

## Math 320 — Exam I

Make sure your reasoning is clear, in most cases in English sentences, with symbols used only for abbreviation and then used correctly. By  $\mathbb{N}$  is meant the set of nonnegative integers,  $\{0, 1, 2, 3, \dots\}$ . TURN OVER — there are six questions.

- (16 points) Which of the following are groups? For each of those that are not groups, cite a property of groups that it doesn't have.
  - $(\mathbb{Z}^+, +)$
  - $(\mathcal{P}(X), \cap)$ , where  $X$  is a nonempty set
  - $(GL(2, \mathbb{R}), *)$ , where  $A * B = AB^{-1}$
  - $(\mathbb{Q} - \{0\}, \text{multiplication})$

- (10 points) (a) Draw the subgroup lattice of  $\mathbb{Z}_{18}$ .  
 (b) Where in your diagram do  $\langle 12 \rangle$  and  $\langle 13 \rangle$  lie?

- (14 points) Let  $S$  be a set with an associative operation  $*$ .

- Prove that, if elements  $e, f$  of  $S$  satisfy  $e * x = x$  and  $x * f = x$  for every  $x$  in  $S$  (i.e.,  $e$  is a “left identity” and  $f$  is a “right identity”), then  $e = f$ .
- Show that, under matrix multiplication, the set

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

has infinitely many left identities but no right identity. (You do not need to show that  $S$  is closed under multiplication.)

- (25 points) Let  $G, H$  be groups, and let  $\varphi : G \rightarrow H$  be a function that “respects the operations”, i.e.,  $\varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2)$  for all  $g_1, g_2$  in  $G$ . Such a function is called a *homomorphism* (of groups). (Here,  $\circ$  denotes the operation on  $G$  and  $*$  denotes the operation on  $H$ . From here on we will denote both by juxtaposition, as if they were multiplication, but if it is helpful to you, you may continue to use  $\circ$  and  $*$ .) It is not hard to show that  $\varphi(e_G) = e_H$  and  $\varphi(x^n) = \varphi(x)^n$  for all  $x \in G$  and  $n \in \mathbb{Z}$ , but you may use these facts without proving them.

- Prove that  $K = \{g \in G : \varphi(g) = e_H\}$  is a subgroup of  $G$ . (The subgroup  $K$  is called the *kernel* of  $\varphi$ .)
- Prove that, for  $g$  in  $G$  of finite order,  $o(\varphi(g))$  is a factor of  $o(g)$ .
- For a fixed  $x$  in  $G$ , the function “conjugation by  $x$ ” is defined by  $\theta_x : G \rightarrow G : g \mapsto xgx^{-1}$ . Prove that  $\theta_x$  is a homomorphism from  $G$  to  $G$ , i.e., it respects the operation on  $G$ .
- What is the kernel of  $\theta_x$ ?
- What must be true about  $x$  if  $\theta_x$  is the identity function on  $G$ ?

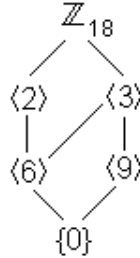
- (15 points) (a) Let  $a$  be an element of a group  $G$  and  $H$  be a subgroup of  $G$ . Prove that  $a \in H$  if and only if  $\langle a \rangle \subseteq H$ . (This is very easy; it is here as preparation for (b).)  
 (b) Let  $x$  be an element of a group for which  $o(x) = n$ , and let  $r, s$  be factors (i.e., divisors) of  $n$ . Prove that  $\langle x^r \rangle \subseteq \langle x^s \rangle$  if and only if  $s$  divides  $r$ . (Warning:  $x^r = (x^s)^d$  does not imply  $r = sd$ .)

6. (20 points) Let  $f, g$  be elements of a group, neither equal to the identity  $e$ , for which  $g^2 = e = f^4$  and  $gfg^{-1}$  is a power of  $f$  but not equal to  $f$  itself.
- (a) What power  $f^k$  of  $f$  must  $gfg^{-1}$  be? (Note this gives  $gf = f^k g$ . This fact is used below.)
  - (b) Write all the different elements of the form  $f^m g^n$  with  $m, n$  in  $\mathbb{N}$ , starting with  $e$  (which is just  $f^0 g^0$ ),  $g$  (which is  $f^0 g^1$ ), and  $f$ . You need not prove that all the symbols in your list are distinct — that would be an easy but ugly cancellation argument.
  - (c) It is possible to write  $(f^m g^n)(f^p g^q)$  in the form  $f^r g^s$ , where  $m, n, p, q, r, s \in \mathbb{N}$ , using the equation from (a). Express  $r$  and  $s$  in terms of  $m, n, p, q$ .
  - (d) Because the finite set of products  $f^m g^n$  is closed under the operation, it forms a group  $D$ . What are the orders of the elements?
  - (e) The groups  $\mathbb{Z}_8$  and  $Q_8$  have the same number of elements as  $D$ . Does either of these groups “behave just like”  $D$ ?

## Solutions to Exam I

1. (a) No identity: 0 isn't in the set. (b) No inverses (except that the identity,  $X$ , is its own inverse). (c) Not associative:  $(A*B)*C = AB^{-1}C^{-1}$  but  $A*(B*C) = A(BC^{-1})^{-1} = ACB^{-1}$ . (d) A group.

2. (a)



- (b)  $\langle 12 \rangle = \langle 6 \rangle$ , because  $\gcd(18, 12) = 6$ , and  $\langle 13 \rangle = \mathbf{Z}_{18}$  because  $\gcd(18, 13) = 1$ .

