Abstract Algebra | FINAL EXAM | May 23, 2003

Name: ____________________ R. Hammack Score: ________

Directions: Please answer the questions in the space provided. To get full credit you must show all of your work. Use of calculators and other computing or communication devices is **not** allowed on this test.

---

1. Draw the subgroup lattice for $\mathbb{Z}_{18}$.

$$\begin{tikzcd}
& \mathbb{Z}_{18} \arrow[dl] \arrow[dr] & & \\
\langle 2\rangle \arrow[dr] & & \langle 3\rangle \arrow[dl] \arrow[dr] & \\
& \langle 6\rangle \arrow[dr] & & \langle 9\rangle \arrow[dl] \\
& & \langle 0\rangle &
\end{tikzcd}$$

2. List the elements of the cyclic subgroup $\langle$-i$\rangle$ of $\mathbb{C}^*$. Answer: $1, -i, -1, i$

3. Find the order of the largest cyclic subgroup of the symmetric group S_{10}.
Consider the element (1,2,3,4,5)(6,7,8)(9,10).
It has order $(5)(3)(2) = 30$, so the subgroup generated by it has 30 elements.
Can you do better than this? Any permutation in S_{10} can be written as a product of disjoint cycles, and its order is at most the sum of the lengths of the cycles. A quick exhaustive search confrims that the above element has the greatest possible order.

4. Consider the set $H = \{\sigma \in S_5 \mid \sigma(3)=3\}$.

   (a) $|H| = 4! = \mathbf{24}$

   (b) Explain why H is a subgroup of S_5.

   Note that
   1. H is closed. If π, $\mu \in H$, then $\pi(3)= 3$ and $\mu(3)= 3$. Thus $\pi\mu(3) = \pi(\mu(3)) = \pi(3) = 3$, so $\pi\mu \in H$.
   2. The identity permutatio i is in H because $i(3) = 3$.
   3. If $\mu \in H$, then $3 = \mu(3)$, so $\mu^{-1}(3) = \mu^{-1}\mu((3)) = 3$, which means μ^{-1} is in H.
   It follows that H is a subgroup.

   (c) Is H a normal subgroup of S_5? Explain.

   NO.
   For example, look at the cycle (1,2,4), which is in H because it leaves 3 unchanged.
   Cosnsider the permutation (1,3) which is its own inverse.
   Notice that (1,3)(1,2,4)(1,3) is NOT in H because it sends 3 to 2.
   This shows that its not true that $g^{-1}hg$ is H for every element h in H, so H is not normal.

   (d) How many left cosets of H are there in S_5?

   There are $|S_5|/|\ H| = 120/24 = 5$ such cosets.

5. List all the nonisomorphic groups of order 180.
   $180 = 2^2 3^2 5$

   $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
   $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
   $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
   $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

6. Find the order of (3,6,9) in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.

   Look at $n(3, 6, 9) = (n3, n6, n9)$, where n is an integer.
   n must be a multible of 4 to make $n3 = 0$
   n must be a multible of 2 to make $n6 = 0$
   n must be a multible of 5 to make $n9 = 0$

   The least common multiple is 20, so that is the order of (3, 6, 9).

7. Are the groups $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_3$ and $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{15}$ isomorphic? Why or why not?

   $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_3 = \mathbb{Z}_8 \times \mathbb{Z}_{30}$ (since 3 and 10 are relatively prime)
   $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{15} = \mathbb{Z}_8 \times \mathbb{Z}_{30}$ (since 2 and 15 are relatively prime)
   Therefore the two groups are isomorphic.

8. Find the kernel of the homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}_8$ for which $\phi(1)=6$.

   Note $\phi(n) = \phi(1+1+...+1) = \phi(1)+\phi(1)+..+\phi(1) = 6+6+...+6 = 6n \pmod 8$
   Thus the kernel will be all integers n for which $6n = (3)(2)n$ is a multiple of 8.
   Such an n must be a multiple of 4.
   Thus kernel is $4\mathbb{Z}$.

