

Math 411–Spring 2006

SOLUTIONS TO EXAM 1

1. Write 1 as a linear combination of 130 and 19 with integer coefficients.

Do the Euclidean algorithm. Work backwards to obtain  $1 = 6 \cdot 130 - 41 \cdot 19$ .

2. Solve a system of congruences:

$$\begin{cases} 5x \equiv 3 \pmod{6} \\ 3x \equiv 1 \pmod{7} \end{cases}$$

Answer:  $x \equiv 33 \pmod{42}$ .

- 3(b) Let  $\Sigma(2, \mathbb{R})$  be the set of all stochastic matrices in  $GL(2, \mathbb{R})$ , i.e. matrices whose row sums equal 1. Show that  $\Sigma(2, \mathbb{R})$  is a subgroup of the multiplicative group  $GL(2, \mathbb{R})$ .

Every matrix in  $\Sigma(2, \mathbb{R})$  has the form  $\begin{pmatrix} a & 1-a \\ b & 1-b \end{pmatrix}$ , for some  $a, b \in \mathbb{R}$ . We need to show:

- (1) For any  $A, B \in \Sigma(2, \mathbb{R})$  their product  $AB$  is also in  $\Sigma(2, \mathbb{R})$ :

$$\begin{pmatrix} a & 1-a \\ b & 1-b \end{pmatrix} \begin{pmatrix} c & 1-c \\ d & 1-d \end{pmatrix} = \begin{pmatrix} ac+d-ad & a-ac+1-a-d+ad \\ bc+d-bd & b-bc+1-b-d-bd \end{pmatrix}.$$

Clearly, the row sums of the latter matrix are 1.

- (2) For any  $A \in \Sigma(2, \mathbb{R})$  its inverse  $A^{-1}$  is also in  $\Sigma(2, \mathbb{R})$ :

$$\begin{pmatrix} a & 1-a \\ b & 1-b \end{pmatrix}^{-1} = \frac{1}{\det A} \begin{pmatrix} 1-b & a-1 \\ -b & a \end{pmatrix} = \begin{pmatrix} \frac{1-b}{a-b} & \frac{a-1}{a-b} \\ \frac{-b}{a-b} & \frac{a}{a-b} \end{pmatrix}.$$

Clearly, the row sums of the latter matrix are 1.

For the rest of the problem let  $G$  be a group of order 4.

- 4(b) Prove that  $G$  cannot contain elements of order 3. (Hint: Suppose  $a \in G$  has order 3. Consider the element  $b \in G$  not in  $\langle a \rangle$ . What can you say about  $ab$ ?)

Suppose  $a$  has order 3. Then  $G = \{e, a, a^2, b\}$ . If  $ab \in \langle a \rangle$  then  $b = a^{-1}ab \in \langle a \rangle$  (since  $\langle a \rangle$  is a group), a contradiction. Thus  $ab = b$ , which implies  $a = e$ , a contradiction.

- 4(c) Prove that either  $G$  is a cyclic group or the order of every element in  $G$  is at most 2.

The order of an element cannot exceed the order of the group (otherwise the subgroup it generates is bigger than the group itself). If  $G$  has an element  $a$  of order 4 then  $G = \langle a \rangle$  (i.e.  $G$  is cyclic), otherwise every element has order at most 2 by 4(b).

- 4(d) Write all possible group tables for  $G$ . For each table give an example of a group with this table.

If  $G$  is cyclic then  $G = \{e, a, a^2, a^3\}$  and the table is

$*$	$e$	$a$	$a^2$	$a^3$
$e$	$e$	$a$	$a^2$	$a^3$
$a$	$a$	$a^2$	$a^3$	$e$
$a^2$	$a^2$	$a^3$	$e$	$a$
$a^3$	$a^3$	$e$	$a$	$a^2$

Example:  $G = \mathbb{Z}_4$

If the order of each element of  $G = \{e, a, b, c\}$  is at most two we have  $a^2 = b^2 = c^2 = e$  and there is only one way to complete the table (e.g.  $ab$  cannot be  $b$  so it must be  $c$  etc.):

$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

Example:  $G = V_4$ , the Klein group.

