Math 30710
Practice Final Exam 1
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 isn't clear, ask me! If you need more space, there is a blank sheet at the back.

The Honor Code is in effect for this examination, including keeping your own exam under cover. 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 $\varphi(20)$. Explain your answer.

   The relatively prime numbers are $\{1, 3, 7, 9, 11, 13, 17, 19\}$ so $\varphi(20) = 8$

   (b) (10 points) If p is a prime number, find $\varphi(p^2)$ and carefully explain your answer.

   The numbers that are not relatively prime are $\{p, 2p, 3p, \ldots, p^2\}$. ($p$ of them)
   All the numbers from 1 to p^2 are $\{1, 2, \ldots, p^2\}$ (p^2 of them)
   So $\varphi(p^2) = p^2 - p = p(p-1)$

   (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 $a^{\varphi(n)} \equiv 1 \pmod{n}$. (Alt: ... Then $a^{\varphi(n)} - 1$ is divisible by n.)

   (d) (10 points) It happens to be true that $\varphi(30) = 8$. (You don't have to prove this.) Find the remainder of 13^{2018} when divided by 30. Explain your answer using Euler's theorem. (Writing the answer with no justification will not get credit.)

   Since 13 is relatively prime to 30 we can use Euler. We know $13^8 \equiv 1 \pmod{30}$. Since $2018 = 252(8) + 2$ we have

   $$13^{2018} = (13^8)^{252} \cdot 13^2 \equiv 13^2 = 169 \equiv 19 \pmod{30}$$

2. (10 points) Let $G = \langle a \rangle$ be a cyclic group (not necessarily finite) and let G' be another group (not necessarily finite or abelian). If $\phi : G \to G'$ is a group homomorphism, prove that $\phi[G]$ is cyclic and in the process specify a generator of $\phi[G]$.

Let $b \in \phi[G]$. So $b = \phi(x)$ for some $x \in G$. But $G = \langle a \rangle$ is cyclic, so $x = a^m$ for some $m \in \mathbb{Z}$. Then $b = \phi(x) = \phi(a^m) = \phi(a)^m$. Since $b \in \phi[G]$ was an arbitrary element, $\phi[G] = \langle \phi(a) \rangle \subset G'$.

3. (10 points) Assume that G is a **finite** group (not necessarily abelian), and let G' be another group (not necessarily finite or abelian). Let $b \in G$ be any element and let $x = \phi(b)$. Prove that the order of x in G' divides $|G|$. [Notice that you are to prove that the order of x divides $|G|$, not $|G'|$.]

[Sorry, the problem should have said that $\phi: G \to G'$ is a homomorphism. This is a great example of a question you should ask me during the exam!]

$x = \phi(b) \in \phi[G]$ which is a subgroup of G', so the order of x divides $|\phi[G]|$. On the other hand, $G/\ker(\phi) \cong \phi[G]$ and $|G| < \infty$, so $|\phi[G]| = |G|/|\ker(\phi)|$ divides $|G|$. Then combining, $\operatorname{ord}(x) \mid |G|$.

4. Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ be the group homomorphism defined by $\phi(1) = 8$. (You do not have to verify that this really gives a well-defined homomorphism.)

(a) (5 points) Find $\ker \phi$.

$\mathbb{Z}_{10} = \langle 1 \rangle = \{1, 2, \ldots, 9, 0\}$. $\phi(1) = 8$ $\phi(2) = 16, \ldots$ so

$\ker(\phi) = \{x \in \mathbb{Z}_{10} \mid \phi(x) = 0\} = \{0, 5\}$.

(b) (5 points) Find $\phi[\mathbb{Z}_{10}]$.

$\phi[\mathbb{Z}_{10}] = \{8, 16, 4, 12, 0\}$

(c) (5 points) Find $\phi(6)$.

