Math 306, Spring 2012
First Midterm Exam Solutions

Name: ______________________________ Student ID: __________________________

Directions: Check that your test has 9 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. (5 points) ____________
3. (5 points) ____________
4. (5 points) ____________
5. (7 points) ____________
6. (8 points) ____________
7. (9 points) ____________

Total (out of 55): ____________

Curved score (out of 100): ____________

Letter grade: ____________

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

   (a) An integral domain which is not a field.

   Solution: $\mathbb{Z}$

   (b) An infinite ring which is not an integral domain.

   Solution: $\mathbb{Z} \times \mathbb{Z}$

   (c) A unique factorization domain that is not a principal ideal domain.

   Solution: $\mathbb{Z}[x]$

   (d) A field of order 8.

   Solution: $\mathbb{Z}_2[x]/(x^3 + x + 1)$

   (e) A cubic polynomial in $\mathbb{Z}[x]$ that is irreducible by Eisenstein Criterion.

   Solution: $x^3 - 2$

   (f) A quadratic polynomial in $\mathbb{Z}_5[x]$ that is irreducible.

   Solution: $x^2 + x + 1$

   (g) A transcendental field extension $L\colon K$.

   Solution: $\mathbb{C}\colon \mathbb{Q}$

   (h) A field L such that $[L\colon \mathbb{Q}(\pi)] = 2$.

   Solution: $\mathbb{Q}(\sqrt{\pi})$

2. (5 pts) Let K be a subfield of $\mathbb{C}$. Let α be algebraic over K with minimal polynomial m. Show that there is an isomorphism

$$K[x]/(m) \cong K(\alpha).$$

Please be sure to verify that your isomorphism is well-defined. (Note that another way to do this is to exhibit a surjective homomorphism from $K[x]$ to $K(\alpha)$ whose kernel is (m).)

Solution: This was outlined in class, but here are the details: The isomorphism, call it ϕ, is given by $\phi([p(x)]) = p(\alpha)$. To see that this is well-defined, suppose $p(x)$ and $q(x)$ are both representatives of the same class in $K[x]/(m)$. This means that they differ by an element of the ideal (m), i.e.

$$p(x) = q(x) + r(x)m(x)$$

where $r(x)$ is some polynomial over K. But then

$$p(\alpha) = q(\alpha) + r(\alpha)m(\alpha) = q(\alpha)$$

because $m(\alpha) = 0$.

Also, ϕ is clearly a homomorphism since

$$\begin{aligned} \phi(p(x) + r(x)) &= p(\alpha) + r(\alpha) = \phi(p(x)) + \phi(r(x)) \\ \phi(p(x)r(x)) &= p(\alpha)r(\alpha) = \phi(p(x))\phi(r(x)). \end{aligned}$$

For injectivity, suppose $[p(x)] \neq [r(x)]$. Then it must be that $p(\alpha) \neq r(\alpha)$ because otherwise it would follow that $p(\alpha) - r(\alpha) = 0 = m(\alpha)$ or $p(\alpha) = m(\alpha) + r(\alpha)$, which means that $[p(x)] = [r(x)]$.

For surjectivity, given $p(\alpha) \in K(\alpha)$, we have $\phi([p(x)]) = p(\alpha)$.

3. (5 pts) Determine whether the polynomial $f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$ is reducible over $\mathbb{Q}$.

Solution: The given polynomial $f(x)$ is reducible if and only if $9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$ is. However, $9f(x)$ is irreducible by Eisenstein criterion with $p = 3$.

4. (5 pts) List all the irreducible monic quadratic polynomials in $\mathbb{Z}_2[x]$. Justify your answer.

Solution: All possible monic quadratic polynomials over $\mathbb{Z}_2[x]$ are x^2, x^2+x, x^2+1, and x^2+x+1. The first two are clearly reducible. The third has 1 as a zero and it factors as $(x+1)(x+1)$. The last is the only one that is irreducible since, if it factored as $(x+a)(x+b)$, we would have to have $a+b=1$ and $ab=0$ but this system has no solutions in $\mathbb{Z}_2$.

5. (a) (4 pts) Show directly that the polynomial $f = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$. Do not use general facts we know from class about polynomials of this form.

Solution: See notes from class for proof of why $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ for any prime p and let $p = 5$.

(b) (3 pts) Find $\alpha \in \mathbb{C}$ such that f is the minimal polynomial for α. (Hint: You should be able to just say what α is without any work.) What subgroup of $\mathbb{C}$ does α generate?

Solution: Any fifth primitive root of unity is a root of this polynomial, so for example, $\alpha = e^{2\pi i/5}$ works. This α generates the group of fifth roots of unity.

6. (4 pts each) Let p and q be distinct primes in $\mathbb{Z}$.

   (a) Prove that $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is a simple extension of $\mathbb{Q}$.

   Solution: This was a homework problem.

   (b) Prove that $\alpha = \sqrt{p} + \sqrt{q}$ is algebraic over $\mathbb{Q}$ by exhibiting (with justification) an appropriate quartic polynomial in $\mathbb{Q}[x]$ with α as a root.

   Solution: This was a homework problem.

7. Let α and β be complex numbers, and let $\mathbb{A}$ be the collection of algebraic numbers over $\mathbb{Q}$. Do not assume in this problem that $\mathbb{A}$ is a field.

(a) (4 pts) Prove that, if α and β belong to $\mathbb{A}$, then $\alpha + \beta$ and $\alpha\beta$ both belong to $\mathbb{A}$.

Solution: (This is essentially a problem from the review exercises.) Certainly we know that $\mathbb{Q}(\alpha, \beta) \colon \mathbb{Q}$ is a finite extension, since both α and β are algebraic over $\mathbb{Q}$. Now $\alpha\beta$ and $\alpha + \beta$ both lie in $\mathbb{Q}(\alpha, \beta)$, so $\mathbb{Q}(\alpha\beta) \subseteq \mathbb{Q}(\alpha, \beta)$ and $\mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$. Therefore by the Tower Law, we conclude that both $\mathbb{Q}(\alpha\beta) \colon \mathbb{Q}$ and $\mathbb{Q}(\alpha + \beta) \colon \mathbb{Q}$ are finite, so $\alpha\beta$ and $\alpha + \beta$ are both algebraic over $\mathbb{Q}$.

(b) (5 pts) If $\beta \in \mathbb{A}$ is nonzero, let $f = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$ be its minimum polynomial over $\mathbb{Q}$. Prove that $\beta^{-1} \in \mathbb{A}$ by explicitly finding a monic polynomial in $\mathbb{Q}[x]$ which has β^{-1} as a root.

Solution: First note that c_0 is nonzero, for otherwise f would be reducible. Now $c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1} + \beta^n = 0$, so

$$0 = c_0\beta^{-n} + c_1\beta^{-n+1} + \cdots + c_{n-1}\beta^{-1} + 1 = c_0(\beta^{-1})^n + c_1(\beta^{-1})^{n-1} + \cdots + c_{n-1}\beta^{-1} + 1 = 0.$$

Since $c_0 \neq 0$, we can write

$$0 = (\beta^{-1})^n + \frac{c_1}{c_0}(\beta^{-1})^{n-1} + \cdots + \frac{c_{n-1}}{c_0}\beta^{-1} + \frac{1}{c_0}.$$

Hence

$$x^n + \frac{c_1}{c_0}x^{n-1} + \cdots + \frac{c_{n-1}}{c_0}x + \frac{1}{c_0}$$

is the polynomial that we want.