9. Find the kernel of the homomorphism $\phi: \mathbb{Z}_{40} \to \mathbb{Z}_5 \times \mathbb{Z}_8$ for which $\phi(1)=(1,4)$.

   Note $\phi(n) = \phi(1+1+...+1) = \phi(1)+\phi(1)+..+\phi(1) = n(1,4) = (n, 4n)$
   For this equal (0,0), n must be a multiple of 5 and $4n$ must be a multiple of 8.
   It follows that the kernel is $\{0, 10, 20, 30\}$

10. (a) List the units in the ring $\mathbb{Z}_{12}$.

    1, 5, 7, 11

    (b) List the zero divisors in the ring $\mathbb{Z}_{12}$.

    2, 3, 4, 6, 8, 9, 10

    (c) List the prime ideals in the ring $\mathbb{Z}_{12}$.

    Recall that an ideal N is prime if and olly if $\mathbb{Z}_{12}/N$ is an integral domain.
    The ideals in this ring are $\langle 0 \rangle$, $\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$, $\langle 2 \rangle = \langle 10 \rangle$, $\langle 3 \rangle = \langle 9 \rangle$, $\langle 6 \rangle$, $\langle 4 \rangle = \langle 8 \rangle$.

    $\mathbb{Z}_{12}/\langle 0 \rangle \cong \mathbb{Z}_{12}$ is not an integral domain so $\langle 0 \rangle$ is not prime.
    $\mathbb{Z}_{12}/\langle 1 \rangle \cong \{0\}$ is not an integral domain so $\langle 1 \rangle$ is not prime.
    $\mathbb{Z}_{12}/\langle 2 \rangle \cong \mathbb{Z}_2$ is an integral domain so $\langle 2 \rangle$ is prime.
    $\mathbb{Z}_{12}/\langle 3 \rangle \cong \mathbb{Z}_4$ is not an integral domain so $\langle 3 \rangle$ is not prime.
    $\mathbb{Z}_{12}/\langle 4 \rangle \cong \mathbb{Z}_3$ is an integral domain so $\langle 4 \rangle$ is prime.
    $\mathbb{Z}_{12}/\langle 6 \rangle \cong \mathbb{Z}_6$ is not an integral domain so $\langle 6 \rangle$ is not prime.

    Prime ideals are $\langle 2 \rangle$ and $\langle 4 \rangle$.

11. What familiar group is $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle$ (2,3) $\rangle$ isomorphic to?

Note $H = \langle(2,3)\rangle = \{$(0,0), (2,3)$\}$ has just 2 elements.
It follows that the factor group has $(4)(6)/2 = 12$ elements.
We claim that the factor group is generated by the element (1, 1)+ H.
0((1, 1)+ H) = (0, 0)+ H
1((1, 1)+ H) = (1, 1)+ H
2((1, 1)+ H) = (2, 2)+ H
3((1, 1)+ H) = (3, 3)+ H
4((1, 1)+ H) = (0, 4)+ H
5((1, 1)+ H) = (1, 5)+ H
6((1, 1)+ H) = (2, 0)+ H
7((1, 1)+ H) = (3, 1)+ H
8((1, 1)+ H) = (0, 2)+ H
9((1, 1)+ H) = (1, 3)+ H
10((1, 1)+ H) = (2, 4)+ H
11((1, 1)+ H) = (3, 5)+ H
12((1, 1)+ H) = (0, 0)+ H <—— *finally "cycles" back to the identity here.*

Thus (1, 1)+ H generates the entire group. Group is cyclic with 12 elements. It's $\mathbb{Z}_{12}$.

12. Explain why $\mathbb{C}^*/\text{U} \simeq \mathbb{R}^+$.

Consider the function $\phi : \mathbb{C}^* \to \mathbb{R}^+$, given by $\phi(z) = |z|$.
This is a homomorphism becuase $\phi(zw) = |zw| = |z||w| = \phi(z)\phi(w)$.
It's surjective because given any x in $\mathbb{R}^+$, $\phi(x) = x$.
Also, its Kernel is $\{z \in \mathbb{C}^* : \phi(z) = 1\} = \{z \in \mathbb{C}^* : |z| = 1\} = U$.
By the Fundamental Theorem of Homomorphisms, there is an isomorphism $\mu : \mathbb{C}^*/U \to \mathbb{R}^+$.