$\phi(6) = \phi(1+1+1+1+1+1) = 8+8+8+8+8+8 = 8$ in $\mathbb{Z}_{20}$

5. Consider the symmetric group S_{12} and the alternating group A_{12}. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 11 & 5 & 10 & 8 & 2 & 4 & 7 & 1 & 12 & 9 & 3 \end{pmatrix}$$

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

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

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

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

(c) (5 points) Is $\sigma \in A_{12}$? Explain why or why not.

yes since σ is a prod. of an even number of transpositions

(d) (5 points) Find the order of σ and briefly explain your answer.

$\operatorname{ord}(\sigma) = \operatorname{lcm}(5,7) = 35$

(e) (5 points) It turns out that σ does not have the highest possible order among elements of S_{12}. Give an example of a permutation in S_{12} whose order is higher (i.e. larger) than that of σ; write your answer as a product of disjoint cycles.

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

order $= \operatorname{lcm}(2,3,7) = 42$

6. Let R be a ring and let $R[x]$ be the polynomial ring with coefficients in R. For the following two parts you can use without proof the fact that $x^d \cdot x^e = x^{d+e}$ for any non-negative integers d and e. (This has nothing to do with the ring in question.)

   (a) (10 points) First assume that R is **not** an integral domain. Choose a suitable R and give an example in the spaces below of polynomials $f, g \in R[x]$, such that

   (i) $\deg f = d > 0$,
   (ii) $\deg g = e > 0$, and
   (iii) $\deg fg \neq d + e$.

   $R = \mathbb{Z}_{12}$ $\quad d = 2$ $\quad e = 2$

   $f = 2x^2 + 1$ $\quad g = 6x^2 + 1$

   $fg = (2x^2+1)(6x^2+1) = 0x^4 + 2x^2 + 6x^2 + 1 = 8x^2 + 1$

   $\deg fg = 2 \neq 4$

   (b) (5 points) Now assume that R is an integral domain. Prove that $R[x]$ is also an integral domain. (Hint: why is the result of (a) impossible when R is an integral domain?)

   Let $f = a_0 + a_1 x + \cdots + a_d x^d$ and $g = b_0 + b_1 x + \cdots + b_e x^e$, where $a_d \neq 0$, $b_e \neq 0$. Then $fg = (a_0 b_0 + \cdots + a_d b_e x^{d+e})$. Since R is an integral domain, $a_d b_e \neq 0$. Therefore $fg \neq 0$. Since f and g were arbitrary, R is an integral domain.

7. (15 points) Let $R = \mathbb{Z}_6[x]$, the polynomial ring with coefficients in $\mathbb{Z}_6$. Which of the following statements are true for R? For each statement, give a short justification of your answer (i.e. if the answer is yes, explain why; if the answer is no, explain why not).

   - R is a ring with unity? Yes, $1 \in \mathbb{Z}_6[x]$ is a poly. with coefficients in $\mathbb{Z}_6$
   - R is a commutative ring? Yes, since $\mathbb{Z}_6$ is a commutative ring.
   - R is an integral domain? No, since $(2x)(3x) = 0$
   - R is a finite ring? No, since polynomials can have arbitrarily large degree.
   - R contains no units? No, since $1 \in R$.

8. Compute the factor group $(\mathbb{Z}_8 \times \mathbb{Z}_8)/\langle(2,4)\rangle$ as follows.

(a) (5 points) Write out the elements of $\langle(2,4)\rangle$.

$\langle(2,4)\rangle = \{(2,4), (4,0), (6,4), (0,0)\}$

(b) (5 points) How many elements does the factor group have?

$\frac{64}{4} = 16$

(c) (10 points) Up to isomorphism, what are *all* the possible finite abelian groups with the order you gave in (b)?

$\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

(d) (10 points) To which of the answers from (c) is the given factor group isomorphic? Explain.

Let $H = \langle(2,4)\rangle$.

Rule out:
- $\mathbb{Z}_{16}$ since even $\mathbb{Z}_8 \times \mathbb{Z}_8$ has elements of order at most 8 so the same is true of a factor group
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ since $(1,1) + H$ has order 8
- $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ for the same reason

So the answer is $\mathbb{Z}_2 \times \mathbb{Z}_8$.