M 622 HW, due Monday, April 21

1. Let p and q be prime numbers, and let $t(x) = x^p - q$.

   (a) Explain why $t(x)$ is irreducible over $\mathbb{Q}$. **ANSWER.** It's Eisenstein at the prime q.

   (b) Describe the roots of $t(x)$ (they are contained in $\mathbb{C}$): **They are..** $\{q^{1/p}\psi^m : m = 0, 1, \ldots, p-1\}$, where $\psi = e^{2\pi i/p}$. Note that if $p = 2$, $\psi = -1$.

   (c) Describe the splitting K of $t(x)$, and determine $[K : \mathbb{Q}]$.

   Description of K. Any extension field B that contains all the above roots, and is closed under multiplication and inverse, contains ψ. But now any extension B of $\mathbb{Q}$ that contains $q^{1/p}$ and ψ contains all roots of $t(x)$. Thus the least extension of $\mathbb{Q}$ containing all the roots of $t(x)$ is equal to $\mathbb{Q}(q^{1/p}, \psi)$.

   Dimension of K over $\mathbb{Q}$: Since $q^{1/p}$ is a root of the degree-p irreducible $t(x)$, $[\mathbb{Q}(q^{1/p}) : \mathbb{Q}] = p$. Since ψ is a primitive p-th root of unity, as we have proven, ψ is a root of $\Phi_p(x) = x^{p-1} + x^{p-2} + x^2 + x + 1$, a $\mathbb{Q}$-irreducible, and $[\mathbb{Q}(\psi) : \mathbb{Q}] = p - 1$. Of course $\mathbb{Q}(\psi)$ is the splitting field of $\Phi_p(x)$.
   Since $K = \mathbb{Q}(q^{1/p})(\psi)$, $[K : \mathbb{Q}] = [\mathbb{Q}(q^{1/p})(\psi) : \mathbb{Q}(\psi)][\mathbb{Q}(\psi) : \mathbb{Q}]$. Since ψ is a root of a degree p-1 polynomial over $\mathbb{Q}$, $p-1 \geq [\mathbb{Q}(q^{1/p})(\psi) : \mathbb{Q}(\psi)]$, so $(p-1)p \geq [K : \mathbb{Q}]$. But both $p - 1$ and p divide $[K : \mathbb{Q}]$, so $[K : \mathbb{Q}] = p(p-1)$. Note that if $p = 2$, $[K : \mathbb{Q}] = 2$ (and $K = \mathbb{Q}(\sqrt{q})$).

   (d) Let $G = Gal(K/\mathbb{Q})$. Use the appropriate part of the Sylow Theorem to explain why G has just one Sylow-p subgroup, which we'll call N. Use another part of the Sylow Theorem to explain why N is normal.

   If p=2 G is the 2-element group, $2 = p$, and the statement above is obviously true. Suppose $p > 2$. Since $K/\mathbb{Q}$ is Galois, $|G| = [K : \mathbb{Q}] = p(p-1)$. By the Sylow Theorem, $n_p = 1 + ps$, some non-negative integer s, and $n_p | p - 1$—these imply $n_p = 1$. Thus, there is a unique Sylow-p subgroup N, a subgroup that must be normal—any conjugate hNh^{-1} has $|N|$ elements, so $hNh^{-1} = N$.

   (e) By the Fundamental Theorem of Galois Theory (FTGT), the fixed field J of N is a splitting field of some polynomial $a(x) \in \mathbb{Q}[x]$. Since $|N| = p$, use FTGT (be explicit about which part) to determine $[J : \mathbb{Q}]$, and then determine J explicitly and $a(x)$ explicitly.

   By FTGT, there is an order-reversing bijection ι from intermediate fields to subgroups of G, where $\iota(J) = Aut(K/J)$. Let $J = \iota^{-1}(N)$, the intermediate field associated with N. Another part of FTGT states that if H is a normal subgroup of G if and only if $\iota^{-1}(H)$ is Galois over the base field $\mathbb{Q}$ (in this case). FTGT also states that the map ι "preserves indices": if A is contained in B, and both A

and B are intermediate subfields, then $[B : A] = [\iota(A) : \iota(B)]$. In this case, $[G : N] = p(p-1)/p = p-1$. Thus, $[J : \mathbb{Q}] = p-1$. The preservation of indices aspect of FTGT guarantees that there is a unique intermediate subfield of dimension $p-1$ over $\mathbb{Q}$, that unique field being J. As mentioned, $[\mathbb{Q}(\psi) : \mathbb{Q}] = p-1$. Thus, $J = \mathbb{Q}(\psi)$. Also mentioned: J is the splitting field of $\Phi_p(x)$.

(f) Use FTGT to explain why G can't be Abelian. (Here I erred. If p=2, G is the 2-element Abelian group.) Assume $p > 2$. Since $Aut(\mathbb{Q}(q^{1/p})/\mathbb{Q})$ carries roots of $t(x)$ to the same, $\mathbb{Q}(q^{1/p})$ contains only root of $t(x)$, and $\sigma \in Aut(\mathbb{Q}(q^{1/p})/\mathbb{Q})$ is determined completely by $\sigma(q^{1/p})$, it follows that $Aut(\mathbb{Q}(q^{1/p})/\mathbb{Q})$ has one element, which means that $\mathbb{Q}(q^{1/p})$ is not Galois over $\mathbb{Q}$.