13. Is $2x^3+x^2+$ 2x +2 an irreducible polynomial in $\mathbb{Z}_5$[x]? If not, write it as a product of irreducible polynomials.

Let $f(x) = 2x^3+x^2+$ 2x +2.
If this factored, then it would factor into a linear and a quadratic term, or 3 linear terms.
Either way, there would be a linear term, so the polynomial would have a root.
But a quick check shows there are no roots:
$f(0) = 2$
$f(1) = 2$
$f(2) = 1$
$f(3) = 1$
$f(4) = 4$
Conclusion. It can't be factored. It's irreducible.

14. Find all $c \in \mathbb{Z}_3$ for which $\mathbb{Z}_3$[x]/$\langle$ x^2+c $\rangle$ is a field.

These would be all the elements c for which the ideal $\langle x^2 + c\rangle$ is maximal,
which in turn is all elements c for which x^2+c is irrecucible.
If c = 0, the polynomial is x^2= $(x)(x)$ which is not irreducible.
If c = 1, the polynomial is x^2+1, and its of degree 2 with no roots, so its irreducible.
If c = 2, the polynomial is x^2+2, and its of degree 2 with no roots, so its irreducible.

ANSWER: $c = 1$ and $c = 2$.

15. Prove that if G is a finite group with identity e, and $m = |G|$, then $x^m = e$ for any element $x \in G$.

Proof. Take any x in G and consider the cyclic subgroup $\langle x\rangle$.
Let's say $k = |\langle x\rangle|$, which means $\langle x\rangle = \{e, x, x^2, x^3, x^4, \cdots, x^{k-1}\}$, so $x^k = e$.
Lagrange's Theorem says k divides m, so $m = kn$ for some integer n.
Now, $x^m = x^{kn} = \left(x^k\right)^n = e^n = e$.

16. Suppose that G is a group with identity e. Prove that if $x^2 = e$ for every element x in G, then G is abelian.

Proof.
Suppose a and b are arbitrary elements of G.
We want to show $ab = ba$.
By hypothesis, $(ab)^2 = abab = e$.
Multiply both sides of $abab = e$ on the left by a and you get $aabab = a$.
But, since $aa= e$, this becomes $bab = a$.
Now multiply both sides of $bab = a$ on the right by b to get $babb = ab$.
But since $bb = e$ this becomes $ba = ab$.
Therefore G is abelian.

17. Prove that if G is an abelian group, then the set of all elements $x \in G$ for which $x^2 = e$ form a subgroup of G.

Proof. Let $H = \{x \in G | x^2 = e\}$. We must show this is a subgroup of G.
Notice that:
1. H is closed. If $a, b \in H$, then $a^2 = e$ and $b^2 = e$, so $(ab)^2 = abab = aabb = a^2b^2 = ee = e$, so ab is in H.
2. The identity e is in H because $e^2 = e$.
3. If a is in H, then $a^2 = e$ so $\left(a^2\right)^{-1} = e^{-1}$, which is $a^{-2} = e$, or $\left(a^{-1}\right)^2 = e$. This means a^{-1} is in H.

18. Prove that the units of a ring with unity form a multiplicative group.

Proof. Suppose R is a ring with unity and M⊂R is the set of all its units.
Notice that M is closed under multiplication, for if a and b are in M then ab is a unit with inverse $b^{-1}a^{-1}$.
Thus ring multiplication gives a binary operation on M.
We now just need to show the 3 group axioms hold for multiplication in M.
1. Multiplication is assosiative because it's assosiative in the ring R.
2. Unity 1 is in M because it's a unit, and this serves as the identity.
3. If a is in M, then a is a unit and so is its inverse because $aa^{-1} = 1$, so a^{-1} is in M.
We're done.