Math 30710
Practice Final Exam 2
December, 2017 **Name** ____________________

This is a 2-hour exam. Books and notes are not allowed. Make sure that your work is legible, and make sure that it is clearly marked where your answers are. **Show all work!** If a problem calls for a proof or explanation, you will not get full credit for a correct answer if you don't supply the proof or explanation. If you have some ideas for solving a problem but can't figure out how to finish it, be sure to show me what you do know!! If something is not clear, ASK ME!! Good luck!

1. Let φ be the Euler phi-function, namely $\varphi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

   (a) (5 points) Compute $\varphi(18)$ and put your answer in the provided space.

   $\boxed{\varphi(18) = 6}$

   The numbers relatively prime to 18 are $1, 5, 7, 11, 13, 17$ so $\varphi(18) = 6$

   (b) (10 points) If p is a prime, compute $\varphi(p^2)$ and carefully explain your answer. [Note that this is asking for $\varphi(p^2)$, not $\varphi(p)$. A correct answer with no explanation will not get full credit.]

   The numbers not relatively prime to p^2 are $p, 2p, \dots, p^2$. There are p of them. So $\varphi(p) = p^2 - p = p(p-1)$.

   (c) (5 points) State Euler's theorem (the generalization of Fermat's Little Theorem). Be sure to include all the hypotheses.

   Let n be a positive integer. Let $a \in \mathbb{Z}$ be relatively prime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$. Equivalently, $a^{\varphi(n)} - 1$ is divisible by n.

   (d) (10 points) Find the remainder of $7^{123,322}$ when divided by 11 and put your answer in the provided space.

   Answer:

   Since 11 is prime we can use Fermat's Little theorem (or Euler works too). We have $7^{10} \equiv 1 \pmod{11}$. So

   $$7^{123322} = (7^{10})^{12332} \cdot 7^2 \equiv 49 \equiv 5 \pmod{11}$$

   So the remainder is 5.

2. Consider the symmetric group S_6 and its subgroup, the alternating group A_6. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}.$$

(a) (5 points) Give the orders of S_6 and of A_6 and put your answers in the provided space.

$\boxed{|S_6| = 6! = 720}$ $\boxed{|A_6| = 360}$

(b) (5 points) Write σ as a product of disjoint cycles.

$(1,6)(2,5,3)$

(c) (5 points) Write σ as a product of transpositions.

$(1,6)(2,3)(2,5)$

(d) (5 points) Is $\sigma \in A_6$? Explain why or why not.

No because it is the product of an odd number of transpositions

(e) (10 points) Find the order of σ and put your answer in the provided space.

$\boxed{\textbf{Answer:}\ 6}$

since $\sigma = (1,6)(2,5,3)$ (disjoint)

$\text{ord}(\sigma) = \text{lcm}(2,3) = 6$

3. YOU CAN DISREGARD THIS PROBLEM! Consider the polynomial $f(x) = 2x^2 + x + 1$ in $\mathbb{Z}_7[x]$.

   (a) (10 points) How do you know that $f(x)$ is **not** irreducible over $\mathbb{Z}_7$ before you even try to factor it?

   (b) (10 points) Factor $f(x)$. (Remember that the field is $\mathbb{Z}_7$. Your work in (a) should help.)

4. (10 points) We know that a factor group of a cyclic group is cyclic. Is it also true that a factor group of a *non-cyclic* group is non-cyclic? If it's true, give a proof. If it's not true, give a counterexample.

No. $G = S_5$, $H = A_5$

Since $|H| = \frac{1}{2}|G|$, A_5 is a normal subgroup and $|G/H| = 2$.

So $G/H \cong \mathbb{Z}_2$, which is cyclic. But G is not cyclic.

5. Let F be the additive group of all continuous functions mapping $\mathbb{R}$ to $\mathbb{R}$. Let $\mathbb{R}$ be the additive group of real numbers. Let $\phi : F \to \mathbb{R}$ be given by

$$\phi(f) = \int_{-1}^{1} f(x)dx.$$

(a) (10 points) Prove that ϕ is a group homomorphism.

$\phi(f+g) = \int_{-1}^{1} (f+g)(x)\,dx = \int_{-1}^{1} f(x)dx + \int_{-1}^{1} g(x)\,dx = \phi(f) + \phi(g)$

(b) (5 points) Give an example of a non-zero element in $\ker \phi$.

$\phi(f) = 0$ if $\int_{-1}^{1} f(x)dx = 0$. The easiest example is $f(x) = x$

but you can find plenty of others.

(c) (5 points) To what familiar group is $F/\ker\phi$ isomorphic? Justify your answer.

We know $\phi : F \to \mathbb{R}$ and $F/\ker(\phi) \cong \phi[F] \subseteq \mathbb{R}$. So we need to find $\phi[F]$. For which real numbers r is it true that there exists $f \in F$ with $\int_{-1}^{1} f(x)dx = r$? Clearly any real number works. So $F/\ker\phi \cong \mathbb{R}$.

6. (10 points) Let G be a group of finite order n and let $g \in G$. Prove that $g^n = e$, where e is the identity element of G. [Hint: use Lagrange's theorem.]

Let $H = \langle g \rangle$. Let $m = \mathrm{ord}(g)$. Then $|H| = m$ divides $|G| = n$. Say $n = ml$.

Then $g^n = g^{ml} = (g^m)^l = e^l = e$.

7. Let $\phi : \mathbb{R}[x] \to \mathbb{R}$ be defined by $\phi(f) = f(3)$.

   (a) (10 points) Prove that ϕ is a **ring** homomorphism. (You can take for granted that $\mathbb{R}[x]$ and $\mathbb{R}$ are rings.)

$$\phi(f+g) = (f+g)(3) = f(3) + g(3) = \phi(f) + \phi(g)$$

$$\phi(fg) = (fg)(3) = f(3)g(3) = \phi(f)\phi(g)$$

   (b) (10 points) Give a geometric interpretation of $\ker \phi$ in terms of the graphs of the elements of $\mathbb{R}[x]$ (i.e. how can you tell from the graph of a polynomial $y = f(x)$ that $f \in \ker \phi$?).

$\ker \phi = \{ f \in \mathbb{R}[x] \mid \phi(f) = 0 \}$

$= \{ f \in \mathbb{R}[x] \mid f(3) = 0 \}$

$= \{ f \in \mathbb{R}[x] \mid$ the graph of f in $\mathbb{R}^2$ passes through the point $(3,0) \}$

8. (10 points) Let G be a group and let H be a subgroup of G (not necessarily normal). Let a, b be elements of g such that $aH = bH$. Prove that $Ha^{-1} = Hb^{-1}$.

We are assuming that $aH = bH$, ie that $a^{-1}b \in H$.

Claim? $Ha^{-1} \subseteq Hb^{-1}$

Let $x \in Ha^{-1}$. WTS $x \in Hb^{-1}$. ie $\boxed{\text{WTS } xb \in H.}$

By assumption $\exists\ h_1 \in H$ such that $x = h_1 a^{-1}$

Then $xb = (h_1 a^{-1}) b = h_1 (a^{-1} b)$

We know $h_1 \in H$ and $a^{-1}b \in H$ so the product is in H since H is a subgroup. That is, $xb \in H$ as desired.