

# Midterm # 1 Solutions

The Nintendo game “Baseball Stars”

February 12, 2008



*Hi baseball fans! We're coming to you from video game land to give you the solutions to the first test. We're lazy aging video game superstars and don't feel the need to type out something that has already been typed out, or can be found verbatim from the book. We hope you enjoy them! ROCK ON!*

1. All of these first ones are definition and can be found in the book.
2. (a) (i)  $U(12)$  is the set of all elements mod 12 that are relatively prime to 12. This would be the set containing the integer representatives  $\{1, 5, 7, 11\}$ . The multiplication table is as follows:

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(ii) This group is not cyclic: you can see this from the multiplication table that  $\langle 1 \rangle = \{1\}$ ,  $\langle 5 \rangle = \{1, 5\}$ ,  $\langle 7 \rangle = \{1, 7\}$ ,  $\langle 11 \rangle = \{1, 11\}$ . None of these elements generate  $U(12)$ , so  $U(12)$  is not cyclic.

- (b) (i) I'm sure at some point we produced a Cayley table for  $D_3$ . We computed in class (ii) the the center of  $D_3$  is  $Z(D_3) = \{e\}$ . Should your class notes be incomplete on this matter or we never did a Cayley table of  $D_3$ , then speak with Corey. Nobody chose this problem to do, so we Baseball Stars feel okay about leaving it at that.
- (c) (i) The group  $Gl(n, \mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) | \det(A) \neq 0\}$ . The group operation is multiplication of matrices.
- (ii) We use the 1-step subgroup test. Let  $A, B \in H$ , so that  $\det(A) = 3^i$ , and  $\det(B) = 3^j$ , where  $i$  and  $j$  are integers. Then  $\det(B^{-1}) = 3^{-j}$ , and  $\det(AB^{-1}) = \det(A)\det(B^{-1}) = 3^i 3^{-j} = 3^{i-j}$ , so  $AB^{-1} \in H$ , which completes the proof.
3. (a) (i) Consider the matrix consisting of all 1's. The (additive) inverse of this matrix is the matrix consisting of all  $-1$ 's, and this matrix is not an element of  $H$ . So this is not a subgroup of  $M_{n \times n}(\mathbb{R})$  since it does not always contain inverses.
- (ii) This is the set of odd integers (under addition!). There are two reasons this is not a subgroup of  $\mathbb{Z}$ : there is no (additive) identity (the element 0 is not in the set), and it is not closed under addition as the sum of two odd numbers is not odd.
- (iii) This is a subgroup. First notice that the element  $a + bi\sqrt{-1} \in H$  has multiplicative inverse  $a - b\sqrt{-1}$  for the following reason. If  $a + b\sqrt{-1} \in H$ , then  $a^2 + b^2 = 1$ . Then

$$\begin{aligned} (a + b\sqrt{-1})(a - b\sqrt{-1}) &= a^2 + b^2 \\ &= 1. \end{aligned}$$

Now consider the elements  $a + b\sqrt{-1}, c + d\sqrt{-1} \in H$ . We have  $a^2 + b^2 = c^2 + d^2 = 1$ . Then we have  $(a + b\sqrt{-1})(c - d\sqrt{-1}) = (ac + bd) + (bc - ad)\sqrt{-1}$ , and

$$\begin{aligned} (ac + bd)^2 + (bc - ad)^2 &= a^2c^2 + b^2d^2 + 2acbd + b^2c^2 + a^2d^2 - 2bcad \\ &= a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= a^2 + b^2 \\ &= 1. \end{aligned}$$

So  $(a + b\sqrt{-1})(c - d\sqrt{-1}) \in H$ , and it follows that  $H \leq G$  by the 1-step subgroup test.

- (b) Suppose that  $\mathbb{Q}^* = \langle \frac{a}{b} \rangle$ , for  $a, b \in \mathbb{Z}$ . Let  $\mathcal{P}$  be the set of primes that divide either  $a$  or  $b$ . Since the set of primes is infinite, we may choose a  $q \notin \mathcal{P}$  which is prime. We claim that the nonzero rational number  $q \notin \langle \frac{a}{b} \rangle$ . Suppose that  $(\frac{a}{b})^n = \frac{a^n}{b^n} = q$ . Then the integer  $\frac{a^n}{b^n}$  must have exactly one factor of  $q$  in its

prime decomposition. But since  $q \notin \mathcal{P}$ ,  $q$  is not a factor of  $a$  or  $b$ , and since  $q$  is prime, the prime decomposition of  $(a/b)^n$  must not have any factors of  $q$  for any  $n$ , a contradiction.

