MATH 343 (Rusin) — FINAL ANSWERS — May 11 2012

As usual, your answers may be very different from the answers shown here and yet still be quite correct.

1. Show that for every natural number n, $\displaystyle\sum_{i=1}^{i=n} \frac{1}{i(i+1)} = \frac{n}{n+1}$, that is,

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

Answer: Let $S(n) = \displaystyle\sum_{i=1}^{i=n} \frac{1}{i(i+1)}$ and $T(n) = \frac{n}{n+1}$, and let $P(n)$ be the statment "$S(n) = T(n)$". (Note that $S(n)$ and $T(n)$ are NUMBERS, while $P(n)$ is a SENTENCE.)

$P(1)$ is true because $S(1) = T(1)$: they're both $\frac{1}{2}$.

If $P(k-1)$ is a true statement for some integer k, then $P(k)$ is also true: $S(k) = \frac{1}{2} + \frac{1}{6} + \ldots + \frac{1}{(k-1)k} + \frac{1}{k(k+1)}$ is obviously the same as $S(k-1) + \frac{1}{k(k+1)}$, while $T(k)$ exceeds $T(k-1)$ by $\frac{k}{k+1} - \frac{k-1}{k} = \frac{k^2-(k+1)(k-1)}{k(k+1)} = \frac{1}{k(k+1)}$ as well. That is, we have $S(k) = S(k-1) + \frac{1}{k(k+1)} = T(k-1) + \frac{1}{k(k+1)} = T(k)$, as desired.

Thus $P(n)$ is a true statement for all natural numbers n, by the Principle of Mathematical Induction.

2. If a and b are integers we will say that a is *entangled with* b if there exist positive integers m and n with $a|b^m$ and $b|a^n$.

(a) Show that 12 is entangled with 6, but 12 is not entangled with 8.

(b) Give a description of the set of all integers entangled with 12.

(c) **Extra Credit**: Show that entanglement is transitive, that is, if a is entangled with b and b is entangled with c then a is entangled with c.

Answer: (a) $6|12^1$ and $12|6^2$; also $8|12^2$, but no power of 8 is a multiple of 12 because of the Fundamental Theorem of Arithmetic: 3 divides 12 but does not divide any power of 2.

(b) The numbers entangled with 12 are all the numbers of the form $n = 2^r 3^s$ with positive integers r and s. (Certainly $12|n^2$ and $n|12^{r+s}$ so these are all entangled with 12. No integer divisible by other primes is entangled with 12 since such an n cannot divide a power of 12 – the same FTA constraint. Likewise no integer divisible by fewer primes is entangled with 12 because 12 cannot divide a power of 2 nor a power of 3.

(c) If a is entangled with b and b is entangled with c then we have four positive integers p, q, r, s with $a|b^p, b|a^q, b|c^r, c|b^s$. But then $a|c^{pr}$ and $c|a^{qs}$, so a and c are entangled with each other.

In fact, (c) is just part of the proof of the statement that: entanglement is an equivalence relation. What the members of each equivalence class have in common is precisely the fact that they have the same prime divisors (to different multiplicities); (b) is an example of this.

3. Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ and let $f : S \to S$ be the function defined by the following table:

x:	1	2	3	4	5	6	7	8	9	10	11	12
$f(x)$:	6	4	9	11	12	10	1	7	5	8	2	3

Notice that f is one-to-one and onto, i.e. it is a permutation.

(a) Find a positive integer n so that the n-fold composite $f^{(n)} = f \circ f \circ f \circ \ldots \circ f$ is the identity function.

(b) Express f as a product of disjoint cycles.

Answer: (b) $f = (2\ 4\ 11)\ (3\ 9\ 5\ 12)\ (1\ 6\ 10\ 8\ 7)$.

(a) The order of f is thus the least common multiple of 3, 4, and 5 : f^{60} is the identity permutation.

This problem should help you recognize the power of Group Theory! Imagine how long it would have taken you to find that "60" just starting with f itself in (a)!

4. Suppose G is an *abelian* group. Let $H = \{x^2; x \in G\}$, that is, H is the set of squares of elements in G. Show that H is a subgroup of G.

(I will also give a little extra credit if you can show that in a non-abelian group G, the set H need not be a subgroup of G.)

Answer: Well $e = e^2$ is in H. And H is closed under inversion: if $h \in H$ is a square, say $h = x^2$, then $h^{-1} \in H$ too: it's the square of x^{-1}.

Products are just a bit more subtle: if $h, k \in H$ then each of them is a square, say $h = a^2, k = b^2$. But then $hk = a^2b^2 = aabb$; since G is abelian, this is equal to $abab = (ab)^2$; thus hk is a square too, and so it's in H.

