

3. MATH 30A, FALL 2009
Take Home Final (corrected)

Rules: Same as homework. You can work with other people, get outside help, etc. Just make sure your answers are in your own words and that you understand what you are writing.

This take home exam is due in 15 days (on Tuesday, Dec 08). If you are not here, please scan it and email it to me. **Corrections in boldface** *Hints in italics*

3.1. This problem studies “exponents.” If G is an abelian group, the *exponent* of G is defined to be the smallest positive integer n so that $g^n = e$ for all $g \in G$. If no such integer exists then the exponent of G is defined to be infinite. For example, $G = \mathbb{Z}$ has infinite exponent but $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ has exponent 4 (and order 8).

- (1) Show that the exponent of the group S_3 is equal to 6.
- (2) Show that any group of order n has exponent $\leq n$.
- (3) Show that the group of units of $GF(7) \times GF(25)$ is not cyclic by showing that its exponent is less than its order.
- (4) Find an infinite sequence of finite groups whose exponents are smaller than their orders. *For every positive integer n (or for every prime p) take ... Then its order is ... and its exponent is ...*
- (5) Find an infinite sequence of finite groups whose orders are equal to their exponents.

3.2. In this problem we will **use** the finite field $GF(3) = \mathbb{Z}_3$ to construct a group with 6 elements. Your job is to analyze this group and prove that it is isomorphic to one of the familiar groups that we studied.

Let T be the subgroup of $SL(2, 3)$ given by:

$$T := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_3, ac = 1 \right\}$$

- (1) First, explain why this is a group.
- (2) There are 6 elements in this group. Write them down in an organized way.
- (3) Find the orders of the elements of T .
- (4) Is T isomorphic to S_3 or $\mathbb{Z}_2 \times \mathbb{Z}_3$ or some other group that we have studied?
- (5) Find the center of T .

3.3. Euclidean algorithm: Find integers a and b so that

$$125a + 81b = 1$$

After you find these numbers, use them to find the inverse of 81 in the ring \mathbb{Z}_{125} .

To find a and b , Euclid said: Start with the two numbers and keep subtracting the smaller number from the larger one.

$$125 = (1, 0) \cdot (125, 81)$$

$$81 = (0, 1) \cdot (125, 81)$$

This is dot product

$$44 = (1, -1) \cdot (125, 81)$$

and finally:

$$1 = (a, b) \cdot (125, 81)$$

This was used to find the numbers for problem #2 in Homework 10:

$$7 = (1, 0) \cdot (7, 5)$$

$$5 = (0, 1) \cdot (7, 5)$$

$$2 = (1, -1) \cdot (7, 5)$$

Subtract 2 twice from 5 to get:

$$1 = (-2, 3) \cdot (7, 5) = (-2)7 + (3)5$$

3.4. This problem is computational and uses the Euclidean algorithm which you practiced in the previous problem. You receive the following coded message:

$$5192, 2604, 4222$$

Your job is to deduce the original message. The formula by which this message was sent is the following.

Take a message and convert it into a sequence of 4 digits number by taking every pair of numbers and writing them as numbers in the following way: $A = 11, B = 12, \dots$. Then take each 4 digit number M and raise it to the power 1789 modulo 7081 to get $C = 5192$ and so on.

Given that

$$M^{1789} \equiv 5192 \pmod{7081}$$

we can deduce the message M as follows.

- (1) Find the prime factorization of the number $n = 7081$.
- (2) Use Euler's formula to find the Euler phi function $\phi(7081)$.
- (3) Find the number a which is the inverse of the number **1789** modulo $\phi(7081)$.
- (4) Prove that $5192^a \equiv M \pmod{7081}$.

- (5) To compute 5192^a , write a as a sum of powers of 2. For example, if $a = 18$ then $\mathbf{a} = \mathbf{2}^4 + \mathbf{2}^1$ and we just have to square the number four times:

$$5192^2 \equiv 6578 \pmod{7081}$$

$$6578^2 \equiv 5174 \pmod{7081}$$

$$5174^2 \equiv 4096 \pmod{7081}$$

$$4096^2 \equiv 2327 \pmod{7081}$$

So,

$$5192^{18} = 5192^2 5192^{16} \equiv 6578 \cdot 2327 \equiv 4965 \pmod{7081}$$

6578 2327 = 15307006 divide by 7081 to get 2161.70117 Take the fractional part times 7081 to get 4965.

- (6) What was the message?

3.5. This problem studies the action of the group $SL(2, \mathbb{R})$ on the xy plane.

- (1) Show that matrix multiplication gives an action of $SL(2, \mathbb{R})$ on \mathbb{R}^2 .
- (2) Let p be a unit vector in \mathbb{R}^2 . Find the stabilizer subgroup of p . Do (3)(4) first. Then let $p = (x, y)$. Find a rotation matrix which sends $(1, 0)$ to (x, y) .
- (3) Take the special case $p = (1, 0)$. Show that the stabilizer subgroup is abelian in this case.
- (4) Show that **the stabilizer subgroup of any nonzero vector is abelian**. [Hint: all stabilizer subgroups are conjugate. Why is that? And all conjugate subgroups are isomorphic to each other. Why is that?]

3.6. This problem is about semi-direct products.

- (1) Show that the dihedral group D_n (the symmetry group of the regular n -gon) is a semi-direct product of a cyclic group of order n and a group of order 2.
- (2) Suppose that G is a semi-direct product

$$G = K \rtimes Q$$

where Q is also a normal subgroup of G . Then prove that $G = K \times Q$ (the product of the two groups). Show that the commutator $xa x^{-1} a^{-1}$ lies in both K and Q if $x \in K, a \in Q$.

- (3) Describe which elements of $K \rtimes_{\theta} Q$ are in the center of G . The center of G consists of (x, a) where x, a satisfy 3 conditions. Can you find these three conditions?

3.7. This problem concerns the action of a group on its set of subgroups of order p .

Let G be any finite group of order n . Let p be the smallest prime number which divides n . Let X be the set of all subgroups of G of order p .

- (1) Show that G acts on X by conjugation:

$$g \cdot P = gPg^{-1}$$

- (2) The stabilizer of $P \in X$ contains P . Why?
- (3) If P is normal in G then what is the stabilizer of P ?
- (4) Show that G acts trivially on any set having fewer than p elements. *The index of any subgroup of G divides the order of G .*
- (5) Show that if P is normal in G then P is central in G by looking at the action of G on the elements of P . *G acts by conjugation on P .*