Math 5591H **Solutions to Final exam**

You may use any fact proven in class, in the textbook, or in homework.

15% **1.** *Let θ be such that $\cos\theta = 5/7$; prove that the angle $\theta/5$ is not constructible with ruler and compass. (You may use the identity $\cos(5x) = 16\cos^5 x - 20\cos^3 x + 5\cos x$.)*

Solution. Let $\alpha = \cos(\theta/5)$; then $16\alpha^5 - 20\alpha^3 + 5\alpha = \cos\theta = 5/7$, so α is a root of $f = 7 \cdot 16x^5 - 7 \cdot 20x^3 + 7 \cdot 5x - 5$. f is irreducible in $\mathbb{Q}[x]$ by Eisenstein and Gauss, so α has degree 5 over $\mathbb{Q}$, is not an element of a 2-extension of $\mathbb{Q}$, and thus is not constructible.

15% **2.** *Let F be a finite field and let $f \in F[x]$ be a product of k irreducible polynomials of degrees $n_1, \dots, n_k$. Find $\mathrm{Gal}(f/F)$.*

Solution. For any n an extension K/F with $[K : F] = n$ is unique (up to isomorphism) and Galois with cyclic $\mathrm{Gal}(K/F)$. (It is a subgroup of the cyclic group $\mathrm{Gal}(K/\mathbb{F}_p)$ where $p = \mathrm{char}\, F$.) Any irreducible polynomial of degree d dividing n splits in K completely, and has no roots in K if $d \nmid n$. Hence, the splitting field of f is the extension of F of the minimal degree n divisible by n_i for all i, that is, of $n = \mathrm{l.c.m.}(n_1, \dots, n_k)$. Hence, $\mathrm{Gal}(K/F) \cong \mathbb{Z}_n$, $n = \mathrm{l.c.m.}(n_1, \dots, n_k)$.

20% **3.** *Let F be a field with $\mathrm{char}\, F \neq 2$, let $f \in F[x]$ be a separable polynomial, let $G = \mathrm{Gal}(f/F)$. Let $\widetilde{G} = \mathrm{Gal}(f(x^2)/F)$; prove that there is an exact sequence $1 \longrightarrow \mathbb{Z}_2^d \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$ (in other words, $\widetilde{G}$ has a normal subgroup N isomorphic to $\mathbb{Z}_2^d$ such that $\widetilde{G}/N \cong G$) for some $d \geq 0$.*

Solution. Since $\mathrm{char}\, F \neq 2$, $f(x^2)$ is also separable. Let $\alpha_1, \dots, \alpha_n$ be the roots of f, let $K = F(\alpha_1, \dots, \alpha_n)$ be the splitting field of f, and let E be the splitting field of $f(x^2)$. We have $\widetilde{G} = \mathrm{Gal}(E/F)$ and $G = \mathrm{Gal}(K/F)$; since K/F is normal, by Galois's theorem $G \cong \widetilde{G}/N$ where $N = \mathrm{Gal}(E/K)$. E/K is a composite of quadratic extensions, $E = K(\sqrt{\alpha_1}) \cdots K(\sqrt{\alpha_n})$ with $\alpha_i \in K$ for all i. For any i, $K(\sqrt{\alpha_i})$ has no nontrivial subextensions, so either $K(\sqrt{\alpha_i})) \subseteq \prod_{j \neq i} K(\sqrt{\alpha_j})$, in which case $K(\sqrt{\alpha_i})$ can be excluded from the list, or $K(\sqrt{\alpha_i}) \cap \prod_{j \neq i} K(\sqrt{\alpha_j}) = K$; hence, the composite $E = K(\sqrt{\alpha_{i_1}}) \cdots K(\sqrt{\alpha_{i_d}})$ is direct for some $i_1, \dots, i_d$, and $N = \prod_{j=1}^{d} \mathrm{Gal}(K(\sqrt{\alpha_{i_j}})/K) \cong \mathbb{Z}_2^d$.

20% **4.** *An irreducible quartic $f \in \mathbb{Q}[x]$ has two real and two non-real complex roots and its cubic resolvent has a single root in $\mathbb{Q}$. Prove that $\mathrm{Gal}(f/\mathbb{Q}) \cong D_8$.*

Solution. By the "classification of Galois groups of irreducible quartics", $\mathrm{Gal}(f/\mathbb{Q}) \cong D_8$ or $\mathbb{Z}_4$. The complex conjugation transposes two non-real roots and fixes the real roots of f, so acts as a transposition on the set of roots of f. The group $\mathbb{Z}_4$, as a subgroup os S_4, contains no transposition, so $\mathrm{Gal}(f/\mathbb{Q}) \cong D_8$.

