannot be trisected.)

   (e) Using part (b), find the minimal polynomial of ω over $\mathbb{Q}$ for $n = 3, 4, 5$, and 6.

   (f) $m_\omega^{\mathbb{Q}}(x)$ is called the n^{th} *cyclotomic polynomial*, denoted Φ_n. Find the degree of Φ_n.

   (g) Let $\omega = e^{2\pi i/8}$. Identify explicitly all fields F such that $\mathbb{Q} \subseteq F \subseteq E$ with $|F:\mathbb{Q}| = 2$.

3. (a) Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of odd degree n, and not all roots of f are real. Show that the Galois group of f has order strictly greater than n. Here, the Galois group of a polynomial $f \in F[x]$ is, by definition, the Galois group of a splitting field of f over F. (Hint: Complex conjugation is an automorphism of $\mathbb{C}$; show that it must send a splitting field of f in $\mathbb{C}$ to itself.)

   (b) Identify the Galois group of a cubic polynomial in $\mathbb{Q}[x]$ that has only one real root.

(1) $x^4 - 4 = 0 \Rightarrow x^4 = 4$, $x^2 = \pm 2$, $x = \pm\sqrt{2}, \pm\sqrt{2}i$. Then $E = \mathbb{Q}[\sqrt{2}, \sqrt{2}i]$ is a splitting field for f. Since $i = (\sqrt{2})(\sqrt{2}i)$, $E = \mathbb{Q}[\sqrt{2}, i]$. Then $|E:\mathbb{Q}| = |E:\mathbb{Q}[\sqrt{2}]|\,|\mathbb{Q}[\sqrt{2}]:\mathbb{Q}| = \deg(m_i^{\mathbb{Q}[\sqrt{2}]})\deg(m_{\sqrt{2}}^{\mathbb{Q}}) = \deg(x^2+1)\deg(x^2-2) = 2\cdot 2 = 4$. Then $|\mathrm{Gal}(E,F)| = 4$. If $\varphi \in \mathrm{Gal}(E,F)$, then φ permutes the roots of x^2+1 and of x^2-2 in E, so $\varphi(i) = \pm i$ and $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Then φ has order 2. Thus $\mathrm{Gal}(E,F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(over)

(1) (cont'd.) Let $\alpha = \sqrt{2} + i$. Then $\alpha^2 = 1 + 2\sqrt{2}\,i$, so $\alpha^2 + b\alpha + c = (1 + c) + b\sqrt{2} + (b + 2\sqrt{2})\,i \neq 0$ for any $b, c \in \mathbb{Q}$. Thus $\deg(m_\alpha^{\mathbb{Q}}) > 2$. Then $|\mathbb{Q}[\alpha] : \mathbb{Q}| > 2$, and $|\mathbb{Q}[\alpha] : \mathbb{Q}|$ divides $|E : \mathbb{Q}| = 4$, so $|\mathbb{Q}[\alpha] : \mathbb{Q}| = 4$. Thus $E = \mathbb{Q}[\alpha]$.

(2) (a) The roots of $f(x) = x^n - 1$ in $\mathbb{C}$ are ω^k, $0 \leq k < n$, which all lie in $\mathbb{Q}[\omega]$. Then $\mathbb{Q}[\omega] = \mathbb{Q}[1, \omega, \omega^2, \dots, \omega^{n-1}]$ is a splitting field for $x^n - 1$. Since $\operatorname{char} \mathbb{Q} = 0$, f is separable, so $\mathbb{Q}[\omega]$ is Galois over $\mathbb{Q}$.

