Math 306, Spring 2012
Midterm 2 Review Solutions

(1) Determine the splitting field and degree over $\mathbb{Q}$ for the following polynomials.
  (a) $x^4 + x^2 + 1$
  (b) $x^4 + 4$
  (c) $x^6 + x^3 + 1$
  (d) $x^6 + 1$

Solution:
  (a) We have $x^2 = \frac{-1\pm\sqrt{-3}}{2} = e^{2\pi i/3}$ or $e^{4\pi i/3}$. Hence $x = e^{\pi i/3}$, $e^{2\pi i/3}$, $e^{4\pi i/3}$ or $e^{5\pi i/3}$. Therefore the splitting field is $\mathbb{Q}(e^{\pi i/3}) = \mathbb{Q}(i\sqrt{3})$, so the degree is 2.
  (b) We have $x^4 = 4e^{\pi i}$, $4e^{3\pi i}$, $4e^{5\pi i}$ or $4e^{7\pi i}$, so $x = \sqrt{2}e^{\pi i/4}$, $\sqrt{2}e^{3\pi i/4}$, $\sqrt{2}e^{5\pi i/4}$ or $\sqrt{2}e^{7\pi i/4}$. But each of these is of the form $\pm 1 \pm i$, so the splitting field is $\mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$.
  (c) Notice that $(x^6 + x^3 + 1)(x^3 - 1) = x^9 - 1$, so $\mathbb{Q}(e^{2\pi i/9})$ is the splitting field. The polynomial $x^6 + x^3 + 1$ is irreducible over $\mathbb{Q}$ (plug in $x + 1$ for x) with root $e^{2\pi i/9}$. Since $e^{2\pi i/9}$ generates all the roots of $x^9 - 1$, it must generate all the roots of $x^6 + x^3 + 1$. So the degree of the extension is 6.
  (d) The splitting field is $\mathbb{Q}(e^{\pi i/6}) = \mathbb{Q}\left(\frac{\sqrt{3}}{2} + \frac{i}{2}\right) = \mathbb{Q}(\sqrt{3} + i) = \mathbb{Q}(\sqrt{3}, i)$, which has degree 4 over $\mathbb{Q}$.

(2) Let K be a field.
  (a) Let $a, b \in K$ and $a \neq 0$. Consider the map $\phi\colon K[t] \to K[t]$ defined by $\phi(f) = f(at + b)$. Prove that ϕ is a K-automorphism of $K[t]$.
  (b) Conversely, let ϕ be a K-automorphism of $K[t]$. Prove that there are $a, b \in K$ with $a \neq 0$ such that $\phi(f) = f(at + b)$. (Hint: Show that $\deg \phi(t)$ must be 1 by contradiction.)

Solution:
  (a) Clearly ϕ has an inverse $\psi\colon K[t] \to K[t]$ defined by $\psi(g) = g(\frac{t-b}{a})$, so ϕ is bijective. Also, for all $f, g \in K[t]$, we have $\phi(fg) = (fg)(at + b) = f(at + b)\, g(at + b) = \phi(f)\phi(g)$ and $\phi(f + g) = (f + g)(at + b) = f(at + b) + g(at + b) = \phi(f) + \phi(g)$.
  (b) Suppose that ϕ is a K-automorphism of $K[t]$. Let $n = \deg \phi(t)$. If $n \leq 0$, then ϕ is not surjective. If $n \geq 2$, then $\deg \phi(g) \neq 1$ for all $g \in K[t]$. Therefore ϕ is not surjective. Therefore $\phi(t)$ has degree 1, i.e. $\phi(t) = at + b$ for some $a, b \in K$ and $a \neq 0$. The map ϕ is determined by $t \mapsto at + b$. In fact $\phi(f) = f(at + b)$ for all $f \in K[t]$, which was shown in (a) to be a K-automorphism.

(3) Consider the extension $K\colon F$ and let $\phi\colon K \to K'$ be an isomorphism. Suppose that $\phi(F) = F'$.
  (a) If $\sigma \in \mathsf{Gal}(K/F)$, prove that $\phi\sigma\phi^{-1}$ lies in $\mathsf{Gal}(K'/F')$.
  (b) Prove that the map $\psi\colon \mathsf{Gal}(K/F) \to \mathsf{Gal}(K'/F')$, defined by $\psi(\sigma) = \phi\sigma\phi^{-1}$, is a group isomorphism.

