GALOIS THEORY: SOLUTIONS TO HOMEWORK 14

1. (a) Show that $f = t^3 - 3t + 1$ is irreducible over $\mathbb{Q}$.
Solution: Reduce modulo 2 to get $t^3 + t + 1$, which is irreducible over $\mathbb{F}_2$ since neither 0 nor 1 is a root. Thus f is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$ by Gauss' Lemma.

(b) Show that whenever α is a root of f in a splitting field extension of $\mathbb{Q}$, then $\beta = \alpha^2 - 2$ is also a root of f.
Solution: We have $\beta^2 = \alpha^4 - 4\alpha^2 + 4 = -\alpha^2 - \alpha + 4$ and

$$\beta^3 = -\alpha^4 - \alpha^3 + 6\alpha^2 + 2\alpha - 8 = 3\alpha^2 - 7,$$

so $\beta^3 - 3\beta + 1 = (3\alpha^2 - 7) - 3(\alpha^2 - 2) + 1 = 0$.

(c) Let L be a splitting field for f over $\mathbb{Q}$. Use your answer to part (b) to show that $[L : \mathbb{Q}] = 3$, and conclude that the Galois group of f is isomorphic to $A_3 \cong C_3$.
Solution: Let α be a root of f in L. By part (b), we have that $\beta = \alpha^2-2$ is a root of f. Note also that $(\alpha^2 - 2) - \alpha \neq 0$ since the minimal polynomial of α is f, and thus $\beta \neq \alpha$. Therefore, the polynomial f has at least two roots in $\mathbb{Q}(\alpha) \subseteq L$. If f were to split as $(t-\alpha)(t-\beta)(t-\delta)$ in L, then by equating coefficients with t^3-3t+1 we see that one would have $\alpha + \beta + \delta = 0$, whence $\mathbb{Q}(\alpha)$ contains δ as well. Thus f splits over $\mathbb{Q}(\alpha)$, so we must have $L = \mathbb{Q}(\alpha)$ and $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since L is a splitting field for f and $\mathbb{Q}$ has characteristic 0, the field extension $L : \mathbb{Q}$ is Galois and the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ has order $[L : \mathbb{Q}] = 3$. Finally, note that there is a unique group (up to isomorphism) of order 3, isomorphic to $C_3 \cong A_3$.

(d) Show that there is no $\gamma \in L$ such that $\gamma \notin \mathbb{Q}$ and $\gamma^3 \in \mathbb{Q}$, and conclude that $L : \mathbb{Q}$ is not a radical extension.
Solution: Suppose that $\gamma \in L \setminus \mathbb{Q}$ and that γ is a root of $t^3 - \lambda$ for some $\lambda \in \mathbb{Q}$. By the Tower Law we have $3 = [L : \mathbb{Q}] = [L : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}]$. Since 3 is prime and $\gamma \notin \mathbb{Q}$, we must have $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$, from which it follows that $t^3 - \lambda$ is irreducible over $\mathbb{Q}$. Since $L : \mathbb{Q}$ is a normal extension containing a root of $t^3 - \lambda$, that polynomial must split over L, so L contains another root, say γ'. Now let $\omega = \gamma'/\gamma \in L$. Then one may check that ω is a root of $t^3 - 1$ different from 1, so it is a root of $t^2 + t + 1$. Since the latter polynomial is irreducible over $\mathbb{Q}$, it must be the minimal polynomial of ω. But then the Tower Law implies that $[L : \mathbb{Q}] = 3$ is divisible by $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, which is false. Thus no such γ can exist.

(e) By Cardano's formula, the equation $f = 0$ is soluble by radicals. How do you reconcile this observation with your answer to part (d)?
Solution: This does not contradict the fact that $f = 0$ is soluble by radicals, since for that to occur it is sufficient (and also necessary) for

the splitting field L to be *contained* in a radical extension. In the present example, $L = \mathbb{Q}(\alpha)$ is contained in $\mathbb{Q}(\alpha, \omega)$, where ω is a root of t^2+t+1, and $\mathbb{Q}(\alpha, \omega) : \mathbb{Q}$ is a radical extension. In fact, Cardano's formula shows that α may be expressed in terms of cube roots of elements of $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$.