(b) If $(k, n) = 1$ then $ak + bn = 1$ for some $a, b \in \mathbb{Z}$. Then $\omega = (\omega^k)^a$ since $\omega^n = 1$. Then $\omega \in \mathbb{Q}[\omega^k]$, which implies $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^k]$. Let $G = \mathrm{Gal}(E, F)$. If $\varphi \in G$ then $\varphi(\omega) = \omega^k$ for some k, since φ permutes the roots of $x^n - 1$. Moreover, $\varphi(\omega)$ must generate E over $\mathbb{Q}$, which implies $(k, n) = 1$. Indeed, the set of roots of $f(x)$ form a cyclic group generated by ω, of order n, and φ restricts to an automorphism of this group. Since φ is determined by $\varphi(\omega)$, this gives an injective homom. $G \longrightarrow \mathrm{Aut}(\langle \omega \rangle) \cong \mathrm{Aut}(\mathbb{Z}_n) \cong U(\mathbb{Z}_n)$. To show this is an isomorphism, let $(k, n) = 1$. We show $\exists\, \varphi \in G$ with $\varphi(\omega) = \omega^k$. Consider $p(x) = \prod_{(k,n)=1} (x - \omega^k)$. Since $\mathrm{Gal}(E, \mathbb{Q})$ permutes the roots of p, as we have shown, the coefficients of p are fixed by $\mathrm{Gal}(E, \mathbb{Q})$. Since E is Galois over $\mathbb{Q}$, it follows that $p \in \mathbb{Q}[x]$. According to the "stipulation," p is irreducible over $\mathbb{Q}$. Then $\mathrm{Gal}(E, \mathbb{Q})$ acts transitively on the roots of p, hence for every $(k, n) = 1$, $\exists\, \varphi \in \mathrm{Gal}(E, \mathbb{Q})$ with $\varphi(\omega) = \omega^k$. Thus $\mathrm{Gal}(E, \mathbb{Q}) \cong U(\mathbb{Z}_n)$. $\square$

2(c) Since 17 is prime, $\mathbb{Z}_{17}$ is a (finite) field, so $U(\mathbb{Z}_{17})$ is cyclic of order 16, isomorphic to $\mathbb{Z}_{16}$. The series of (normal) subgroups of $\mathbb{Z}_{16}$ $\langle 0\rangle \trianglelefteq \langle 8\rangle \trianglelefteq \langle 4\rangle \trianglelefteq \langle 2\rangle \trianglelefteq \langle 1\rangle$ has the property that each successive quotient is cyclic of order 2. Let E be a splitting field for $x^{17}-1$ over $\mathbb{Q}$. Then $Gal(E,\mathbb{Q}) \cong U(\mathbb{Z}_{17}) \cong \mathbb{Z}_{16}$, and E is Galois/$\mathbb{Q}$, so by the Galois correspondence, there is a sequence of intermediate fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3 \subseteq F_4 = E$ with $|F_i : F_{i-1}| = 2$ for all $i > 0$. Then the elements of E, in particular $e^{2\pi i/17}$, are constructible. Then one can lay off 17 equidistant points on the unit circle, to construct a regular 17-gon, with compass and straight-edge.* (see footnote)

(d) $|U(\mathbb{Z}_{18})| = \varphi(18) = 6$. Since 6 is not a power of 2, and any field containing $e^{2\pi i/18}$ contains a splitting field for $x^{18}-1$, it follows that $e^{2\pi i/18}$ is not constructible.

(e) $m_\omega(x) = \prod_{(k,n)=1} (x-\omega^k)$: For $n=3$, $m_\omega(x) = (x-\omega)(x-\omega^2) = x^2 - (\omega+\omega^2)x + \omega\cdot\omega^2 = \boxed{x^2+x+1}$ since $\omega = e^{2\pi i/3}$. For $n=4$, $m_\omega(x) = (x-\omega)(x-\omega^3) = x^2 - (\omega+\omega^3)x + \omega\cdot\omega^3 = \boxed{x^2+1}$ since $\omega = e^{2\pi i/4} = i$. For $n=5$, $m_\omega = (x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4) = \frac{x^5-1}{x-1} = \boxed{x^4+x^3+x^2+x+1}$. For $n=6$, $m_\omega(x) = (x-\omega)(x-\omega^5) = x^2 - (\omega+\omega^5)x + \omega\omega^5 = x^2 - 2\cos\left(\frac{2\pi}{6}\right)x + 1 = x^2 - 2\left(\frac{1}{2}\right)x + 1 = \boxed{x^2-x+1}$ since $\omega = e^{2\pi i/6}$

(f) $\deg(\Phi_n) = |\mathbb{Q}[\omega] : \mathbb{Q}| = |U(\mathbb{Z}_n)| = \varphi(n)$, the Euler φ-function.

