MAT 512 Final Exam Solutions

Solutions are due by 6pm on **Wednesday, May 10**. You can email your solutions to me; or leave them at my office; or have someone at the main office put them into my mailbox. Please use a separate page for each question, so that I have space for comments.

1. Consider the cubic polynomial $x^3 + px + q$, where $p, q \in \mathbb{R}$ are real numbers. Suppose that this polynomial has three distinct real roots. Using examples where appropriate, explain clearly why Cardano's formula gives these real roots in terms of complex numbers.

Solution: Cardano's formula for the roots of the cubic equation $x^3 + px + q = 0$ is

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \sqrt[3]{-\frac{q}{2} - \sqrt{R}}$$

where $R = (p/3)^3 + (q/2)^2$. Denote by r_1, r_2, r_3 the three roots of the cubic. Recall that the discriminant of the cubic polynomial is

$$\Delta = (r_1 - r_2)^2 (r_1 - r_3)^2 (r_2 - r_3)^2.$$

Now the point is that the quantity R in Cardano's formula is related to the discriminant by $\Delta = -108R$. If the roots of the cubic are distinct real numbers, then $\Delta > 0$, and therefore $R < 0$. In Cardano's formula, we therefore need to take the square root of the negative number R, and so we end up with complex numbers in the formula, even though the roots themselves are real numbers.

For example, consider the case $r_1 = 0$, $r_2 = 1$, and $r_3 = -1$; the cubic polynomial is

$$x(x-1)(x+1) = x^3 - x$$

and so $p = -1$ and $q = 0$. (The sum of the three roots must be 0, in order to get a polynomial of the form $x^3 + px + q$.) We then have $R = -1/27$, and so the formula for the roots involves the complex number $\sqrt{-3}$.

2. Let R be a ring. A nonempty subset $I \subseteq R$ is called an *ideal* if

   1. For every $a, b \in I$, one has $a + b \in I$.
   2. For every $r \in R$ and every $a \in I$, one has $ra \in I$.

   In words, I is closed under addition, and under multiplication by elements in R.

   Let I be an ideal in the ring of integers $\mathbb{Z}$. Show that there is an integer $m \geq 1$ such that I is the set of all multiples of m.

Solution: One possibility is that $I = \{0\}$ contains only the zero element of the ring. In this case, we can take $m = 0$. We may therefore assume from now on that I has other elements besides 0.

Now let us find the integer m. If we already knew that

$$I = \{\dots, -2m, -m, 0, m, 2m, \dots\},$$

then m would be the smallest positive integer contained in I. The idea is to use this as the definition. First, we note that I does contain positive integers: if $a \in I$ and $a < 0$, then because I is an ideal, we get $-a = (-1) \cdot a \in I$, and $-a$ is positive. We may therefore define $m \geq 1$ as the smallest positive integer that belongs to the ideal I. Then $m \in I$, and because I is an ideal, I also contains every multiple of m. In symbols,

$$\{\dots, -2m, -m, 0, m, 2m, \dots\} \subseteq I.$$

It remains to prove that every element of I is a multiple of m. Let $a \in I$ be an arbitrary element. Using division with remainder, we can write

$$a = qm + r$$

where $q \in \mathbb{Z}$ and $0 \leq r < m$. Because $a \in I$ and $m \in I$, we get $r = a - qm \in I$. But $r < m$, and because m was the smallest positive integer in I, it follows that $r = 0$. Therefore $a = qm$ is indeed a multiple of m.

3. Determine all the units in the ring $\mathbb{Z}_{18}$. Find the smallest number $n \geq 1$ such that $u^n = 1$ for every unit in $\mathbb{Z}_{18}$. Clearly explain the process you used to find the answers.

Solution: We can think of the elements of $\mathbb{Z}_{18}$ as the congruence classes of $0, 1, \dots, 17$, modulo 18. The congruence class of a is a unit if and only if $\gcd(a, 18) = 1$. The units are therefore $1, 5, 7, 11, 13, 17$. The number of units can also be computed using Euler's ϕ-function. We have

$$\phi(18) = \phi(2) \cdot \phi(9) = 6.$$

The reason is that $\phi(ab) = \phi(a)\phi(b)$ whenever a, b are relatively prime. This confirms that there are 6 units.

We then compute powers of each unit and look for the smallest power that is equal to 1. Here is a table with the results:

$$1^1 \equiv 1, \quad 5^6 \equiv 1, \quad 7^3 \equiv 1, \quad 11^6 \equiv 1, \quad 13^3 \equiv 1, \quad 17^2 \equiv 1$$

So the smallest value of n that works for all units is $n = 6$.

4. Let $\varphi \colon R \to S$ be a ring homomorphism. The kernel $\ker \varphi$ is the set of elements $r \in R$ such that $\varphi(r) = 0$. Show that φ is injective if, and only if, $\ker \varphi = \{0\}$.