2. Is the polynomial $t^5 - 4t^4 + 2$ soluble by radicals over $\mathbb{Q}$?
Solution: No. The polynomial $f(t) = t^5 - 4t^4 + 2$ is irreducible over $\mathbb{Q}$, as a consequence of Eisenstein's theorem using the prime 2. Let $L : \mathbb{Q}$ be a splitting field extension for f, and let $\alpha \in L$ be a root of f. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 5$, and from the tower law we find that 5 divides $[L : \mathbb{Q}]$. Thus $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ is a subgroup of S_5 of order $|G| = [L : \mathbb{Q}]$ divisible by 5. In particular, since 5 is a prime number, we perceive that G has an element of order 5. Observe next that $f'(x) = x^3(5x - 16)$, so that $f'(x) = 0$ for precisely 2 real values of x, and so since

$$f(-1) = -3, \quad f(0) = 2, \quad f(1) = -1, \quad f(4) = 2,$$

then f has 3 real roots and 2 complex roots. Hence $\mathrm{Gal}_{\mathbb{Q}}(f)$ contains a transposition fixing the real roots and interchanging the 2 complex roots by conjugation. Then since $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of S_5, and contains an element of order 5 and a transposition, it follows that in fact $\mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to the whole of S_5 (the group of permutations on 5 symbols). But S_5 contains the insoluble subgroup A_5, and hence is itself insoluble. We therefore conclude that $\mathrm{Gal}_{\mathbb{Q}}(f)$ is insoluble, and hence that $f(t) = 0$ cannot be solved by using radical extensions of $\mathbb{Q}$.

3. Is the polynomial $t^6 - 4t^2 + 2$ soluble by radicals over $\mathbb{Q}$?
Solution: Yes. The polynomial $g(x) = x^3 - 4x + 2$ is soluble by radicals since it is cubic (this is due to Cardano). Since $f(t) = t^6 - 4t^2 + 2 = g(t^2)$, it follows that if α is any root of f lying in a splitting field extension, then $g(\alpha^2) = 0$, so that $a = \alpha^2$ lies in a radical extension L of $\mathbb{Q}$. But $\alpha = \pm\sqrt{a}$, and hence α lies in $L(\sqrt{a})$, which is a radical extension of L, and hence also a radical extension of $\mathbb{Q}$. Thus $t^6 - 4t^2 + 2$ is indeed soluble by radicals over $\mathbb{Q}$.

4. Let n be a positive integer and K a field with characteristic not dividing n. Let $L = K(\zeta)$, where ζ is a primitive nth root of unity.
   (a) Show that $\mathrm{Gal}(L : K)$ is isomorphic to a subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.
   Solution: The group of all nth roots of unity in L is easily seen to be generated by the primitive root ζ. From this it follows that L is a splitting field for $t^n - 1$ over K. Since the characteristic of K does not divide n, the polynomial $t^n - 1$ is relatively prime to its derivative nt^{n-1}, so $t^n - 1$ is a separable polynomial. Therefore $L : K$ is normal and separable, and hence is a Galois extension.
   Next, let $\sigma \in \mathrm{Gal}(L : K)$. Applying σ to the equation $\zeta^n = 1$, we have $\sigma(\zeta)^n = 1$, and thus $\sigma(\zeta)$ is also an nth root of unity. Thus, we find

that $\sigma(\zeta) = \zeta^{e(\sigma)}$ for some integer $e(\sigma)$. Let $\sigma' \in \mathrm{Gal}(L : K)$. Then

$$(\sigma' \circ \sigma)(\zeta) = \sigma'(\sigma(\zeta)) = \sigma'(\zeta^{e(\sigma)}) = \sigma'(\zeta)^{e(\sigma)} = (\zeta^{e(\sigma')})^{e(\sigma)} = \zeta^{e(\sigma')e(\sigma)}.$$

On the other hand, reversing the roles of σ and σ' and using the commutativity of integer multiplication (so that $e(\sigma')e(\sigma) = e(\sigma)e(\sigma')$), we arrive at the same expression. That is to say that σ and σ' commute, so $\mathrm{Gal}(L : K)$ is abelian.

