Math 306, Spring 2012
Second Midterm Exam Solutions

Name: ______________________________ Student ID: ___________________________

Directions: Check that your test has 8 pages, including this one and the blank one on the bottom (which you can use as scratch paper or to continue writing out a solution if you run out room elsewhere). Please **show all your work**. **Write neatly: solutions deemed illegible will not be graded, so no credit will be given.** This exam is closed book, closed notes. You have 70 minutes. Good luck!

1. (16 points) _____________
2. (15 points) _____________
3. (7 points) _____________
4. (9 points) _____________
5. (12 points) _____________
6. (9 points) _____________

Total (out of 68): _____________

Curved score (out of 100): _____________

Letter grade: _____________

1. (2 pts each) Give examples of the following.

   (a) An angle that cannot be trisected.

   Solution: $\pi/3$

   (b) A splitting field of $x^4 + 4 \in \mathbb{Q}[x]$.

   Solution: $\mathbb{Q}(i)$ (We have the factorization $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, where the factors are irreducible by Eisenstein's criterion (using $p = 2$). The roots are $\pm 1, \pm i$, so the splitting field is $\mathbb{Q}(i)$.)

   (c) An irreducible cubic polynomial $f \in \mathbb{Q}[x]$ such that $[L \colon \mathbb{Q}] = 6$, where L is the splitting field of f.

   Solution: $x^3 - 2$

   (d) A nonnormal extension.

   Solution: $\mathbb{Q}(\sqrt[3]{2}) \colon \mathbb{Q}$

   (e) An inseparable extension.

   Solution: $\mathbb{Z}_2(\sqrt{u}) \colon \mathbb{Z}_2(u)$

   (f) A nontrivial $\mathbb{Q}$-automorphism $\sigma \colon \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   Solution: σ determined by $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$.

   (g) An extension $L \colon K$ such that $\mathrm{Gal}(L/K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

   Solution: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \colon \mathbb{Q}$

   (h) An extension $L \colon K$ such that $\mathrm{Gal}(L/K) \cong \mathbb{Z}_3$.

   Solution: $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \colon \mathbb{Q}(e^{2\pi i/3})$

2. (a) (10 pts) Prove that, if L is the splitting field of some $f \in K[x]$, then the extension $L\colon K$ is normal. (This is one direction of Theorem 5.)

Solution: This is Theorem 9.9 on page 111 which you were asked to read. Here are the details:

Let L be the splitting field of g. Then $L\colon K$ is finite. Let f be irreducible in $K[x]$ with a zero in L. Let $M \supseteq L$ be a splitting field for fg in $K[x]$ with a zero in L. Suppose θ_1 and θ_2 are zeros of f in M. For $j = 1, 2$, we have

$$[L(\theta_1)\colon L][L\colon K] = [L(\theta_1)\colon K(\theta_1)][K(\theta_1)\colon K]$$

and

$$[L(\theta_2)\colon L][L\colon K] = [L(\theta_2)\colon K(\theta_2)][K(\theta_2)\colon K].$$

Now $[K(\theta_1)\colon K] = [K(\theta_2)\colon K]$ because θ_1 and θ_1 have the same minimum polynomial over K. Also $[L(\theta_1)\colon K(\theta_1)] = [L(\theta_2)\colon K(\theta_2)]$ since $L(\theta_1) \to L(\theta_2)$ is an isomorphism of splitting fields extending $K(\theta_1) \to K(\theta_2)$. Therefore $[L(\theta_1)\colon L] = [L(\theta_2)\colon L]$.

(b) (5 pts) Prove that, if L is algebraic over K and every element of L belongs to an intermediate field that is normal over K, then L is normal over K.

Solution: Let $L\colon K$ be algebraic. Suppose $f \in K[x]$ is irreducible with root $\alpha \in L$. Then α belongs to some intermediate field M, where $M\colon K$ is normal, so all roots of f lie in M. Therefore all roots of f lie in L. Therefore $L\colon K$ is normal.

3. (7 pts) Let p be prime and let $b \in \mathbb{Z}_p$ be fixed. If α is a root of the polynomial $f = x^p - x + b \in \mathbb{Z}_p[x]$, prove that $\mathbb{Z}_p(\alpha)$ is a normal extension of $\mathbb{Z}_p$. (Hint: You may use without proof that, for all $c \in \mathbb{Z}_p$, $c^p = c$.)

