Math 225 Modern Algebra
Second test answers

Prof. D. Joyce

November, 2008

Scale: 87–100 A, 70–86 B, 50–69 C. Median 87.

Problem 1. On ring isomorphisms. [20]

In this problem, you'll prove that the ring $\mathbf{Z}_5 \times \mathbf{Z}_8$ is isomorphic to the ring $\mathbf{Z}_{40}$ as rings with a multiplicative identity. The isomorphism depends on 5 and 8 being relatively prime.

a. [4] First, what is the multiplicative identity of the ring $\mathbf{Z}_5 \times \mathbf{Z}_8$?

It's $(1, 1)$, or in congruence class notation $([1]_5, [1]_8)$, since $(1, 1)(x, y) = (x, y) = (x, y)(1, 1)$.

Now, suppose f is an isomorphism $f : \mathbf{Z}_{40} \to \mathbf{Z}_5 \times \mathbf{Z}_8$ preserving the multiplicative identity. Since every element of $\mathbf{Z}_{40}$ is a multiple of 1, therefore $f(n) = nf(1)$. Also, f must send 1 in $\mathbf{Z}_{40}$ to the multiplicative identity of $\mathbf{Z}_5 \times \mathbf{Z}_8$, which you identified in part a. Therefore, there can be only one such isomorphism.

b. [8] If you try to define a ring homomorphism $f : \mathbf{Z}_{39} \to \mathbf{Z}_5 \times \mathbf{Z}_8$ in the same way, it doesn't work, and you don't get a ring homomorphism. In your own words, explain what goes wrong. (Here are some possibilities of what can go wrong: f is not well-defined, f doesn't preserve addition, f doesn't preserve multiplication. Note that it has something to do with 5 and 8 dividing 40, but not 39.)

It's not well-defined, and it won't preserve either addition or multiplication.

It's not well-defined, since $[0]_{39} = [39]_{39}$, but $f([0]_{39})$ would be $([0]_5, [0]_8)$, while $f([39]_{39})$ would be $([39]_5, [39]_8)$, and 0 is not congruent to 39 either mod 5 or mod 8.

Perhaps it's easier to see it doesn't preserve addition. Take two numbers that add to more than 39, say 21 and 22. $f(21 + 22) = f(43) = f(4) = (4, 4)$, but $f(21) + f(22) = (21, 21) + (22, 22) = (43, 43) = (3, 3)$. Since $(4, 4) \neq (3, 3)$, f doesn't preserve addition. Similarly, you can show f doesn't preserve multiplication by taking two numbers that multiply to more than 39.

c. [8] If f is an isomorphism, then it has an inverse, $f^{-1} : \mathbf{Z}_5 \times \mathbf{Z}_8 \to \mathbf{Z}_{40}$. What is f^{-1}? (Note that it's enough to specify $f^{-1}(1, 0)$ and $f^{-1}(0, 1)$ since all the other elements of $\mathbf{Z}_5 \times \mathbf{Z}_8$ are linear combinations of $(1, 0)$ and $(0, 1)$.)

Let $f^{-1}(1, 0) = m$, and $f^{-1}(0, 1) = n$. To find m and n mod 40.

If $f(m) = (1, 0)$, then $(m, m) = (1, 0)$, or, in more detailed notation, $([m]_5, [m]_8) = ([1]_5, [0]_8)$. In other words,

$$\begin{aligned} 1 &\equiv m \pmod 5, \qquad \text{and} \\ 0 &\equiv m \pmod 8 \end{aligned}$$

What multiple of 8 is congruent to 1 mod 5? It's $m = 16$.

Similarly, n is a multiple of 5 congruent to 1 mod 8, namely 25.

Thus, $f^{-1}(1, 0) = 16$, and $f^{-1}(0, 1) = 25$. In general, $f^{-1}(a, b) = 16a + 25b$.

Problem 2. On automorphisms. [20; 10 points each part]

Consider the field $\mathbf{Q}[\sqrt{5}]$. Every element in this field can be written as $x + y\sqrt{5}$ where x and y are rational numbers. Also consider the function $f : \mathbf{Q}[\sqrt{5}] \to \mathbf{Q}[\sqrt{5}]$, where $f(x + y\sqrt{5}) = x - y\sqrt{5}$.

a. Carefully prove that f is a ring homomorphism.