Solution:
  (a) Clearly $\phi\sigma\phi^{-1}$ is a map from K' to K'. Since ϕ and σ are both isomorphisms, then $\phi\sigma\phi^{-1}$ is also an isomorphism. Let $a \in F'$. Then $\phi^{-1}(a) \in F$, so it is fixed by σ. Therefore $\phi\sigma\phi^{-1}(a) = \phi(\phi^{-1}(a)) = a$, so $\phi\sigma\phi^{-1}$ fixes F' and is therefore an F'-automorphism of K'.
  (b) Clearly, for all $\sigma, \rho \in \mathsf{Gal}(L/K)$, we have

$$\psi(\sigma\rho) = \phi\sigma\rho\phi^{-1} = \phi\sigma\phi^{-1}\phi\rho\phi^{-1} = \psi(\sigma)\psi(\rho).$$

  Showing this is a bijection is not difficult.

(4) (a) Suppose that char $K = p \neq 0$. Consider the map $\phi\colon K \to K$ given by $\phi(\alpha) = \alpha^p$ for all $\alpha \in K$. Prove that ϕ is a ring monomorphism. This mapping is called the *Frobenius monomorphism*.
  (b) Suppose that char $K = p > 0$. Prove that K is perfect (i.e. every polynomial in $K[x]$ is separable) iff the Frobenius monomorphism is an automorphism.

Solution:

(a) For all $a, b \in K$, we have $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$ and $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$. If $\phi(a) = 0$, then $a^p = 0$. Since K is an integral domain, we have $a = 0$, so ϕ is injective.

(b) Suppose that K is perfect but the Frobenius monomorphism is not an automorphism, i.e. it is not surjective. Then there is $b \in K$ such that b is not a p-th power. Let $g = x - b$, which is irreducible. Then $f = x^p - b$ is irreducible (since $\alpha^p \neq b$ for any α, this means that $x^p - b = 0$ has no solutions). However, we know that $Df = 0$, so f is inseparable (this was a homework problem), contradicting the fact that K is perfect. Therefore the Frobenius monomorphism is an automorphism. Conversely, suppose that K is not perfect. Then there is an irreducible inseparable

$$f = a_0 + a_1 x^p + \cdots + a_n x^{np}$$

where $g = a_0 + a_1 x + \cdots + a_n x^n$ is irreducible and some a_i is not a p-th power. Therefore the Frobenius monomorphism is not surjective, and thus is not an automorphism.

(5) Let $n \in \mathbb{Z}_{\geq 3}$ and let $f = x^n - 1 \in \mathbb{Q}[x]$. If L is the splitting field for n, prove that $\mathrm{Gal}(L/\mathbb{Q})$ is abelian. (Hint: show that an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ must send $e^{2\pi i/n}$ to $e^{2\pi i k/n}$ for some $k \in \mathbb{Z}$ and σ is determined by $e^{2\pi i/n} \mapsto e^{2\pi i k/n}$.)

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

$$e^{2\pi i/n} \mapsto e^{2\pi i j/n} \text{ and } e^{2\pi i/n} \mapsto e^{2\pi i k/n},$$

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

$$\sigma(\rho(e^{2\pi i/n})) = \sigma(e^{2\pi i k/n}) = e^{2\pi i jk/n} \text{ and } \rho(\sigma(e^{2\pi i/n})) = \sigma(e^{2\pi i j/n}) = e^{2\pi i jk/n}.$$

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) Let $L\colon K$ be a field extension. Let H be a subgroup of $\mathrm{Gal}(L/K)$ and M be an intermediate subfield. Prove that $H \subseteq H^{\dagger *}$.

Solution: Let $h \in H$ and let $a \in H^\dagger$. Then $h(a) = a$. Therefore h fixes everything in $H^\dagger$, so $h \in H^{\dagger *}$.