We now take $\sigma' = \sigma^{-1}$ in the above to obtain $\zeta = \zeta^{e(\sigma^{-1})e(\sigma)}$. Since ζ is a primitive nth root of unity, it follows that $e(\sigma^{-1})e(\sigma) - 1$ is divisible by n, and thus $e(\sigma^{-1})e(\sigma) \equiv 1 \pmod n$. In particular, $e(\sigma)$ is invertible modulo n. Thus the reduction of $e(\sigma)$ modulo n defines a map $\varphi : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$. Again since ζ is a primitive root, it follows from the above equation that $e(\sigma'\sigma) \equiv e(\sigma')e(\sigma) \pmod n$, whence φ is a homomorphism.

Finally, note that since $L = K(\zeta)$, any $\sigma \in \mathrm{Gal}(L/K)$ is determined by its action on ζ. Thus, if $e(\sigma) \equiv e(\sigma') \pmod n$ then $\sigma(\zeta) = \sigma'(\zeta)$, so that $\sigma = \sigma'$. Therefore, φ is injective, and $\mathrm{Gal}(L/K)$ is isomorphic to its image in $(\mathbb{Z}/n\mathbb{Z})^\times$ under φ.

(b) Show that if n is prime and $K = \mathbb{Q}$ then either $L = K$ or $\mathrm{Gal}(L : K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution: If K already contains a primitive nth root of unity then we have $L = K$ and there is nothing to prove. Otherwise ζ is a root of $t^n - 1$ that does not lie in K; in particular, $\zeta \neq 1$, so it is a root of $\frac{t^n-1}{t-1} = t^{n-1} + \ldots + 1$. We know already that this polynomial is irreducible when n is prime, and thus it is the minimal polynomial of ζ. Therefore $[L : \mathbb{Q}] = n - 1$, so $\mathrm{Gal}(L : \mathbb{Q})$ has order $n - 1$, and thus is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Note: There was a question in class about what happens in general, when K is not necessarily equal to $\mathbb{Q}$ – can $\mathrm{Gal}(L : \mathbb{Q})$ be a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$? The answer is yes, one can have that this is a proper subgroup. The reason for this is that K may already contain d-th roots of unity for certain divisors d of n. For example, if $p \equiv 1 \pmod 3$, then $\mathbb{F}_p$ contains primitive cube-roots of unity. Then, when $K = \mathbb{F}_p$, a situation wherein $\mathrm{char}(K) = p$, one has $(p, 3) = 1$ and yet when ζ is a primitive cube root of unity we have $L = K(\zeta) = K$ and $\mathrm{Gal}(L : \mathbb{Q})$ is trivial.

5. Let n be a positive integer. By Dirichlet's theorem, there exists a prime number p with $p \equiv 1 \pmod n$.

(a) Let $L = \mathbb{Q}(e^{2\pi i/p})$. Show that $\mathrm{Gal}(L : \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Solution: The desired conclusion here is immediate from part (b) of question 4, since $e^{2\pi i/p}$ is a primitive p-th root of unity.

(b) Show that $\mathbb{Q}(e^{2\pi i/p})$ contains a subfield M with the property that $\mathrm{Gal}(M : \mathbb{Q}) \cong C_n$.

Solution: Let p be a prime number with $p \equiv 1 \pmod n$. Recall that the multiplicative group of residues modulo p is cyclic for each prime number p. Thus, from part (a), there is some $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ with the property that $\mathrm{Gal}(L:\mathbb{Q}) = \langle\sigma\rangle$, and moreover σ has order $p-1 = nd$, say. But then it follows that $\mathrm{Gal}(L:\mathbb{Q})$ has the subgroup $H = \langle\sigma^n\rangle$ of index d. Let $M = \mathrm{Fix}_L(H)$. Then, by the Fundamental Theorem of Galois Theory, one has $\mathrm{Gal}(L:M) = H$ and

$$\mathrm{Gal}(M:\mathbb{Q}) \cong \mathrm{Gal}(L:\mathbb{Q})/\mathrm{Gal}(L:M) \cong \langle\sigma\rangle/\langle\sigma^n\rangle \cong C_n,$$

since the cosets of $H = \langle\sigma^n\rangle$ within $\langle\sigma\rangle$ take the shape $\sigma^r H$ with $r = 0, 1, \ldots, n-1$.