In some nonabelian groups the result continues to be true. (For example, if $|G|$ is odd, then Lagrange's theorem can be used to show that *every* element is a square, i.e. $H = G$.) But in other (nonabelian) groups, the same set H is not a subgroup. For example, it's not hard to see that in the symmetric groups, the elements which are squares are those whose cycle decompositions include an even number of k-cycles for each even integer k. Thus e.g. $(12)(3456)$ is not a square. But it can be written as a product of squares, e.g. $((123)(456))^2 \cdot (14365)^2$.

5. If G is a group and $g \in G$, then we may define a function $f : G \to G$ by $f(x) = g^{-1}xg$.

(a) Show that f is an isomorphism.

(b) If g' is another element of G then f' may be similarly defined by $f'(x) = (g')^{-1}xg'$. Show that f and f' are the same functions iff g and g' lie in the same coset in $G/Z(G)$

Answer: (a) This f is a homomorphism because for all $x, y \in G$, $f(x)f(y) = g^{-1}xg \cdot g^{-1}yg = g^{-1}(xy)g = f(xy)$. It's also one-to-one and onto because there is an inverse function $h : G \to G$ defined by $h(x) = gxg^{-1}$.

(b) Two functions $G \to G$ are equal iff they produce the same output for every input $x \in G$. But $f(x) = f'(x)$ iff $g^{-1}xg = (g')^{-1}xg'$; multiplying by g' on the left and by g^{-1} on the right, we see this condition is equivalent to $(g'g^{-1})x = x(g'g^{-1})$, that is, it's equivalent to the statement that x commutes with $h = g'g^{-1}$. Thus, the statement that $f(x) = f'(x)$

for *all* $x \in G$ is equivalent to the statement that h lies in the center of G. But since $g' = hg$, this is in turn equivalent to the fact that the cosets $Z(G)g$ and $Z(G)g' = Z(G)hg$ are equal.

Remark: an isomorphism from a group to itself is called an *automorphism*; the collection of all automorphisms of G is a group called $Aut(G)$. The automorphisms described in this problem are called the *inner automorphisms*, and they form a subgroup of $Aut(G)$; this subgroup $Inn(G)$ is isomorphic to $G/Z(G)$. ($Inn(G)$ is also normal in $Aut(G)$; the quotient group $Aut(G)/Inn(G)$ is unsurprisingly but somewhat misleadingly called $Out(G)$, the group of outer automorphisms of G.)

6. Show that in the ring Z_{98}, 35 is a multiple of 77 . (The phrase "is a multiple of" has the same definition in any ring that it has in the ring of integers.)

Answer: $3 \cdot 77 = 231 = 35 + 2 \cdot 98$, so $[3]_{98} \cdot [77]_{98} = [35]_{98}$, making 35 be a multiple of 77.

How did I get this 3 ? Precisely what is needed is an element $x \in \mathbf{Z}_{98}$ for which $[77]x = [35]$, i.e. an integer X with $77X \equiv 35 \pmod{98}$, which in turn means there is a pair of integers X, Y with $77X = 35 + 98Y$. You might recognize this as a Bezout identity, so use the Euclidean Algorithm to find X, Y.

7. Suppose R is a (commutative) ring. Let N be the set of *nilpotent* elements, that is,

$$N = \{r \in R; r^k = 0 \text{ for some positive integer } k\}.$$

Show that N is an ideal of R.

Answer: The harder part, surprisingly, is to show that N is closed under the taking of sums and differences. But if $x, y \in N$ then there are integers k, m with $x^k = y^m = 0$. In that case, use the binomial theorem to expand a power $(x \pm y)^n = \sum b_{n,i} x^i y^{n-i}$; as long as $n \geq k + m - 1$ it must be true for every i that either $i \geq k$ or $n - i \geq m$, in which case either x^i or y^{n-i} is zero. (You might understand this example better if you tried expanding $(x + y)^5$ when $x^2 = y^3 = 0$.)

We also note that if $x^k = 0$ and $r \in R$ then $(rx)^k = r^k x^k = 0$ so $rk \in N$ too.

8. Let $R = \mathbf{Z}_2 \times \mathbf{Z}_3$, that is, R is the set of all ordered pairs (a, b) where $a \in \mathbf{Z}_2$ and $b \in \mathbf{Z}_3$. We can define addition and multiplication on R by doing the operations componentwise, that is, $(a, b) + (c, d)$ is defined to be $(a + c, b + d)$, and $(a, b) * (c, d)$ is defined to be $(a * c, b * d)$,

(a) List the six elements of R.

(b) Construct the addition and multiplication tables for R.

(c) Show that R is isomorphic to the ring Z_6. (Hint: You might want to think about what $\phi(1)$ has to be, where $\phi : \mathbf{Z}_6 \to R$ is the desired isomorphism.)

