Math 100C Final 136 points June 12, 2015

Directions and Notation: Carefully justify all answers. The field of rationals is denoted by $\mathbf{Q}$. The field of q elements is denoted by $\mathbf{F}_q$. A primitive complex n-th root of unity is denoted by ζ_n. Given a complex number β, its complex conjugate is denoted by $\overline{\beta}$. Problems 1-6 are worth 24,16,16,24,40,16 points, respectively.

(1) For each Galois group below, give its size and also list every automorphism in that group. Be explicit.

(A) $\mathrm{Gal}(\mathbf{Q}(\zeta_{28})/\mathbf{Q})$ **(B)** $\mathrm{Gal}(\mathbf{Q}(\zeta_7+\zeta_7^2+\zeta_7^4)/\mathbf{Q})$ **(C)** $\mathrm{Gal}(\mathbf{F}_{125}/\mathbf{F}_5)$

SOLUTION: These groups have sizes 12, 2, and 3, respectively. The 12 autos for (A) are defined by mapping ζ_{28} to ζ_{28}^m, where $m = 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27$. The two autos for (B) are defined by mapping $\zeta_7+\zeta_7^2+\zeta_7^4$ to $\zeta_7^n+\zeta_7^{2n}+\zeta_7^{4n}$, where $n = 1, 3$. The three autos for (C) are the k-th power maps, where $k = 1, 5, 25$. (The map for $k = 5$ is called the Frobenius automorphism.)

(2) Let $\alpha \in \mathbf{F}_{25}$ be a root of the irreducible polynomial $x^2 - 2x - 2$ over $\mathbf{F}_5$. (Recall that $\mathbf{F}_5 = \{0, 1, 2, 3, 4\}$ mod 5.)

(A) Find the smallest positive integer k for which $\alpha^k = 1$.

(B) Find numbers a and b in $\mathbf{F}_5$ for which $x^2 + ax + b$ is the minimal polynomial of α^7 over $\mathbf{F}_5$.

SOLUTION: Since $\alpha^2 = 2\alpha + 2$, the values of α^m for $m =$3, 4, 5, 6, 7, 8, 9, 10, 11, 12 are respectively $\alpha - 1$, $\alpha + 2$, $2 - \alpha$, 3, 3α, $\alpha + 1$, $2 - 2\alpha$, $1 - 2\alpha$, $2\alpha + 1$, -1.
(A) Since $\alpha^{24} = 1$, the order of α divides 24. The calculations above then show that the order of α is exactly 24.
(B) The min poly of α^7 is $(x - \alpha^7)(x - \alpha^{11})$, which equals $x^2 - x + 2$. This can also be proved by using the fact that α^7 equals 3α.

(3) Let F be the splitting field of an irreducible polynomial $f(x)$ over $\mathbf{Q}$. Let $u \in F$ be a root of $f(x)$. Explain why every root of $f(x)$ in F must have the form $\sigma(u)$ for some automorphism $\sigma \in \mathrm{Gal}(F/\mathbf{Q})$.

SOLUTION: Let v be any root of $f(x)$ in F, i.e., v is a conjugate of u

over $\mathbf{Q}$. There is a $\mathbf{Q}$-isomorphism τ which maps $\mathbf{Q}(u)$ onto $\mathbf{Q}(v)$, such that $\tau(u) = v$. This isomorphism can be extended to a $\mathbf{Q}$-automorphism σ of F, as described on page 369. Thus $\sigma(u) = \tau(u) = v$.

(4) Let $\alpha = \zeta_7^3 + \zeta_7^5 + \zeta_7^6$. Let $\beta = 2^{1/3}\zeta_3$.
(A) Prove that $\overline{\beta} \notin \mathbf{Q}(\beta)$.
(B) Prove that for any $v \in \mathbf{Q}(\alpha)$, we have $\overline{v} \in \mathbf{Q}(\alpha)$. *Hint*: FTGT
(C) Find u and v for which the minimal polynomial of ζ_7 over $\mathbf{Q}(\alpha)$ is $x^3 + ux^2 + vx - 1$. Express u and v in terms of α.

SOLUTION:
(A) Let $K = \mathbf{Q}(\beta)$. Note that β is a root of the irreducible polynomial $x^3 - 2$ over $\mathbf{Q}$. If $\overline{\beta}$ were in K, then $\overline{\beta}/\beta = \zeta_3$ would be in K, so K would be the field $\mathbf{Q}(2^{1/3}, \zeta_3)$, which has dimension 6 over $\mathbf{Q}$. This contradicts the fact that K has dimension 3 over $\mathbf{Q}$.
(B) $\mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q}(\alpha))$ is a normal subgroup of the big group $\mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q})$ because the big group is abelian. Thus by the FTGT, $\mathbf{Q}(\alpha)$ is normal over $\mathbf{Q}$, so for $v \in \mathbf{Q}(\alpha)$, any conjugate of v over $\mathbf{Q}$ is also in $\mathbf{Q}(\alpha)$. Since $\overline{v}$ is a conjugate of v over $\mathbf{Q}$, the result is proved.
(C) The desired minimal polynomial is $(x-\zeta_7)(x-\zeta_7^2)(x-\zeta_7^4)$, since the auto that sends ζ_7 to ζ_7^m fixes α when $m = 2$ or 4. Thus $u = -(\zeta_7+\zeta_7^2+\zeta_7^4) = 1+\alpha$ and $v = \alpha$.

(5) Let F be the splitting field of $f(x) = x^4 - 12x^2 - 24x - 12$ over $\mathbf{Q}$.
(A) Explain why $f(x)$ is irreducible over $\mathbf{Q}$.
(B) One root of $f(x)$ in F is $c + \sqrt{3 + 2c}$, where $c = \sqrt{3}$. List the 3 other roots of $f(x)$ in F.
(C) Show that $F = \mathbf{Q}(i, \sqrt{3 + 2c})$.
(D) Give two automorphisms which together generate $\mathrm{Gal}(F/\mathbf{Q})$.
(E) True or false: $\mathrm{Gal}(F/\mathbf{Q})$ is isomorphic to the dihedral group D_4.

SOLUTION:
(A) $f(x)$ is 3-Eisensteinian.
(B) The four roots are $c \pm \sqrt{3 + 2c}$, $-c \pm \sqrt{3 - 2c}$.
(C) This follows because $\sqrt{3 - 2c} = i\{c/\sqrt{3 + 2c}\}$.
(D) One of the two autos is complex conjugation τ, the other is the auto σ that fixes i and maps $\sqrt{3 + 2c}$ to $\sqrt{3 - 2c}$.

(E) True, because τ has order 2, σ has order 4, and $\tau\sigma\tau = \sigma^{-1}$, i.e., $\tau\sigma\tau\sigma$ is the identity automorphism.

(6) Let $f(x)$ be an irreducible polynomial of degree 5 over $\mathbf{Q}$ with exactly two nonreal complex roots. Explain briefly why $f(x)$ is not solvable by radicals.

SOLUTION: The Galois group of $f(x)$ is (iso to) a subgroup of S_5 which contains a 5-cycle (since 5 divides the order of the Galois group) and a 2-cycle (since complex conjugation corresponds to a 2-cycle when there are exactly two nonreal roots). Thus the Galois group is S_5, which is not a solvable group. Therefore $f(x)$ is not solvable by radicals.