40% **5.** *Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \in \mathbb{R}$ and let $K = \mathbb{Q}(\alpha)$. Take it for granted that $\alpha \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$.*

(a) *Prove that $\deg_{\mathbb{Q}}(\alpha^2) = 4$ and deduce that $\sqrt{2}, \sqrt{3} \in K$.*

Solution. $\alpha^2 = (2+\sqrt{2})(3+\sqrt{3}) = 6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a biquadratic extension of $\mathbb{Q}$, its only nontrivial subextensions are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$, and α^2 is not contained in any of them, so $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\deg_{\mathbb{Q}} \alpha = 4$.

(Alternatively, α^2 has 4 conjugates, $(2 \pm \sqrt{2})(3 \pm \sqrt{3})$.)

(b) *Find the degree and all the conjugates of α over $\mathbb{Q}$.*

Solution. Since $\alpha \notin \mathbb{Q}(\alpha^2)$, $\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha^2)$ is a quadratic extension, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)][\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2 \cdot 4 = 8$, so $\deg_{\mathbb{Q}} \alpha = 8$. The conjugates of α are $\pm\sqrt{\rho}$ where ρ runs over the set of conjugates of α^2, that is, these are $\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$.

(c) *Show that the extension $K/\mathbb{Q}$ is normal.*

Solution. Since $K = \mathbb{Q}(\alpha) \supseteq \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, we have $\sqrt{2}, \sqrt{3} \in K$. For $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$ we have $\alpha\beta = \sqrt{2}(3+\sqrt{3}) \in K$, so $\beta \in K$. For the other conjugates $\gamma = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$ and $\delta = \sqrt{(2-\sqrt{2})(3-\sqrt{3})}$ of α we also have $\alpha\gamma = (2+\sqrt{2})\sqrt{6} \in K$ and $\alpha\delta = \sqrt{2}\sqrt{6} \in K$, so $\pm\alpha, \pm\beta, \pm\gamma, \pm\delta \in K$. Hence, $K/\mathbb{Q}$ is normal.

(d) *Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Prove that there exists $\varphi \in G$ such that $\varphi(\sqrt{2}) = -\sqrt{2}$ and $\varphi(\sqrt{3}) = \sqrt{3}$. Prove that $|\varphi| = 4$.*

Solution. The automorphism $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$ of $\mathbb{Q}(\alpha^2)$ extends to $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$. For this φ we have $\varphi(\alpha^2) = \sqrt{(2-\sqrt{2})(3+\sqrt{3})} = \beta^2$, so $\varphi(\alpha) = \pm\beta$. W.l.o.g. assume that $\varphi(\alpha) = \beta$, then since $\varphi(\alpha\beta) = \varphi(\sqrt{2}(3+\sqrt{3})) = -\sqrt{2}(3+\sqrt{3}) = -\alpha\beta$, we obtain that $\varphi^2(\alpha) = \varphi(\beta) = -\alpha\beta/\varphi(\alpha) = -\alpha$, $\varphi^3(\alpha) = -\beta$, and $\varphi^4(\alpha) = \alpha$, so $|\varphi| = 4$.

(e) *Find two more automorphisms of K of order 4 and deduce that $G \cong Q_8$ (the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$).*

Solution. These are $\psi(\alpha) = \gamma$ and $\eta(\alpha) = \delta$. Hence, G has (at least) 3 cyclic subgroups of order 4: $\langle\varphi\rangle$, $\langle\psi\rangle$, and $\langle\eta\rangle$.

The only groups of order 8 are (up to isomorphism) Q_8, D_8, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2^3$. The groups D_8 and $\mathbb{Z}_8$ have only one cyclic subgroup of order 4, $\mathbb{Z}_4 \times \mathbb{Z}_2$ has two such subgroups, and $\mathbb{Z}_2^3$ has no such subgroups. Hence, $G \cong Q_8$.

(f) *Draw the lattice (the diagram) of all the subfields of K.*

Solution. The lattice of subgroups of Q_8 and the corresponding lattice of subextensions of $K/\mathbb{Q}$ are

$$\begin{tikzcd}
& 1 \arrow[d, dash, "2"'] & \\
& \langle -1\rangle \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle i\rangle \arrow[dr, dash, "2"'] & \langle j\rangle \arrow[d, dash, "2"] & \langle k\rangle \arrow[dl, dash, "2"] \\
& Q_8 &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
& K \arrow[d, dash, "2"'] & \\
& \mathbb{Q}(\alpha^2) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash, "2"] \\
& \mathbb{Q}. &
\end{tikzcd}$$

where $-1 = \varphi^2 = \psi^2 = \eta^2$, $i = \psi$, $j = \varphi$, and $k = \eta$: $-1(\alpha) = -\alpha$, $i(\alpha) = \gamma = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$, $j(\alpha) = \beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$, $k(\alpha) = \delta = \sqrt{(2-\sqrt{2})(3-\sqrt{3})}$.

Good luck! and have a nice vacation