Solution: We first prove that if φ is injective, then $\ker \varphi = \{0\}$. This is easy. Suppose that $a \in \ker \varphi$. This means that $\varphi(a) = 0$. We also have $\varphi(0) = 0$, and because φ is injective, it follows that $a = 0$. Therefore $\ker \varphi = \{0\}$.

Next, we prove that if $\ker \varphi = \{0\}$, then φ is injective. Suppose that we have two elements $a, b \in R$ with $\varphi(a) = \varphi(b)$. Because φ is a ring homomorphism, we get

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0,$$

and therefore $a - b \in \ker\varphi$. But $\ker\varphi = \{0\}$, and so $a - b = 0$. This gives $a = b$, and so φ is injective.

5. Prove that the polynomial $f(x) = x^5 - 2x^4 + 2x^3 + 2x + 8$ does not factor as a product of lower-degree polynomials in $\mathbb{Z}[x]$. Clearly explain your reasoning.

Solution: We use reduction modulo the prime $p = 3$. This gives us the polynomial

$$\bar{f}(x) = x^5 + x^4 + 2x^3 + 2x + 2 \in \mathbb{Z}_3[x].$$

If $f(x)$ factors as a product of lower-degree polynomials in $\mathbb{Z}[x]$, then of course $\bar{f}(x)$ factors as a product of lower-degree polynomials in $\mathbb{Z}_3[x]$. So it is enough to prove that $\bar{f}(x)$ is an irreducible polynomial.

Let us first check that $\bar{f}(x)$ has no roots in $\mathbb{Z}_3$, and therefore no linear factors. This is easy:

$$\bar{f}(0) = 2, \quad \bar{f}(1) = 2, \quad \bar{f}(2) = 1$$

Since $\bar{f}(x)$ has degree 5, the only other possibility is that it has an irreducible monic factor of degree 2. There are three irreducible quadratic polynomials in $\mathbb{Z}_3[x]$:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2$$

We can find these by listing all 9 monic polynomials of degree 2, and then eliminating those that have a root in $\mathbb{Z}_3$. We then check, using division with remainder, that none of these three polynomials divide $\bar{f}(x)$. Therefore $\bar{f}(x)$ is irreducible.

6. Let F be a finite field with q elements. Explain why every element of F is a root of the polynomial $x^q - x \in F[x]$.

Solution: Every nonzero element of F is a unit (because F is a field). The number of units in F is therefore $q - 1$. By Euler's theorem, we have $a^{q-1} = 1$ for every nonzero $a \in F$. After multiplying by a, we get $a^q = a$. This also holds for $a = 0$, and so every element of F is a root of the polynomial $x^q - x$.

7. Let R be an integral domain with finitely many elements. Prove that every nonzero element $a \in R$ has a multiplicative inverse.

Solution: Let $a \in R$ be a nonzero element. The idea is to look at what happens when we multiply the elements of R by a. This gives us a function

$$f \colon R \to R, \quad f(r) = ar.$$

The fact that R is an integral domain means that f is injective. Indeed, suppose we have $f(r) = f(s)$. Then

$$a(r - s) = ar - as = f(r) - f(s) = 0,$$

and since $a \neq 0$, it follows that $r - s = 0$, hence $r = s$. Therefore f is injective. Now an injective function from a finite set to itself is necessarily also surjective (for reasons of size). In our case, R is a finite set, and so f must be surjective. In particular, there is an element $r \in R$ such that $f(r) = 1$. But then $ra = 1$, and so r is a multiplicative inverse.

8. A number $p \geq 2$ is prime if it cannot be written as a product of two smaller natural numbers. This is also true for 1, but 1 is not considered to be a prime number. How would you explain to a student why 1 should be excluded from the definition?

Solution: We should exclude 1 from the definition of prime numbers because we want the factorization into prime numbers to be unique. Recall that every natural number $a \geq 2$ can be uniquely written as a product of prime numbers

$$a = p_1 p_2 \cdots p_m,$$

where $p_1 < p_2 < \cdots < p_m$ are the prime factors of a in increasing order. If 1 was a prime number, this factorization would no longer be unique, because we could add any number of 1's as factors. For example, the prime factorization of 6 is $6 = 2 \cdot 3$, but we also have $6 = 1 \cdot 2 \cdot 3$ and $6 = 1 \cdot 1 \cdot 2 \cdot 3$, and so on.

Rules: You may quote results from the textbook or from class in your solution, provided that they do not make a problem trivial. (For example, "This is just Theorem 9.7 in the textbook" is not allowed.) You are not allowed to discuss these problems with anyone, and you are not allowed to look up facts or solutions online. On the first page of your exam, please include a statement (dated and signed) that you have followed these rules faithfully.