Remark. The book proceeds differently, and we have discussed this proof quite a bit. We Baseball Stars provide a different proof for the interested, and for the uninterested, we refer you to the other proof that Gallian suggests.

- (c) Consider  $G = \mathbb{R}^*$ . The element  $-1$  has order 2 since  $(-1)^2 = 1$  (the identity), while the element 2 has infinite order since each  $i \neq j \in \mathbb{Z}$  has  $2^i \neq 2^j$ .
4. (a) Let  $p$  be prime, and suppose that  $a \times b = 0 \pmod{p}$ . Then  $p|ab$ , and since  $p$  is prime we have  $p|a$  or  $p|b$ . But this implies  $a$  or  $b = 0 \pmod{p}$ . Conversely, suppose every nonzero element  $x \in \mathbb{Z}_p$  has a multiplicative inverse. Then to each  $x$  there exists  $y_x$  such that  $xy_x = 1 \pmod{p}$ . Thus we must have  $p|(xy_x - 1)$ , or that there exists a  $k_x$  so that  $pk_x = xy_x - 1$ , or that  $pk_x + xy_x = 1$ , or that  $\gcd(x, p) = 1$ . So none of the numbers  $x = 2, \dots, p-1$  have any divisors common to  $p$ . Thus  $p$  must have only itself and 1 as divisors, and hence,  $p$  must be prime.
- (b) (i) The identity element in this group is the identity map  $i(x) = x$ .  
(ii) Consider the function  $f^{-1}(x) = \frac{1}{2}x - \frac{1}{2}$ . Clearly  $f \circ f^{-1} = f^{-1} \circ f = i$ , so  $f^{-1} \in C(f)$ . But it is not hard to see that  $f^{-1}$  does not commute with the function  $g(x) = 2x$ :

$$f^{-1}(g(x)) = f^{-1}(2x) = x - \frac{1}{2}, g(f^{-1}(x)) = g\left(\frac{1}{2}x - \frac{1}{2}\right) = x - 1.$$

So  $f^{-1} \in C(f)$ , but we've shown that  $f^{-1} \notin Z(G)$ , so that in general  $Z(G) \neq C(a)$  for some  $a \in G$ .

- (c) Please see the solutions to the second homework assignment, the problems are identical.
5. (a) Let  $H \leq \mathbb{Z}$ . Then we know that  $H$  is cyclic by the fundamental theorem of cyclic groups, as  $\mathbb{Z} = \langle 1 \rangle$  is cyclic. Let  $t$  be the smallest positive integer in  $H$ . We remark that the trivial subgroup  $\{0\}$  is a finite subgroup, and Corey meant to exclude this from consideration. No one seemed to notice this, and so no blunder stars are to be awarded, and we assume henceforth that  $H$  is not the trivial group. Since  $t \in H$ , and  $H$  is finite,  $kt = 0$  for some nonzero integer  $k$ . But this implies that  $t = 0$ , and since  $H$  is assumed to be nontrivial, the element  $t > 0$ , and so we have reached a contradiction.
- (b) Let  $x \in Z(G)$ . Then we note that  $xa = ax$  since  $xy = yx$  for any  $y$  in  $G$ , namely,  $y = a$ . Thus  $Z(G) \subseteq C(a)$  for any  $a \in G$ . Then we use the 2 step subgroup test. Notice that since  $Z(G) \leq G$ , if  $y \in Z(G)$  then  $y^{-1} \in Z(G)$ . Thus for  $x, y \in Z(G)$ , we have  $xyz = xzy = zxy$ , so that  $xy \in Z(G)$ . Thus  $Z(G) \leq C(a)$

for any  $a$ . (We remark that this proof doesn't seem to use the fact that our ambient group is  $C(a)$ , except that we checked that  $Z(G) \subseteq C(a)$  at the start.) See number 4(b)(ii) for an example where  $Z(G) \neq C(a)$  for some  $a$ .

- (c) (i) The number of subgroups of the cyclic group  $\mathbb{Z}_{128}$  is the number of positive divisors of 128, which is 8: 1, 2,  $2^2$ ,  $2^3$ ,  $2^4$ ,  $2^5$ ,  $2^6$ , and  $2^7$ .
- (ii) Each of the subgroups are cyclic because any subgroup of a cyclic group is cyclic.
- (iii) Let  $k$  be a positive divisor of 128. Then each cyclic group of order  $k$  is generated by the element  $128/k$ . We also know (by the fundamental theorem of cyclic groups) that each of these subgroups is unique, so any other generator for a group of the same order would be generating the same subgroup.

**ROCK ON!!!!**