(7) For each of the following extensions $L\colon K$, find (i) $\mathrm{Gal}(L/K)$, (ii) $H^\dagger$ for all the subgroups H of $\mathrm{Gal}(L/K)$,

(a) $\mathbb{Q}(\sqrt{1+\sqrt{3}})\colon \mathbb{Q}$

(b) $L\colon \mathbb{Z}_2$, where L is the splitting field of $x^2 + x + 1 \in \mathbb{Z}_2[x]$

(c) $L\colon \mathbb{Z}_5$, where L is the splitting field of $(x^2 - 2)(x^2 - 3) \in \mathbb{Z}_5[x]$

(d) $L\colon \mathbb{Z}_7$, where L is the splitting field of $x^3 - 5 \in \mathbb{Z}_7[x]$

(e) $L\colon \mathbb{Z}_5$, where L is the splitting field of $(x^5 - t)(x^5 - u) \in \mathbb{Z}_5(t, u)[x]$, where t is transcendental over $\mathbb{Z}_5$ and u is transcendental over $\mathbb{Z}_5(t)$

Solution:

(a) (i) Let $\omega = \sqrt{1+\sqrt{3}}$. Then it suffices to see where an eutomorphism sends ω and $\sqrt{3}$ since those generate all the elements that are in $\mathbb{Q}(\omega)$ but not in $\mathbb{Q}$. It is not hard to see that an automorphism of $\mathbb{Q}(\omega)$ must send ω to ω or to $-\omega$ (the only other option is $\omega \to \sqrt{3}$ but then we would have $\omega^2 = 1 + \sqrt{3} \to 3$ and an irrational number cannot map to a rational; otherwise our map is not $1-1$ since 3 already maps to 3). But it is also not hard to see that both $\sigma_1\colon \omega \mapsto \omega$ and $\sigma_2\colon \omega \mapsto -\omega$ must map $\sqrt{3}$ to itself. Hence $G = \mathrm{Gal}(L/K) \cong \mathbb{Z}_2$, consisting of σ_1 and σ_2.

(ii) We have $\langle e\rangle^\dagger = \mathbb{Q}(\omega)$ and $G^\dagger = \mathbb{Q}(\sqrt{3})$.

(b) (i) If ζ is a root of $x^2 + x + 1$, then $\zeta + 1$ is the other root. Hence $L = \mathbb{Z}_2(\zeta)$ and $G \cong \mathbb{Z}_2$.
(ii) We have $\langle e \rangle^\dagger = \mathbb{Z}_2(\zeta)$ and $G^\dagger = \mathbb{Z}_2$.

(c) (i) Let ζ be a root of $x^2 - 2$. Then the roots of $(x^2-2)(x^2-3)$ are ζ, $-\zeta$, 2ζ and -2ζ (2ζ is a root since $(\zeta^2-2)(\zeta^2-3) = \zeta^4 - 5\zeta^2 + 6 = (2\zeta)^4 + 1 = 0$ or $\zeta^4 + 1 - 0$ or $\zeta^4 = -1 = 4$; but also $(2\zeta)^4 = 16\zeta^4 = \zeta^4 = 4)$. Hence $L = \mathbb{Z}_2(\zeta)$ and $G \cong \mathbb{Z}_2$.
(ii) We have $\langle e \rangle^\dagger = \mathbb{Z}_2(\zeta)$ and $G^\dagger = \mathbb{Z}_2$.

(d) (i) Let ζ be a root of $x^3 - 5$. Then the other roots are 2ζ and 4ζ. Hence $L = \mathbb{Z}_7(\zeta)$ and G has 3 elements, i.e. $G \cong \mathbb{Z}_3$.
(ii) We have $\langle e \rangle^\dagger = \mathbb{Z}_7(\zeta)$ and $G^\dagger = \mathbb{Z}_7$.

(e) (i) There is only one automorphism in Gal$(L/\mathbb{Z}_5)$, so $G = \{e\}$. Here $L = \mathbb{Z}_5(\gamma, \delta)$, where γ is a root of $x^5 - t$ and δ is a root of $x^5 - u$.
(ii) We have $\langle e \rangle^\dagger = L$.