MATH 435, EXAM #2

Your Name

- You have 50 minutes to do this exam.
- No calculators!
- No notes!
- For proofs/justifications, please use complete sentences and make sure to explain any steps which are questionable.
- Good luck!

Problem	Total Points	Score
1	30	
2	26	
3	24	
4	20	
EC	10	
Total	100	

1. Definitions and short answers.
(a) If a group G is acting on a set X, give a precise definition of $\mathrm{Orb}_G(x)$ (in particular, what does the term x denote). (5 points)

Solution: In this case, x is an element of X. Thus $\mathrm{Orb}_G(x) = \{g.x \in X | g \in G\}$ (here I'm assuming a left group action).

(b) Give an example of a group G acting on a set X and an element $y \in X$ such that $\mathrm{Stab}_G(y)$ has 3 elements. (5 points)

Solution: Consider $\mathbb{Z}_{\mathrm{mod}3}$ acting on the set $\{\pi\}$ where $n.\pi = \pi$ for all $n \in \mathbb{Z}_{\mathrm{mod}3}$. Then every element stabilizes π.

(c) Give an example of a non-commutative ring which is not the ring of 2×2 matrices. (5 points)

Solution: The quaternions or 3×3 matrices spring to mind.

(d) Compute $(12)(243)(13)$ and $(123)(234)$ in S_4. (5 points)

Solution: $(12)(243)(13) = (243)$. Also $(123)(234) = (12)(34)$.

(e) Suppose that $\varphi : R \to S$ is a ring homomorphism. Prove that the kernel of φ is an ideal. (5 points)

Solution: We already know that $\ker \varphi$ is a subgroup of R under $+$, so we just need to show it is closed under arbitrary multiplication from R. Indeed, take $r \in R$ and $x \in \ker \phi$. Then $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0$ and so $rx \in \ker \varphi$. This completes the proof.

(f) Give two equivalent definitions of a *maximal ideal* in a commutative ring with unity. (5 points)

Solution: A proper ideal I is called maximal if R/I is a field.
A proper ideal I also called maximal if any ideal $J \supseteq I$ automatically satisfies $J = I$ or $J = R$.

2. First we start with an arbitrary ring R with unity.

(a) Show that the set of invertible elements of R form a group under multiplication (7 points).

Solution: First we show that multiplication is closed. If $a, b \in R$ are invertible, then ab is also invertible with inverse $b^{-1}a^{-1}$.

Associativity follows immediately from the fact that multiplication in R is always associative. The existence of the identity is immediate since identity is certainly invertible (it is its own inverse). The elements of this group are invertible by definition as well.

(b) Now consider the ring $R = \mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$. Show that $1, -1, i, -i$ are invertible elements in R which form a group G under multiplication (in fact, these are the only invertible elements, but you need not prove that fact now). (7 points)

Solution: The elements are invertible since these are the subgroup of the group of invertible elements of R which are in the cyclic subgroup generated by i. Notice that $\{i, i^2 = -1, i^3 = -i, i^4 = 1\}$ form a cyclic group.

(c) With notation as in (b), prove that the group of invertible elements $G = \{1, -1, i, -i\}$ acts on $R = \mathbb{Z}[i]$ by multiplication: $g.f = gf$ for $g \in G$ and $f \in R = \mathbb{Z}[i]$. (6 points).

Solution: We consider our action, $i^k.f = i^k f$. Of course, $1.f = i^4.f = 1f = f$. Notice that $i^j.(i^k.f) = i^j i^k f = (i^{j+k})f = (i^{j+k \bmod 4})f = (i^{j+k \bmod 4}).f = (i^j i^k).f$ which is all we need. One can do this more painfully of course too.

(d) Consider the group $G = \{1, -1, i, -i\}$ acting on $R = \mathbb{Z}[i]$ by multiplication. Find $\mathrm{Orb}_G(7)$ and $\mathrm{Stab}_G(7)$. (6 points)

Solution: $\mathrm{Orb}_G(7) = \{7, -7, 7i, -7i\}$. $\mathrm{Stab}_G(7) = \{1\} \subseteq G$.

3 Suppose that R and S are rings and R has unity.

(a) If $\varphi : R \to S$ is a surjective ring homomorphism. Prove that $\varphi(1_R) = 1_S$ (implicitly, you have just proven that S also has unity). (12 points)

Solution: We will show that $\varphi(1_R)$ is a multiplicative identity for S. Choose $s \in S$, then there exists $r \in R$ such that $\varphi(r) = s$. Then we notice that

$$s\varphi(1_R) = \varphi(r)\varphi(1_R) = \varphi(r1_R) = \varphi(r) = s$$

and likewise that

$$\varphi(1_R)s = \varphi(1_R)\varphi(r) = \varphi(1_R r) = \varphi(r) = s.$$

This completes the proof.

(b) Suppose that R is a field and $\psi : R \to S$ is a non-zero[1] ring homomorphism. Prove that ψ is injective. (12 points)

Hint: The kernel of ψ is an ideal...

Solution: Note $\ker \psi$ is an ideal in a field, so it must be either equal to $\{0\}$ or R. If it is equal to R, then ψ is the zero map, which contradicts our assumptions, thus $\ker \psi$ is the zero ideal. But then by viewing ψ just as a map of (additive) groups, we see that ψ is injective and this completes the proof.

[1] In other words there is at least one $r \in R$ such that $\psi(r) \neq 0_S$.

4. Prove that every finite field has p^n elements for some prime p and integer n using Cauchy's theorem. (20 points)

Solution: We prove this in two steps:

(a) There exists a prime p such that $pa = 0$ for all $a \in F$.

(b) If F has q elements, then $q = p^n$ for some integer n.

First we prove (a). We let $n = |F|$. By Lagrange's theorem, we know $na = 0$ for all $a \in F$. Let p be the smallest positive integer such that $p(1) = 0$ where 1 is the multiplicative identity of F. We will prove that p is prime so suppose that $p = nm$ is composite with $n, m > 1$. Then

$$0 = nm(1) = (n1)(m1).$$

Since every field is an integral domain, we thus know $n1 = 0$ or $m1 = 0$. But either leads to a contradiction since p is the smallest integer such that $p1 = 0$. Thus p is prime. But now if $p1 = 0$, then we notice that $px = (p1)(x) = 0x$ for any $x \in R$ and so $px = 0$ for all $x \in R$ which completes the proof.

Now we prove (b). Suppose that $|F| = q$. Now, we know that the p from part (a) divides q by Lagrange's theorem. On the other hand, if any other prime $p' \neq p$ divides q, then by Cauchy's theorem for the additive group of F, F contains an element y of order p'. Then $p'y = 0$. But we also know that $px = 0$ and so p divides the order of x (which is p' by assumption). But this is clearly impossible since p and p' are distinct primes.

(EC) Suppose that R is an integral domain with unity. We declare two pairs $(a,b),(c,d) \in R \times R$ (with $b \neq 0, d \neq 0$) to be equivalent, $(a,b) \sim (c,d)$ if $ad = cb$. Consider the set of all equivalence classes of pairs

$$S = \{[(a,b)] \,|\, a,b \in R, b \neq 0\}.$$

We define a multiplication in S by $[(a,b)] \cdot [(a',b')] = [(aa',bb')]$ and we define addition by $[(a,b)] + [(a',b')] = [(ab'+ba',bb')]$. Prove that these operations are well defined and also that S is a field with those operations. (10 points)

Solution: This is extra credit due on Monday the 9th...