PRACTICE MIDTERM I

MATH 3140

Friday February 25, 2011.

Name | ________________________________

Please answer the all of the questions, and show your work.

1	2	3	4	5	
10	10	10	10	10	total

Date: February 23, 2011.

1
10 points

1 . Define a binary operation $*$ on $X = \mathbb{R} - \{1\}$ by

$$a * b := ab - a - b + 2,$$

for all $a, b \in X$. Is $(X, *)$ a group? Explain your answer.

Solution.

$(X, *)$ is a group.

To show that $(X, *)$ is a group, we must establish that there exists an identity element, that there exist inverses, and that $*$ is associative. Let us begin with the identity element. I claim that the identity element is 2. Indeed,

$$a * 2 = 2 * a = 2a - a - 2 + 2 = a$$

for all $a \in X$, and so 2 is an identity element. Now I claim that given $a \in \mathbb{X}$, there is an inverse $a/(a-1)$. Indeed,

$$a * \frac{a}{a-1} = \frac{a^2}{a-1} - a - \frac{a}{a-1} + 2 = \frac{a^2 - a(a-1) - a}{a-1} + 2 = 2,$$

establishing the claim. Finally, let us check that $*$ is associative. We have

$$(a * b) * c = (ab - a - b + 2) * c$$

$$= (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 = abc - ab - ac - bc + a + b + c + 2.$$

On the other hand, we have

$$a * (b * c) = a * (bc - b - c + 2)$$

$$= a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 = abc - ab - ac - bc + a + b + c + 2.$$

These expressions agree, and hence $*$ is associative. In conclusion, we have shown that $(X, *)$ is a group. □

2
10 points

2 (a). [3 points] How many subgroups are there of $\mathbb{Z}_{42}$.

Solution.

There are 8 subgroups of $\mathbb{Z}_{42}$.

We have seen in class that every subgroup of a cyclic group is cyclic (and so generated by a single element). Moreover, we have seen that $\langle [m] \rangle = \langle [\gcd(n,m)] \rangle$. Consequently, there is one subgroup of $\mathbb{Z}_n$ for each divisor of n. In our case, since $42 = 2^1 \cdot 3^1 \cdot 7^1$, there must be $2 \cdot 2 \cdot 2 = 8$ divisors of 42. These are are easily seen to be $1, 2, 3, 7, 6, 14, 21, 42$. Thus there are eight subgroups of $\mathbb{Z}_{42}$. □

2 (b). [3 points] Is [21] a generator of $\mathbb{Z}_{100}$?

Solution.

Yes, [21] is a generator of $\mathbb{Z}_{100}$.

We have seen that for an element $[m] \in \mathbb{Z}_n$, the order of the group $\langle [m] \rangle$ is equal to $n/\gcd(n,m)$. In other words, $[m]$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n,m) = 1$. Thus, since $\gcd(100, 21) = 1$ we see that 21 is a generator. □

2 (c). [4 points] Are the groups $\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_8$ and $\mathbb{Z}_3 \times \mathbb{Z}_{24} \times \mathbb{Z}_{10}$ isomorphic?

Solution.

Yes, $\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_8 \cong \mathbb{Z}_3 \times \mathbb{Z}_{24} \times \mathbb{Z}_{10}$.

From the theorem on finitely generated abelian groups, we have

$$\mathbb{Z}_6 \times \mathbb{Z}_{15} \times \mathbb{Z}_8 \cong (\mathbb{Z}_3 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \times \mathbb{Z}_8 \cong \mathbb{Z}_3 \times \mathbb{Z}_{24} \times \mathbb{Z}_{10}.$$

□

3
10 points

3 . Consider the dihedral group D_3; that is the group of symmetries of an equilateral triangle. Using the same notation as in class, let $R \in D_3$ correspond to clockwise rotation by $\pi/3$ radians, and let $D \in D_3$ correspond to flipping through a chosen vertex.

3 (a). Find $i \in \mathbb{Z}$ and $j \in \{0,1\}$ such that $R^2DRDR^{-1} = R^iD^j$.

Solution.

$$\boxed{R^2DRDR^{-1} = R^0D^0.}$$

We have shown in class, and it is not hard to check that $RD = DR^{-1}$. Thus

$$R^2DRDR^{-1} = R^2D(DR^{-1})R^{-1} = Id = R^0D^0.$$

□

3 (b). What is the order of the element RD?

Solution.

$$\boxed{|RD| = 2.}$$

We have $RD \neq Id$ and

$$(RD)(RD) = RR^{-1}DD = Id.$$

□

3 (c). Show that D_3 is isomorphic to S_3, the symmetric group on 3 letters.