3. (a) Because  $e$  is a left identity,  $e * f = f$ ; and because  $f$  is a right identity,  $e * f = e$ . Thus,  $f = e * f = e$ .  
 (b) In order to get

$$\begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

we must have  $ea = a$  and  $eb = b$ , but there is no condition on  $f$ ; so all matrices  $\begin{pmatrix} 1 & f \\ 0 & 0 \end{pmatrix}$ , for any  $f$  in  $\mathbb{R}$ , are left identities. If there were a right identity, by (a) it would have to equal all the left identities; but they are not equal to each other; so there is no right identity.

4. (a) Because  $\varphi(e_G) = e_H$ ,  $e_G \in K$ , so  $K \neq \emptyset$ . If  $g_1, g_2 \in K$ , then  $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = e_H e_H = e_H$ , so  $g_1g_2 \in K$ . If  $g \in K$ , then  $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$ , so  $g^{-1} \in K$ . Therefore,  $K$  is a subgroup.  
 (b)  $\varphi(g)^{o(g)} = \varphi(g^{o(g)}) = \varphi(e_G) = e_H$ , so by a theorem in the text,  $o(\varphi(g))$  is a factor of  $o(g)$ .  
 (c) For all  $g_1, g_2$  in  $G$ , we have  $\theta_x(g_1)\theta_x(g_2) = xg_1x^{-1}xg_2x^{-1} = xg_1g_2x^{-1} = \theta_x(g_1g_2)$ .  
 (d)  $\theta_x(g) = e$  means  $xgx^{-1} = e$ , so  $g = x^{-1}ex = e$ ; so the kernel of  $\theta_x$  is  $\{e\}$ .  
 (e) To say that  $\theta_x$  is the identity function means that  $\theta_x(g) = g$  for all  $g$  in  $G$ , i.e.,  $xgx^{-1} = g$  for all  $g$  in  $G$ ; but this is just saying that  $xg = gx$  for all  $g$  in  $G$ , i.e.,  $x \in Z(G)$ .

5. (a) If  $\langle a \rangle \subseteq H$ , then  $a = a^1 \in H$ . If  $a \in H$ , then because  $H$  is closed under the operation and inverses, all the integer powers of  $a$  are in  $H$ , i.e.,  $\langle a \rangle \subseteq H$ .

(b) Suppose  $s$  divides  $r$ , say  $r = sd$  where  $d \in \mathbf{Z}$ ; then  $x^r = (x^s)^d \in \langle x^s \rangle$ , so  $\langle x^r \rangle \subseteq \langle x^s \rangle$ . Conversely, suppose  $\langle x^r \rangle \subseteq \langle x^s \rangle$ . Then  $x^r = (x^s)^d$  for some  $d \in \mathbf{Z}$ . Thus  $x^{r-sd} = e$ , so  $r - sd = nk$  for some  $k$  in  $\mathbf{Z}$ . Because  $s$  divides both terms on the left side of  $r = nk + sd$ , it also divides the right side,  $r$ , and the proof is complete. Here is another, less elementary, way to prove the converse: We know that  $|\langle x^r \rangle| = n/r$  and  $|\langle x^s \rangle| = n/s$ , and because  $\langle x^r \rangle$  is a subgroup of the cyclic group  $\langle x^s \rangle$ , the order of the smaller divides the order of the larger; so  $r/s = (n/s)/(n/r)$  is an integer. (To justify the warning, suppose  $n = 20$ ,  $r = 4$  and  $s = 2$ ; then  $x^4 = (x^2)^{12}$ , but  $4 \neq 2(12)$ .)

6. (a) Because  $f^4 = e$  and  $f \neq e$ ,  $f$  has order either 2 or 4. If it were 2, then  $gfg^{-1}$  would be a power of  $f$  having order 2; the only such is  $f$  itself, and we are told  $gfg^{-1} \neq f$ . So  $f$  has

order 4, and  $gfg^{-1}$  is the only other power of  $f$  of order 4, namely  $f^3$ .

(b) Because  $f^4 = e$  and  $g^2 = e$ , we only need to run  $m$  up to 3 and  $n$  up to 1:

$$e, g, f, fg, f^2, f^2g, f^3, f^3g$$

(c) From  $gfg^{-1} = f^3$ , we get  $gf = f^3g$ , so by moving the  $f$ 's from the middle past a  $g$  to the left, one at a time, replacing it with  $f^3$  whenever it crosses a  $g$ , we can turn  $f^m g^n f^p g^q$  into  $f^{m+3^n p} g^{n+q}$ , i.e.,  $r = m + 3^n p$  and  $s = n + q$ . Fortunately, we only need the cases where  $n, q$  are 0 or 1; if you noted this and said

$$(f^m g^0)(f^p g^q) = f^{m+p} g^q \quad \text{and} \quad (f^m g^1)(f^p g^q) = f^{m+3p} g^{1+q} ,$$

that would be sufficient.

(d)  $e$  has order 1,  $g$  has order 2, and because  $f$  has order 4,  $f^2$  has order 2 and  $f^3$  has order 4. Now  $(fg)^2 = fgfg = ff^3gg = e$ ,  $(f^2g)^2 = f^2gf^2g = f^2f^6gg = e$  and  $(f^3g)^2 = f^3gf^3g = f^3f^9gg = e$ , so  $fg, f^2g, f^3g$  all have order 2.

(e)  $D$  is not abelian (because  $fg \neq gf$ ), so it does not “behave just like”  $\mathbb{Z}_8$ . It has 5 elements of order 2, so it does not “behave just like”  $Q_8$ , which has only 1 such,  $-I$ .