In the rest of the problem we consider the group  $\mathbb{Z}_{30}$  of integers modulo 30.

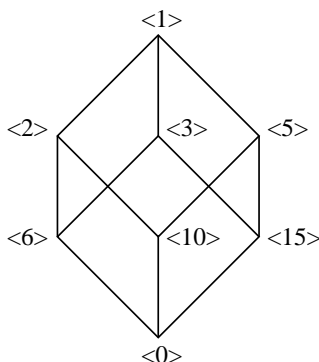
5(b) What elements generate the group? Explain.

Those whose order is 30, i.e. classes mod 30 corresponding to integers relatively prime to 30. They are  $\{1, 7, 11, 13, 17, 19, 23, 29\}$ .

5(c) How many distinct subgroups does the group have? How many of them are cyclic subgroups? Explain.

For every divisor of 30 there exists a unique subgroup of that order. There are 8 divisors of 30 (1, 2, 3, 5, 6, 10, 15, 30) so there are 8 distinct subgroups. They all are cyclic since  $\mathbb{Z}_{30}$  itself is cyclic.

5(d) Draw the subgroup lattice of  $\mathbb{Z}_{30}$ .



6. Give an example of a subgroup of the multiplicative group  $\mathbb{C} - \{0\}$  of order 3.

The three roots of  $z^3 = 1$  form a cyclic subgroup of order 3. They are  $\{1, -1/2 + i\sqrt{3}/2, -1/2 - i\sqrt{3}/2\}$ .

7. Prove that the multiplicative group  $\mathbb{R} - \{0\}$  is not cyclic.

There are many different ways to show that  $\mathbb{R} - \{0\}$  is not cyclic. One can use the fact that  $\mathbb{R}$  is uncountable (and so is  $\mathbb{R} - \{0\}$ ), but for any  $a$  the set  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$  is clearly countable. Thus  $\mathbb{R} - \{0\}$  cannot be equal to  $\langle a \rangle$  for any  $a \in \mathbb{R}$ .

The most straightforward way is probably the following. Assume  $\mathbb{R} - \{0\} = \langle a \rangle$  for some  $a \in \mathbb{R}$ . If  $|a| > 1$  then  $|a^n| > 1$  for any  $n$ , hence  $1/2 \notin \langle a \rangle$ , a contradiction. If  $|a| < 1$  then  $|a^n| < 1$  for any  $n$ , hence  $2 \notin \langle a \rangle$ , a contradiction. If  $|a| = 1$  then  $\langle a \rangle \subseteq \{1, -1\}$ , again a contradiction.

8. (*Bonus.*) Describe all possible groups  $G$  with no non-trivial proper subgroups. Provide proof.

First, note that  $G$  must be cyclic. Indeed, take any element  $a \in G$ ,  $a \neq e$  (the trivial group is clearly cyclic). Then the subgroup  $\langle a \rangle$  is non-trivial (since  $a$  is there), therefore it must coincide with  $G$ .

Second,  $G$  must be finite. Indeed, suppose  $G = \langle a \rangle$  and  $a$  has infinite order. Then also  $G = \langle a^2 \rangle$  (since  $\langle a^2 \rangle$  is non-trivial, hence improper). But then  $a \in \langle a^2 \rangle$  which means  $a = a^{2k}$  for some  $k \in \mathbb{Z}$ . This implies  $e = a^{2k-1}$  which is impossible if  $a$  has infinite order.

Now we know that  $G$  is cyclic of finite order, say  $n$ . Since every divisor of  $n$  gives rise to a unique subgroup of  $G$ ,  $n$  must have exactly 2 divisors (1 and  $n$ ). Therefore  $n$  is prime.

We showed that  $G$  is either trivial or cyclic of prime order, e.g.  $G = \mathbb{Z}_p$ , for  $p$  prime.