Solution. Let $\sigma = (1,2,3) \in S_3$ and let $\tau = (2,3) \in S_3$. Note that

$$\sigma\tau = (1,2,3)(2,3) = (1,2) = (2,3)(3,2,1) = \tau\sigma^{-1}.$$

Now recall that as a set $D_3 = \{Id, R, R^2, D, RD, R^2D\}$. Define a map of sets $\phi : D_3 \to S_3$ by

$$R^iD^j \mapsto \sigma^i\tau^j.$$

I claim this is a homomorphism. Indeed, we have

$$\phi((R^aD^b)(R^cD^d)) = \phi(R^{a+(-1)^bc}D^{d-b}) = \sigma^{a+(-1)^bc}\tau^{d-b} = \sigma^a\tau^b\sigma^c\tau^d = \phi(R^aD^b)\phi(R^cD^d).$$

Finally I claim that ϕ is injective. This can be checked explicitly on the six elements of D_3. For instance $\phi(RD) = \sigma\tau = (1,2) \neq Id$. Now, since ϕ is an injective map of sets of the same order, it is also a surjective map. Thus ϕ is a bijective homomorphism, which is an isomorphism. □

4
10 points

4 . Let $G = \{0, 1, 2, \ldots, n\}$ and let $*$ be a binary operation on G. Assume that $(G, *)$ is a group, and $*$ satisfies

(1) $a * b \leq a + b$ for all $a, b \in G$.

(2) $a * a = 0$ for all $a \in G$

Show that $n = 2^m - 1$ for some $m \in \mathbb{N}$. [Hint: use (1) and (2) to show that 0 is the identity element. Then use (2) to show that G is abelian. Then use (2) and the theorem on finitely generated abelian groups.]

Solution. First I will establish that 0 is the identity element of G. That is I will show that $0 * k = k$ for all $k \in G$. I will do this by induction on k. For the base case, consider that by (2), we have $0 * 0 = 0$. Now assume that we have shown that $0 * k = k$ for all $k \leq r$. I will show that $0 * (r + 1) = r + 1$. Indeed, from (1) it follows that $0 * (r + 1) \in \{0, \ldots, r + 1\}$. But if $0 * (r + 1) = k$ with $k < r + 1$, then $0 * (r + 1) = 0 * k$ by induction. Multiplying by 0^{-1}, we get $r + 1 = k$ a contradiction. Thus $0 * (r + 1) = r + 1$. By induction, we have that $0 * k = k$ for all $k \in G$. Thus 0 is the identity element of the group.

Next I claim that G is abelian. In fact, this is true for any group Γ such that $a^2 = e$ for all $a \in \Gamma$. Indeed, we have $e = (ab)(ab)$. From this we get $b = ababb = aba$, and then $ba = abaa = ab$. This holds for any $a, b \in \Gamma$, so Γ is abelian. We conclude that G is a finite abelian group.

The theorem on finitely generated abelian groups implies that $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m}$ for some numbers $n_1, \ldots, n_m$ all greater than or equal to two. If any of the n_i were greater than 2, there would be an element in G with order greater than 2, contradicting (2). Indeed, we could assume that $n_1 > 2$, and then the element $(1, 0, \ldots, 0)$ would have order equal to n_1, greater than 2. Thus all of the n_i are equal to 2, and $|G| = 2^m$. Finally, since $|G| = n + 1$, we conclude that $n = 2^m - 1$. □

5
10 points

5 . True or false. If true, explain briefly (a sentence or two). If false, provide a counter example.

5 (a). Every cyclic group is abelian. [ ]

Solution. TRUE. We proved this in class (and it is easy to check directly). □

5 (b). Every abelian group is cyclic. [ ]

Solution. FALSE. The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian, but not cyclic. □

5 (c). An element g of a group G has order $n > 0$ if and only if $g^n = e$. [ ]

Solution. FALSE. In $\mathbb{Z}_4$, the element $[2]$ satisfies $4 \cdot [2] = [0]$, but the order of $[2]$ is equal to 2. □

5 (c). A cyclic group has a unique generator. [ ]

Solution. FALSE. $[1]$ and $[2]$ generate $\mathbb{Z}_3$. □

5 (e). If H and H' are subgroups of a group G, then $H \cup H'$ is a subgroup. [ ]

Solution. FALSE. Consider the subgroups $H = \langle([1], [0])\rangle$ and $H' = \langle([0], [1])\rangle$ in $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then $([1], [0]) + ([0], [1]) = ([1], [1]) \notin H \cup H'$. So $H \cup H'$ is not closed under the operation of G. □

5 (f). There exists a finite abelian group of every order $n \in \mathbb{N}$. [ ]

Solution. TRUE. The cyclic group $\mathbb{Z}_n$ is abelian. □