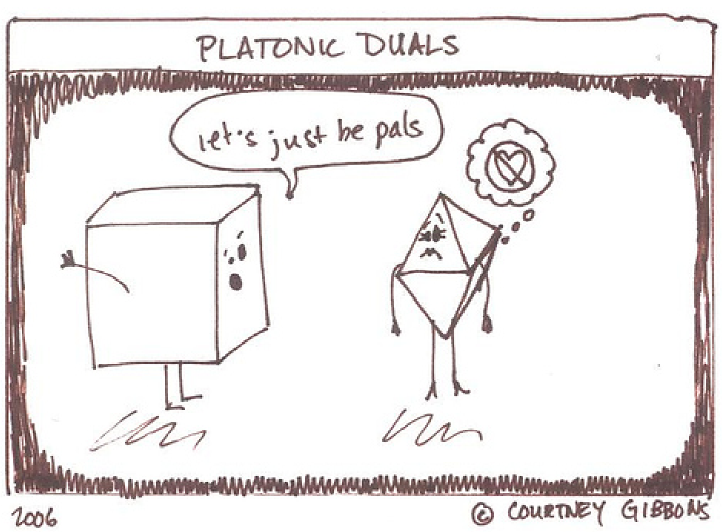
Friday 04/22/2016 Midterm III 50 mins

Name: [ ] Student ID: [ ]

Instructions.

1. Attempt all questions.
2. Do not write on back of exam sheets. Extra paper is available if you need it.
3. Show all the steps of your work clearly.

Question	Points	Your Score
Q1	20	
Q2	20	
Q3	20	
Q4	40	
TOTAL	100	



Miscellaney.

1. **Theorem (Fermat's Little Theorem).** Let p be a prime number and let a be a nonzero element of $\mathbb{Z}_p$. Then
$$a^{p-1} \equiv 1 \mod p.$$

2. **Chinese Remainder Theorem.** Let $m_1, \ldots, m_k$ be pairwise relatively prime natural numbers. The system of simultaneous linear congruences
$$x \equiv a_1 \mod m_1\,, \quad \ldots \quad , x \equiv a_k \mod m_k$$
has a unique solution $\mod M$, where $M = m_1 \ldots m_k$.
This solution is found as follows. Let $z_i = M/m_i$ and note that for each i the congruence
$$z_i y_i \equiv 1 \mod m_i$$
has a solution y_i (because $\gcd(z_i, m_i) = 1$). Now a solution to the simultaneous congruences is found by
$$x = a_1 y_1 z_1 + \cdots + a_k y_k z_k$$

3. **Definition (Group).** A *group* consists of a set G and a binary operation $\circ : G \times G \to G : (g,h) \mapsto g \circ h$ which satisfies the following properties.
   (a) **Associativity.** For all $g, h, k \in G$ we have
   $$(g \circ h) \circ k = g \circ (h \circ k)$$
   (b) **Identity.** There is an element $e \in G$ such that
   $$e \circ g = g \circ e = g$$
   for all $g \in G$.
   (c) **Inverses.** For every $g \in G$ there exists $g^{-1} \in G$ such that
   $$g \circ g^{-1} = g^{-1} \circ g = e$$

   Note that the *closure* property is included in the definition of a binary operation as being a function from $G \times G$ with values in G.

Q1]... [20 points] Solve the following system of congruences. Show the details of your work.

$$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 2 \mod 9 \\ x &\equiv 3 \mod 5 \end{aligned}$$

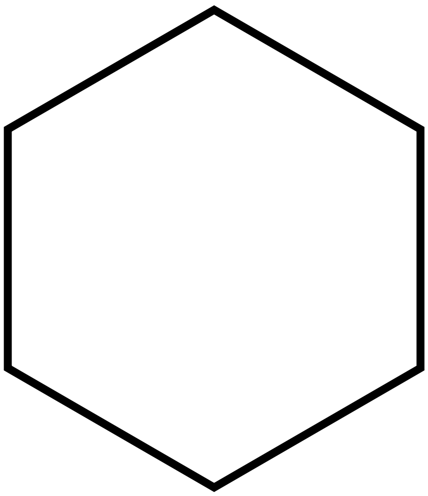
Q2]... [20 points] Let $f : X \to Y$ be a function, and suppose that $A \subseteq X$.

1. Prove that $A \subseteq f^{-1}(f(A))$.

2. Give an explicit example of f, X, Y and $A \subseteq X$ which demonstrates that the inclusion above need not be equality.

3. One of the extra hypotheses f *is injective* or f *is surjective* will guarantee that the inclusion above is actually an equality of sets. Which one? Give a short proof that equality holds under your additional hypothesis.

Q3]. . . [20 points] Describe and list the elements of the group, D_6, of symmetries of the regular hexagon below. Use the space to the right of the image for your answer. You can draw on the diagram too.



Find an isomorphism between D_6 and a subgroup of the symmetric group S_6. Say why your correspondence preserves multiplication.

Find an isomorphism between D_6 and a different subgroup of S_6.

Q4]... [40 points] For each of the following statements, say whether it is true (T) or false (F). Make sure that you give short arguments to support your choice in each case (either providing a counterexample, or a short proof or computation or a connection to a result from the course).

1. $\{\emptyset\} \ = \ \emptyset$

2. If $A = \{1, 2, 3\}$, then $\emptyset \in A$.

3. $12345^{67894} \equiv 4 \mod 11$.

4. The following product of permutations is correct.

$$(12345)(2531) \ = \ (45)(123)$$

5. The following product of permutations is correct.

$$(123456)(135)(24)(654321) \ = \ (246)(35)$$

6. If $f : X \to Y$ is a function and $A \subseteq X$, $B \subseteq X$, then

$$f(A \cap B) \;=\; f(A) \cap f(B)$$

7. Suppose $f : X \to Y$ and $g : Y \to Z$ are functions. If $g \circ f$ is bijective, then f and g are both bijective.

8. If $A \neq \emptyset$ and $A \times B = A \times C$, then $B = C$.