Math 100C **Test 2** **100 points** **May 22, 2015**

Notation: The field of rationals is denoted by Q, and Z_2 denotes a cyclic group of order 2.

(1) Prove that a subgroup of a solvable group is solvable. (10pts)

SOLUTION: First two lines of page 353.

(2) For a positive integer n, let ζ_n be a complex primitive n-th root of unity, and let F denote the field $Q(\zeta_n)$.
(A) Prove in detail that $\mathrm{Gal}(F/Q)$ is an abelian group. (20pts)

SOLUTION: Prop 8.4.2 on page 387.

(B) Let $\alpha = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9$. Prove that α has degree 4 over Q. (10pts)
Hint: For $n = 13$, which of the 12 automorphisms in $\mathrm{Gal}(F/Q)$ fix α?

SOLUTION: Let $E = Q(\alpha)$. The automorphism σ_k that sends ζ_{13} to ζ_{13}^k fixes α if and only if $k \in \{1, 3, 9\}$. Thus $|\mathrm{Gal}(F/E)| = 3$, so $|F : E| = 3$. Since $|F : Q| = 12$, we have $|E : Q| = 4$, so α has degree 4 over Q.
Note: The reason α is not fixed by σ_2, for example, is that $\alpha - \sigma_2(\alpha)$ can't be zero, otherwise ζ_{13} would satisfy a minimal polynomial other than

$$1 + x + x^2 + \cdots x^{12}.$$

Extra credit for anyone who provided the level of detail in this note.

(C) Let α be as in part (B). Prove that if $u \in Q(\alpha)$, then every conjugate of u is also in $Q(\alpha)$. (10pts)

SOLUTION: $\mathrm{Gal}(F/E)$ is a normal subgroup of $\mathrm{Gal}(F/Q)$, since $\mathrm{Gal}(F/Q)$ is abelian by part (A). Thus E is normal over Q by the FTGT.

(3) Let G be the Galois group over Q of an irreducible polynomial of degree n (with rational coefficients). We can view G as a group of permutations of the roots. Prove that if n is prime, then G contains a permutation which is an n-cycle. Be sure to say where you used the primality of n. (10pts)

SOLUTION: Let F be the splitting field of the irreducible polynomial $f(x) \in Q[x]$, where $f(x)$ has degree n. Then G is the Galois group of F over Q. Let u be a root of $f(x)$. Since $Q(u)$ is contained in F and $|Q(u) : Q| = n$, we see that n divides $|F : Q|$. Thus n divides $|G|$. Since n is prime, G has an element of order n by Cauchy's Theorem. Moreover, G is contained in S_n and the only elements of order n in S_n are n-cycles, since n is prime.

(4) Show that the Galois group of $x^4 - 10x^2 + 20$ over Q is isomorphic to the group Z_4. (20pts)
Hint: The four roots of this polynomial are $\pm\sqrt{5 \pm a}$, where $a = \sqrt{5}$.

SOLUTION: Everyone will get full credit on this problem because it was originally stated incorrectly. The splitting field is $Q(\sqrt{5+a})$ which is easily seen to have degree 4 over Q; this is because $\sqrt{5-a} \in Q(\sqrt{5+a})$ since $\sqrt{5-a} = 2a/\sqrt{5+a}$. (Extra credit for anyone that noticed this last equality.) A generator of the Galois group maps $\sqrt{5+a}$ to $\sqrt{5-a}$. This generator has order 4.

(5) Let G be the Galois group of the polynomial $x^7 - 3$ over Q. Prove that $|G| = 42$, and then give two explicit automorphisms α and β in G which together generate the entire group G. (20pts)

SOLUTION: Let $u = 3^{1/7}$, $w = \zeta_7$. Then G is the Galois group of F over Q, where $F = Q(u, w)$. We know $|F : Q| \leq 7 * 6 = 42$ but since $|F : Q|$ is divisible by both 7 and 6, it follows that $|F : Q| = 7 * 6 = 42$. Thus $|G| = 42$. The group G is generated by α, which maps u to uw while fixing w, and by β, which maps w to w^3 while fixing u. Note that α has order 7 and β has order 6.