WORKSHEET # 3

MATH 435 SPRING 2011

We begin by recalling some facts about cyclic groups that we proved on Wednesday.

- A group G is called *cyclic* if there exists $a \in G$ such that $G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a^1, a^2, \dots\}$. Any such a is called *a generator (of G)*.
- If G is cyclic, so is every subgroup $H \subseteq G$.
- If G is cyclic and finite and $H \subseteq G$ is a subgroup, then $|H|$ divides $|G|$ (recall $|G|$ just means the number of elements of G).
- If $G = \langle a \rangle$ and $|G| = n < \infty$, and $m \in \mathbb{Z}$ is such that $\gcd(n, m) = 1$, then a^m generates G as well.
- If $G = \langle a \rangle$ is cyclic and $|G| = n < \infty$, then for every natural number k such that $k|n$, there exists a unique subgroup H of G of order k. That subgroup is $H = \langle a^{n/k} \rangle$.

1. We never proved the last fact yesterday. Prove it now.

Solution: To show that $H = \langle a^{n/k} \rangle$ has order k, it is equivalent to show that $a^{n/k}$ has order k. Certainly $(a^{n/k})^k = a^n = e$. On the other hand, if m satisfies $0 < m < k$, then $(a^{n/k})^m = a^{nm/k}$ and this cannot equal e since $nm/k < n$. Thus the order of $a^{n/k}$ is indeed k as desired. In particular, the existence claim is proven.

Now we prove uniqueness. Suppose that K is a subgroup of order k, we will prove that $K = H$. Since K is a subgroup of a cyclic group, K is also cyclic. Thus $K = \langle a^m \rangle$. If we can show that $a^m \in H$, then it follows that $K \subseteq H$ (since every element of K is a power of a^m). In that case, since K and H have the same number of elements, we would then have $K = H$. Therefore, it is sufficient to show that $a^m \in H$.

We know $a^{mk} = e$ since $|a^m| = |K| = k$. Thus n divides mk or in other words there exists an integer t such that $tn = mk$. We then obtain $m = t(\frac{n}{k})$. Thus $a^m \in \langle a^{n/k} \rangle = H$ as desired.

2. Suppose that you are given two groups A and B. Define a new group, $A \oplus B$ as follows. The elements of $A \oplus B$ is the set of pairs

$$\{(a, b) | a \in A, b \in B\}.$$

The operation is defined as follows $(a, b)(a', b') = (aa', bb')$. Show that $A \oplus B$ is a group. Further prove that $A \oplus B$ is Abelian if and only if A and B are both Abelian.

Solution: First we show that $A \oplus B$ is indeed a group. For associativity notice that

$$\begin{aligned}(a,b)\left((a',b')(a'',b'')\right) &= (a,b)(a'a'',b'b'') = \left(a\left(a'a''\right), b\left(b'b''\right)\right) \\ &= \left(\left(aa'\right)a'', \left(bb'\right)b''\right) = (aa',bb')(a'',b'') = \left((a,b)(a',b')\right)(a'',b'')\end{aligned}$$

where the third comes from the associativity of A and B (since they are groups). Simple computations verify that (e_A, e_B) is the identity of $A \oplus B$. Likewise, the inverse of (a, b) is (a^{-1}, b^{-1}) and so $A \oplus B$ is a group.

For the second statement, suppose that $A \oplus B$ is Abelian. Choose $a, a' \in A$ and $b, b' \in B$, thus $(aa', bb') = (a, b)(a', b') = (a', b')(a, b) = (a'a, b'b)$. Therefore $aa' = a'a$, which implies that A is Abelian and $bb' = b'b$ which implies that B is Abelian. Conversely, if A and B are Abelian, then for any $(a, b), (a', b') \in A \oplus B$ we have that $(a, b)(a', b') = (aa', bb') = (a'a, b'b) = (a', b')(a, b)$ as desired.

3. Suppose that A and B are groups of finite order. Show that $|A \oplus B| = |A||B|$. Further show that $A \oplus B$ has a subgroup H with order $|A|$ and a different subgroup K of order $|B|$ such that $H \cap K = \{e\}$.

Solution: The number of pairs (a, b) is the number of possible as times the number of possible bs, in other words, $|A||B|$. Set $H = \{(a, e_B)|a \in A\}$ and set $K = \{(e_A, b)|b \in B\}$, certainly $H \cap K = \{e\}$. There may be other possible choices of H and K but those given always work.

4. Suppose that A and B are finite cyclic groups $|A| = n$ and $|B| = m$.

(a) If $n = 2$ and $m = 3$, prove that $A \oplus B$ is cyclic.
(b) If $n = 2$ and $m = 2$, prove that $A \oplus B$ is not cyclic.
(c) Is $A \oplus B$ cyclic if $n = 4$ and $m = 6$?
(d) Find a condition on n and m which completely characterizes the n and m such that $A \oplus B$ is cyclic. Prove your condition is correct.

Solution: Write $A = \langle a \rangle$ and $B = \langle b \rangle$.

(a) Then $(a, b), (a, b)^2 = (e_A, b^2), (a, b)^3 = (a, e_B), (a, b)^4 = (e_A, b), (a, b)^5 = (a, b^2), (a, b)^6 = (e_A, e_B)$. Thus (a, b) has order 6, and so $A \oplus B$ is cyclic.
(b) For any $(a', b') \in A \oplus B$, $(a', b')^2 = (e_A, e_B)$ and so $A \oplus B$ has no elements of order 4 (all are order 2), and so $A \oplus B$ is not cyclic.
(c) No, see the answer below.
(d) $A \oplus B$ is cyclic if and only if $\gcd(n, m) = 1$. To see this, we first claim the order of an element $(a', b') \in A \oplus B$ is $\text{lcm}(|a'|, |b'|)$. This is easily seen since $(a', b')^k = (a'^k, b'^k)$ equals (e_A, e_B) if and only if $|a'|$ divides k and $|b'|$ divides k, the smallest such integer is $\text{lcm}(|a'|, |b'|)$. Of course, $A \oplus B$ is cyclic if and only if it contains an element of order $|A \oplus B| = nm$. Now, since the order of (a', b') is $\text{lcm}(|a'|, |b'|)$ and $|a'| \le n$ and $|b'| \le m$, the only way $|(a', b')|$ is if $\text{lcm}(n, m) = nm$ which happens if and only if $\gcd(n, m) = 1$, as desired.

5. Suppose that A and B are cyclic groups but that A has infinitely many elements and $B \neq \{e\}$. Prove that $A \oplus B$ is not cyclic.

Solution: Suppose on the contrary that $A \oplus B = \langle (a, b) \rangle$ was cyclic. Thus for every element $g \in A$ and $h \in B$, there exists an $n \in \mathbb{Z}$ such that $(a, b)^n = (g, h)$. In particular, $a^n = g$ and $b^n = h$. Thus $\langle a \rangle = A$ and $\langle b \rangle = B$. Since A has infinitely many elements, this implies that a has infinite order (ie, $a^n \neq e$ for any $n \in \mathbb{N}$). Consider now the element $(a, e_B) \in A \oplus B$, since $A \oplus B = \langle (a, b) \rangle$, this means that there exists n such that $(a^n, b^n) = (a, b)^n = (a, e_B) = (a^1, e_B)$. But then $n = 1$, so $b = b^1 = e_B$ also, but $B = \langle b \rangle$ so $B = \{e_B\}$. However, we assumed $B \neq \{e_B\}$ at the start, a contradiction.