Solution: (Note: This is very similar to a homework problem.) Suppose that α is a root of f, i.e. we have $\alpha^p - \alpha + b = 0$. Then for all $c \in \mathbb{Z}_p$ we have $(\alpha + c)^p - (\alpha + c) + b = \alpha^p + c^p - \alpha - c + b = c^p - c$. But, by the hint, for all $c \in \mathbb{Z}_p$ we have $c^p = c$, and thus $\alpha + c$ is a root of f for all $c \in \mathbb{Z}_p$. Therefore, we have identified p roots of f. Since f has at most p roots, these are exactly the roots of f. Hence $\mathbb{Z}(\alpha)$ is the splitting field for f and $\mathbb{Z}_p(\alpha)$ is hence normal (by Theorem 5).

4. (a) (4 pts) State a lemma relating the degrees of $K(\alpha, \beta)$, $K(\alpha)$, and $K(\beta)$ over K if the degrees of the minimal polynomials of α and β are relatively prime.

Solution: $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$

(b) (5 pts) Use part (a) to show that the degree of the splitting field of $x^p - 2 \in \mathbb{Q}[x]$, p prime, is $p(p-1)$.

Solution: See class notes.

5. (a) (5 pts) Let $\zeta = e^{2\pi i/5}$. Prove that $\mathbb{Q}(\zeta)$ is a normal extension of $\mathbb{Q}$ and determine with proof the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. (Hint: It suffices to verify the order of one particular element in the Galois group.)

Solution: (Note: Second part was a homework problem.) We know that $\mathbb{Q}(\zeta)$ is the splitting field of $x^5 - 1 \in \mathbb{Q}[x]$, so the extension is normal. We claim that the Galois group is $\mathbb{Z}_4$. The minimum polynomial of ζ over $\mathbb{Q}$ is $f = x^4 + x^3 + x^2 + x + 1$, and the four roots are ζ, ζ^2, ζ^3 and ζ^4. Let σ_2 be the automorphism determined by $\zeta \mapsto \zeta^2$. Then σ_2 has order 4 in the Galois group, so the Galois group must be $\mathbb{Z}_4$.

(b) (7 pts) Let $n \in \mathbb{Z}_{\geq 3}$ be fixed and let $\zeta = e^{2\pi i/n}$. Prove that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian.

Solution: (Note: This was a review problem.) Let $\sigma, \rho \in \mathrm{Gal}(L/\mathbb{Q})$. Then σ and ρ are determined by

$$e^{2\pi i/n} \mapsto e^{2\pi ij/n} \text{ and } e^{2\pi i/n} \mapsto e^{2\pi ik/n},$$

respectively. This is because each root of unity has to go to another root of unity. I.e. suppose $\sigma(\zeta) = c$. Then, since σ fixes $\mathbb{Q}$, we have

$$1 = \sigma(1) = \sigma(\zeta^n) = \sigma(\zeta)^n = c^n,$$

and so $c = \sqrt[n]{1}$. Same for ρ. In addition, it suffices to specify each automorphism on just ζ since where all other roots of unity are sent is determined by this (as they are all powers of ζ).

Then

$$\sigma(\rho(e^{2\pi i/n})) = \sigma(e^{2\pi ik/n}) = e^{2\pi ijk/n} \text{ and } \rho(\sigma(e^{2\pi i/n})) = \sigma(e^{2\pi ij/n}) = e^{2\pi ijk/n}.$$

Since all elements of $\mathrm{Gal}(L/\mathbb{Q})$ are determined by $e^{2\pi i/n}$, it follows that $\sigma \circ \rho = \rho \circ \sigma$ for all automorphisms σ and ρ, so $\mathrm{Gal}(L/\mathbb{Q})$ is abelian.

6. (a) (4 pts) State the Galois Correspondence. Be sure to define the maps $*$ and $\dagger$.

Solution: See class notes.

(a) (5 pts) Show by example that maps $*$ and $\dagger$ need not be inverses of each other in general.

Solution: See class notes.