Answer: The elements of R are $a = ([0]_2, [0]_3), b = ([0]_2, [1]_3), c = ([0]_2, [2]_3), d = ([1]_2, [0]_3), e = ([1]_2, [1]_3), f = ([1]_2, [2]_3)$. You can compute their sums and products directly from the definition I gave in the problem; for example $e+f = ([1]_2, [1]_3)+([1]_2, [2]_3) = ([1]_2 + [1]_2, [1]_3 + [2]_3) = ([0]_2, [0]_3)$. Thus for example you quickly realize that a will be

the identity for addition, that addition in R is commutative, etc. Here are the resulting tables:

$+$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	e	f	a	b	c
e	e	f	d	b	c	a
f	f	d	e	c	a	b

$*$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	c	a	b	c
c	a	c	b	a	c	b
d	a	a	a	d	d	d
e	a	b	c	d	e	f
f	a	c	b	d	f	e

In particular, e is the identity element for multiplication. Since any homomorphism of rings takes 1 to 1, we would have to have $\phi([1]_6) = e = ([1]_2, [1]_3)$; but then ϕ is completely determined: $\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = e + e = c$, and likewise $\phi(3) = d, \phi(4) = b, \phi(5) = f$, and of course $\phi(0) = a$. If you reshuffle the rows and columns of the operation tables of R to match this, you will see the addition and multiplication tables of $\mathbf{Z}_6$ pop out!

More generally, if $\gcd(m,n)$=1, then the rings $\mathbf{Z}_{mn}$ and $\mathbf{Z}_m \times \mathbf{Z}_n$ are isomorphic; the isomorpism is given by $\phi([x]_{mn}) = ([x]_m, [x]_n)$. This leads to the *Chinese Remainder Theorem*.

EXTRA CREDIT: In an episode of Futurama, rebroadcast just last night, about a dozen characters have swapped their minds into each other's bodies, two people at a time, resulting in a very complex permutation. However, a quirk in the mind-swapping machine prevents it from working on any particular pair of bodies a second time. Fortunately the 30-th century Harlem Globetrotters make the claim that, no matter what the permutation, the minds can all be restored using the machine – despite this quirk – using at most two additional bodies (which are supplied by Curly Joe and Sweet Clyde Dixon).

Lrrr, ruler of the planet Omicron Persei Eight, commands you to interpret the situation in group-theoretic terms, state the Globetrotter claim as a conjecture, and prove it.

Answer: Maybe I should have set the stage a little better. (Sorry, I created this Extra Credit question after the show at about 3am!) The show's characters wish to reunite their minds with their bodies, but the obvious solution – swapping back the minds, one pair of bodies at a time, reversing the order of the original scrambling – is prohibited by the quirk of the machine. A new set of permutations is needed.

Mathematically, what we need is what I shall call the *Futurama Theorem*: every permutation in S_n may be written as a product of distinct transpositions (i.e. 2-cycles) (a,b) in S_{n+2} where either $b = n+1$ or $b = n+2$. (In particular, these transpositions do not lie in S_n, so the quirk of the machine will not stand in the way – these are pairs of bodies which have not swapped minds before; distinctness means that in addition, each of these new swaps involves a different pair of bodies.)

The proof is quite easy: first write the permutation in S_n as a product of disjoint cycles (as in problem 3b). Then write these cycles as products of transpositions using

$y = n + 1$ or $z = n + 2$ as one of their terms, and an entry from the cycle as their other term. Specifically, note that

$$(1\,y)(n\,z)(n-1\,z)\ldots(2\,z)(1\,z)(n\,y)$$

will equal $(123\ldots n)(yz)$. Similarly (with a change of labels) we can find a product of our special transpositions which is equal to any product $\sigma \cdot (y\,z)$ of a cycle in S_n with $(y\,z)$. Since $(y\,z)$ commutes with all these cycles, we can insert them into a product at will.

This is perhaps best explained by example. Consider the permutation of problem 3: $f = (2\ 4\ 11)\ (3\ 9\ 5\ 12)\ (1\ 6\ 10\ 8\ 7)$. We first write this as a product

$$f = (y\ z) \quad (2\ 4\ 11)(y\ z) \quad (3\ 9\ 5\ 12)(y\ z) \quad (1\ 6\ 10\ 8\ 7)(y\ z)$$

and then use the general pattern shown above for the three original cycles: $f =$

$$(y\,z)\ (2\,y)(11\,z)(4\,z)(2\,z)(11\,y)\ (3\,y)(12\,z)(5\,z)(9\,z)(3\,z)(12\,y)\ (1\,y)(7\,z)(8\,z)(10\,z)(6\,z)(1\,z)(7\,y)$$

I invite you to confirm that all the transpositions involved are distinct, that each involves either y or z (and so does not duplicate any of the transpositions used to create f in the first place), and of course that the product really equals f.

So it is easy to restore all the minds to all the right bodies; the total number of swaps needed is at most the number of moved minds, plus twice the number of cycles (orbits), plus 1. Once again, the genius Globetrotters have saved the day!

As I said on the exam, thanks for a great semester! I had a lot of fun and hope you did too.