Every subgroup of an Abelian group H is normal in H. But by FTGT, $\iota(\mathbb{Q}(q^{1/p}))$ is not normal in G. So G must not be Abelian.

(g) Is G solvable? Explain—there are several ways to do so.

Yes... K is formed by a series (of two) of radical extensions: $\mathbb{Q} \subset \mathbb{Q}(q^{1/p}) \subset \mathbb{Q}(q^{1/p})(\psi)$. Since this is the case, by the theorem of Galois, $Aut(K/\mathbb{Q}) = Gal(K/\mathbb{Q})$ is solvable.

Another way: Consider $\{e\} \leq N \leq G$. Since $|N| = p$, it is cyclic. By FTGT, $Aut(J/\mathbb{Q})$ is isomorphic to $Aut(K/\mathbb{Q})/Aut(K/J) = G/N$. But $Aut(J/\mathbb{Q})$ is isomorphic to U_5, the multiplicative group of units of that Z_5, a cyclic group. (Note: given $n \in \mathbb{N}$, it is not always true that $U_n \cong \mathbb{Q}(\psi_n)$ is cyclic, where ψ_n is a primitive n-th root of unity...on the other hand, if n is prime, then it is true that U_p is cyclic.) So $N/\{e\}, G/N$ are both cyclic, which implies that G is solvable.

2. Suppose F is a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{R}$, $t(x) \in F[x]$, and S is the splitting field of $t(x) \in F[x]$. Show that if $[S : F]$ is odd, then $S \subset \mathbb{R}$.

   Since $t(x)i$ has coeffiencients in $\mathbb{R}$, its roots are closed under complex conjugation. Let $c : \mathbb{C} \to \mathbb{C}$ be the complex conjugation map–we showed $c \in Aut(\mathbb{C}/\mathbb{R})$; of course $|c| = 2$ there. Since $c(S) \subset S$, the restriction of c to S is an automorphism in $Aut(S/F)$, and $c|_S$, has order one or two. Since S is Galois, $|G| = [S : F]$. By Lagrange, if its order is 2, $|G|$ is even. Since $|G|$ is odd, the order of $c|_S$ is odd, so it's 1, and all roots of $t(x)$ are real. Since S is generated by F and the roots of $t(x)$, S is contained in $\mathbb{R}$.

3. An old exercise from M622 states that if p is a prime number, then if α is a transposition of S_p and β is a p-cycle of S_p, then $S_p =< \alpha, \beta >$. Prove that if $p(x) \in \mathbb{Q}[x]$ is a degree 5 irreducible polynomial having exactly two non-real roots, then the Galois group of $p(x)$ is S_5.

   Let S be the splitting field of $p(x)$. Since S/Q is Galois, $[S : Q] = |G|$, where $G = Aut(S/Q)$. Moreover, G acts on the roots of $t(x)$, and that the field S is generated by $\mathbb{Q}$ and the roots of $t(x)$, implies that S acts faithfully on those roots. Thus, G can be embedded in S_5 via that action. Identify the five roots of $p(x)$ with $1, 2, 3, 4, 5$. Now we can view G as a subgroup of G, each element of $\sigma \in G$ permuting $\{1, 2, 3, 4, 5\}$, in the way σ permutes the roots of $t(x)$.

That $p(x)$ is irreducible of degree 5 means that if $\gamma \in S$ is a root of $p(x)$, $5 = [\mathbb{Q}(\gamma) : \mathbb{Q}]$. By the Double Extension Lemma, $5|[S : Q] = |G|$. By Cauchy's Theorem, there exists an element $\alpha \in G$ such that $|\alpha| = 5$. The only elements of S_5 of order 5 are its 5-cycles. So G contains a 5-cycle, say β.

Since $p(x) \in \mathbb{R}[x]$, its roots come in conjugate pairs, the restriction of c (complex conjugation) to S is in G. The two non-real roots of $p(x)$ must be exchanged by c, while the other roots of $p(x)$ (being real) are fixed by c. Thus the restriction of c to S is a transposition, say α. Since 5 is prime, $S_5 =< \alpha, \beta >$, and G must be S_5.

(Not a part of the exercise, but worth commenting on: S_5 is a not solvable group. In fact it's only non-trivial proper normal subgroup is A_5, the latter a non-Abelian simple group. So any composition series for S_5 contains A_5— in fact, $\{e\} \leq A_5 \leq S_5$ is the only composition series for S_5. But $A_5/\{e\}$ is not cyclic (not even Abelian); hence, S_5 is not solvable. As we proved in class, if the Galois group of a polynomial $t(x) \in \mathbb{Q}[x]$ is not solvable, then the roots of $t(x)$can't all be "extracted" using roots and basic algebraic operations, including inverse. So the roots of a polynomial $p(x)$ satisfying the above hypotheses can't all be extracted using roots and basic operations.)