UMASS AMHERST MATH 411 SECTION 2, FALL 2009, F. HAJIR

PROBLEM SET 6

These problems are all OPTIONAL. You may hand in this Problem Set for Extra Credit.

PROBLEM I. (a) Suppose G is a cyclic group of order n, where $n \geq 1$ is an integer. Show that G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

(b) Suppose G and Q are both finite cyclic groups of order n. Show that G and Q are isomorphic. Hint: you can use (a) but you don't have to.

(c) Show that if G is an infinite cyclic group, then G is isomorphic to $\mathbb{Z}$.

PROBLEM II. Suppose G is a cylcic group. Show that G is commutative. Hint: you can use PROBLEM 1 but you don't have to.

Reminder about LCM and GCD Recall that if a, b are integers, then $\gcd(a, b)$ is the greatest (positive) common divisor of a and b, and $\operatorname{lcm}(a, b)$ is the smallest (positive) common multiple of a and b. If we write a, b in their prime factorizations as

$$a = p_1^{a_1} \cdots p_r^{a_r}, \qquad b = p_1^{b_1} \cdots p_r^{b_r},$$

then you'll have no trouble verifying that

$$\gcd(a, b) = \prod_{j=1}^{r} p_j^{\min(a_j, b_j)}, \qquad \operatorname{lcm}(a, b) = \prod_{j=1}^{r} p_j^{\max(a_j, b_j)}.$$

Since $\min(x, y) + \max(x, y) = x + y$, we get the identity

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

PROBLEM III. Suppose G is a group and $g \in G$ has order n. If a is an integer, show that g^a has order

$$\frac{n}{\gcd(n, a)} = \frac{\operatorname{lcm}(n, a)}{a}.$$

PROBLEM IV. Suppose G is a cyclic group of order n. Show that every subgroup of G is cyclic. Hint: Let g be a generator of G. Let H be a subgroup of G. Consider the smallest integer k such that $g^k \in H$. Show that g^k generates H.

PROBLEM 5. Suppose G is a cyclic group of order n. Let g be a generator of G.

(a) Show that for each integer $d \geq 1$ which divides n, there is exactly one subgroup H of G of order n.

(b) Describe all homomorphic images of G.

(c) How are (a) and (b) related? [Hint: recall the philosophy that every homomorphic image of G is essentially a quotient of G.]

PROBLEM 6. (a) Suppose G is a group and A, B are subgroups of G. Show that if B is a normal subgroup of G, then $AB = \{ab | a \in A, b \in B\}$ is a subgroup of G. Also show that if both A and B are normal in G, then AB is a normal subgroup of G.

(b) Give an example to show that if A and B are subgroups of a group G, then $AB = \{ab | a \in A, b \in B\}$ need not be a subgroup of G. Hint: try $G = S_3$, and keep (a) in mind.

Definition 0.1 (Direct Product of Groups)**.** Suppose $(G_1, *_1, e_1)$ and $(G_2, *_2, e_2)$ are groups. Define a new group $(G, *, e)$, called *the direct product of* G_1 *and* G_2 as follows: as a set, $G = G_1 \times G_2$, i.e. the elements of G are exactly all ordered pairs (g_1, g_2) where $g_1 \in G_1$ and $g_2 \in G_2$. The identity e of G is (e_1, e_2) and the group operation is defined componentwise, i.e.

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2).$$

PROBLEM VII. Check that with the above definition, the direct product of two groups is a group.

PROBLEM 8. Suppose G is a cyclic group of order mn where m, n are positive integers with $\gcd(m, n) = 1$. Suppose M and N are cyclic groups of order m and n respectively. Show that G is isomorphic to the direct product $M \times N$.

Hint: you may want to remind yourself of the following fact. We have $\gcd(m, n) = 1$ if and only if there exist integers a, b such that $am + bn = 1$.