You need to show that

1. $f((x + y\sqrt{5}) + (u + v\sqrt{5})) = f(x + y\sqrt{5}) + f(u + v\sqrt{5})$,
2. $f((x + y\sqrt{5})\,(u + v\sqrt{5})) = f(x + y\sqrt{5})\,f(u + v\sqrt{5})$, and
3. $f(1) = 1$.

Condition (3) is easiest since $f(1 + 0\sqrt{5}) = 1 - \sqrt{5}$. Condition (1) holds since

$$\begin{aligned} f((x + y\sqrt{5}) + (u + v\sqrt{5})) &= f((x + u) + (y + v)\sqrt{5}) \\ &= (x + u) - (y + v)\sqrt{5} \\ &= (x - y\sqrt{5}) + (u - v\sqrt{5}) \\ &= f(x + y\sqrt{5}) + f(u + v\sqrt{5} \end{aligned}$$

Condition (2) holds since

$$\begin{aligned} f((x + y\sqrt{5})\,(u + v\sqrt{5})) &= f((xu + 5yv) + (xv + yu)\sqrt{5}) \\ &= (xu + 5yv) - (xv + yu)\sqrt{5}) \\ &= (x - y\sqrt{5})\,(u - v\sqrt{5}) \\ &= f(x + y\sqrt{5})\,f(u + v\sqrt{5} \end{aligned}$$

b. Prove that f is an isomorphism.

You could show that f is injective and surjective. Slightly easier, you could show that f is its own inverse.

$$f(f(x+y\sqrt{5})) = f(x-y\sqrt{5}) = x+y\sqrt{5}).$$

(Comment. This f along with the identity form a two-element group, the group of automorphisms of $\mathbf{Q}[\sqrt{5}]$ over $\mathbf{Q}$. In general, for any field extension K over F, there is a group of automorphisms of K that fix F, called the Galois group of K/F. Galois groups are used to study field extensions and solutions of polynomial equations.)

Problem 3. On integral domains. [20; 5 points each part]

We saw how to extend any integral domain to a field by introducing fractions. The construction doesn't work properly if the original ring is not an integral domain. Take, for instance, $\mathbf{Z}_6$.

a. Why isn't $\mathbf{Z}_6$ an integral domain?

You could either say that $\mathbf{Z}_6$ has zero divisors since $2\cdot 3 = 0$, or that $\mathbf{Z}_6$ doesn't have the cancellation property since $2\cdot 3 = 4\cdot 3$ but $2 \neq 3$.

Define the binary relation $\sim$ on $\mathbf{Z}_6 \times (\mathbf{Z}_6 - \{0\})$ by

$$(a,b) \sim (c,d) \quad \text{if and only if} \quad ad = bc.$$

This binary relation will not be an equivalence relation because $\mathbf{Z}_6$ is not an integral domain. For each of the following properties, either prove the property or find a counterexample.

b. $\sim$ is reflexive.

Is $(a,b) \sim (a,b)$? Yes, since $ab = ba$.

c. $\sim$ is symmetric.

Does $(a,b) \sim (c,d)$ imply $(c,d) \sim (a,b)$? Does $ad = bc$ imply $cb = da$? Yes.

d. $\sim$ is transitive. It better not be if it's not going to be an equivalance relation. Does $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ imply $(a,b) \sim (e,f)$? That is, does $ad = bc$ and $cf = de$ imply $af = be$? From the first two conditions, we see that $adf = bcf$ and $bcf = bde$, so $adf = bde$. If we had an integral domain, we could cancel the d's and conclude it's transitive, but $\mathbf{Z}_6$ is not an integral domain. If we make $d = 3$ but a, b, c, e, and f even, then $adf = bcf$ and $bcf = bde$ are both 0, therefore equal. But we can make $af \neq be$ if we take a, f, and b to be 2 while taking e to be 4. That gives us a counterexample for transitivity.