---

* The actual subfields can be found by chasing the isomorphisms $Gal(E,\mathbb{Q}) \cong U(\mathbb{Z}_{17}) \cong \mathbb{Z}_{16}$. $U(\mathbb{Z}_{17})$ is generated (multiplicatively) by 3, so, with $\varphi \in Gal(E,\mathbb{Q})$ satisfying $\varphi(\omega) = \omega^3$, we have $Gal(E,\mathbb{Q}) = \langle\varphi\rangle$ and the sequence of fields is $\mathbb{Q} = Fix(\langle\varphi\rangle) \subseteq Fix(\langle\varphi^2\rangle) \subseteq Fix(\langle\varphi^4\rangle) \subseteq Fix(\langle\varphi^8\rangle) \subseteq Fix(\langle\varphi^{16}\rangle) = E$. For example, $\varphi^2(\omega) = \omega^9$, and $Fix(\langle\varphi^2\rangle) = \mathbb{Q}[\alpha]$ with $\alpha = \sum_j (\varphi^2)^j(\omega) = \omega + \omega^2 + \omega^4 + \omega^8 + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16}$ (over)

(2)(f) $\mathrm{Gal}(E,\mathbb{Q}) \cong U(24)$ is the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$. The three subgroups of index 2 are generated by 3, 5, and 7. The corresponding elements of $\mathrm{Gal}(E,\mathbb{Q})$ carry ω to ω^3, ω^5, ω^7, respectively. Let $\varphi \in \mathrm{Gal}(E,\mathbb{Q})$ with $\varphi(\omega) = \omega^3$. Then $\varphi(\omega+\omega^3) = \omega+\omega^3$, and $\omega+\omega^3 = 2i\sin\left(\frac{\pi}{4}\right) = \sqrt{2}\,i \notin \mathbb{Q}$, so $\mathrm{Fix}(\langle\alpha\rangle) = \mathbb{Q}[\sqrt{2}\,i]$, with $m^{\mathbb{Q}}_{\sqrt{2}\,i}(x) = x^2+2$. Similarly, if $\beta \in \mathrm{Gal}(E,\mathbb{Q})$ with $\beta(\omega) = \omega^7$, then $\mathrm{Fix}(\langle\beta\rangle) = \mathbb{Q}[\omega+\omega^7] = \mathbb{Q}[\sqrt{2}]$ with $m^{\mathbb{Q}}_{\sqrt{2}}(x) = x^2-2$. If $\gamma \in \mathrm{Gal}(E,\mathbb{Q})$ with $\gamma(\omega) = \omega^5$, then $\gamma(\omega^2) = \omega^{10} = \omega^2$, so $\mathrm{Fix}(\langle\gamma\rangle) = \mathbb{Q}[\omega^2] = \mathbb{Q}[i]$, with $m^{\mathbb{Q}}_{i}(x) = x^2+1$. ($\omega+\omega^5$ is fixed by γ, but $\omega+\omega^5 = 0 \in \mathbb{Q}$.)

(3) (a) Let E be the splitting field of $f(x)$ over $\mathbb{Q}$, and let $\alpha \in E$ be a real root of f. Since f is irreducible, $|\mathbb{Q}[\alpha]:\mathbb{Q}| = n$, and since α is real, $\mathbb{Q}[\alpha] \subseteq \mathbb{R}$. Since f has some non-real root, $E \not\subseteq \mathbb{R}$, and thus $\mathbb{Q}[\alpha] \subsetneq E$. Then $|E:\mathbb{Q}| > |\mathbb{Q}[\alpha]:\mathbb{Q}| = n$. (The hint was superfluous — je suis désolé !).

(b) Since $\mathrm{Gal}(E,\mathbb{Q})$ acts faithfully on the roots of the cubic, $\mathrm{Gal}(E,\mathbb{Q}) \subseteq S_3$. Since $|\mathrm{Gal}(E,\mathbb{Q})| > 3$ by part (a), $\mathrm{Gal}(E,\mathbb{Q}) \cong S_3$.

---

footnote on 2(c), (cont'd.) This is a sum of conjugate pairs of 17^{th} roots of 1, equal to $2\cos\left(\frac{2\pi}{17}\right) + 2\cos\left(\frac{4\pi}{17}\right) + 2\cos\left(\frac{8\pi}{17}\right) + 2\cos\left(\frac{16\pi}{17}\right)$. It has degree two over $\mathbb{Q}$. Its minimal polynomial has one other root, equal to $\varphi(\alpha) = \omega^3+\omega^5+\omega^6+\omega^7+\omega^{10}+\omega^{11}+\omega^{12}+\omega^{14} = 2\cos\left(\frac{6\pi}{17}\right) + \cdots + 2\cos\left(\frac{14\pi}{17}\right)$. Then $m^{\mathbb{Q}}_{\alpha} = x^2 - bx + c$, $b = \alpha+\varphi(\alpha) = -1$ and $c = \alpha\varphi(\alpha) = -4$ (from Mathematica). Then α is a root of x^2+x-4, $\alpha = \frac{-1 \pm \sqrt{17}}{2}$, constructible!