Problem 4. On ideals and quotients. [20]

Consider the ring R of functions from $\mathbf{R}$ to $\mathbf{R}$. Thus, an element f in R is just a function $f : \mathbf{R} \to \mathbf{R}$. Addition and multiplication in R are just the usual addition and multiplication of functions, that is, $f+g$ is the function whose value at x is $(f+g)(x) = f(x)+g(x)$, likewise, $(fg)(x) = f(x)g(x)$.

Let I be the set $\{f \in R \,|\, f(3) = 0\}$.

a. [8] Prove that I is an ideal of R.

Of course, the 0 function is in I since $0(x) = 0$ for all x, and, in particular, $0(3) = 0$.

Next, I is closed under addition, since if $f(3) = 0$ and $g(3) = 0$, then $(f+g)(3) = f(3) + g(3) = 0 + 0 = 0$.

Finally, if f is any function, and $g(3) = 0$, then $(fg)(3) = f(3)g(3) = f(3)\cdot 0 = 0$.

b. [6] Let S be the quotient ring R/I. When do two functions f and g name the same element of S, that is when is $f \equiv g \pmod{I}$? Your answer should not mention I.

$f \equiv g \pmod{I}$ iff $f - g \in I$ iff $(f-g)(3) = 0$ iff $f(3) - g(3) = 0$ iff $f(3) = g(3)$. So two functions are equivalent mod I iff they have the same value at 3.

c. [6] What well known ring is S isomorphic to? Explain why it's isomorphic to that ring.

An element $f + I$ in $S = R/I$ is named by a function f, but the only thing that's important about the function is its value at 3, so you might as well treat an element $f + I$ of S as the value $f(3)$, and that's a real number. So, it looks like S is isomorphic to $\mathbf{R}$. In fact, here's the isomorphism $\phi : S \to \mathbf{R}$. Let $\phi(f + I) = f(3)$, that is, ϕ is evaluation of the function at 3. Two elements of S, namely $f + I$ and $g + I$ are equal iff they have the same value at 3, so ϕ is a bijection. That ϕ is a homomorphism follows from the equations $(f+g)(3) = f(3)+g(3)$ and $(f\cdot g)(3) = f(3)\cdot g(3)$.

Problem 5. On Euclidean domains. [20]

We discussed the division algorithm for the Gaussian integers $\mathbf{Z}[i]$. The valuation function, also called the norm, is given by $v(x+yi) = x^2+y^2$. In order to divide one Gaussian integer b into another a to get a quotient q and remainder r, you can perform the complex division a/b to get an exact quotient, and choose q to be the closest Gaussian integer to that exact quotient. (If a/b is equally close to two Gaussian integers, either can be taken as q.) The remainder r is then determined by the formula $r = a - bq$.

(Check your computations carefully as you make them. Any arithmetic error along the way will lead to the wrong answer.)

a. [4] Let $b = 4 - 2i$ and $a = 4 + 7i$. Determine $v(b)$ and $v(a)$.

$v(b) = v(4-2i) = 4^2 + (-2)^2 = 16 + 4 = 20$. $v(a) = v(4+7i) = 16 + 49 = 65$.

b. [4] Divide b into a to determine the quotient q_1 and remainder r_1.

Since the complex number

$$\frac{a}{b} = \frac{4+7i}{4-2i}\frac{4+2i}{4+2i} = \frac{2+36i}{20} = \tfrac{1}{10} + \tfrac{9}{5}i$$

is closest to the Gaussian integer $2i$, therefore $q_1 = 2i$ is the quotient, and the remainder is $r_1 = a - q_1 b = 4 + 7i - 2i(4 - 2i) = -i$.

c. [12] The Euclidian algorithm to find the greatest common divisor of two elements proceeds by repeatedly dividing the smaller of the two (smaller in the sense that it has the smaller valuation) into the larger and replacing the larger by the remainder. In part b you have done one step of this process. The next step is to divide r_1 into b to get a quotient q_2 and remainder r_2, and replace b by r_2. Do that, and continue the algorithm until the remainder is 0. The last divisor d is $\text{GCD}(a, b)$.

But $r_1 = -i$ is a unit, so it divides b. Thus the last divisor is $r_1 = -i$. Hence, $\text{GCD}(a, b) = -i$. Greatest common divisors are only defined up to a unit, so we can also say that $\text{GCD}(a, b) = 1$, hence a and b are relatively prime.