SOLUTIONS: MATH 103 MIDTERM II FALL 2009

1. Let H and K be finite subgroups of a group G with $|H| = 24$ and $|K| = 33$.
(a) Show that the intersection $H \cap K$ is a subgroup of G.
(b) Assume that $H \cap K$ contains more than one element. How many elements does it have? Why?

Solution: If a, b are in $H \cap K$, then both a and b are in H. As H is a subgroup, we also have $ab \in H$. By the same argument, $ab \in K$. Hence $ab \in H \cap K$. Similarly, if a is in both H and K, then also a^{-1} is in H (as H is a subgroup) and it also is in K (as K is a subgroup). Hence $H \cap K$ is a subgroup by subgroup test.

To show (b), we use Lagrange's Theorem. As $H \cap K$ is a subgroup of H, $|H \cap K|$ must divide $|H| = 24$. By the same argument, it also divides $|K| = 33$. Hence $|H \cap K|$ divides $gcd(24, 33) = 3$. As $|H \cap K| > 1$ by assumption, it must be equal to 3.

2. Show that the groups $\mathbf{Z}_6$ and $U(7)$ are isomorphic.

Solution: We know that $\mathbf{Z}_6$ is a cyclic group, generated by the element 1 which has order 6. As an isomorphism preserves the order of the element, we have to find an element a in $U(7)$ which has order 6. This can be done by trial and error. We can not take $a = 2$, as $a^3 = 8 \equiv 1 \bmod 7$. But $3^2 \equiv 2 \bmod 7$, $3^3 = 27 \equiv -1 \bmod 7$, $3^4 \equiv -3 \bmod 7$, $3^5 \equiv -9 \equiv 5 \bmod 7$ and $a^6 \equiv 1 \bmod 7$. Hence 3 has order 6 in $U(7)$.

We can now define the isomorphism Φ by $n \mapsto 3^n \bmod 7$ for $n = 1, 2, \ldots, 6$. This is 1-1 and onto, which we see from the calculations above. Moreover,

$$\Phi(n)\Phi(m) = 3^n 3^m = 3^{n+m} = 3^k,$$

where $0 \leq k < 6$ such that $k \equiv n + m \bmod 6$. Here the equality $3^{n+m} = 3^k$ follows from the fact that $n + m = 6q + k$ for some q and $3^{n+m} = 3^{6q+k} = (3^6)^q 3^k = 3^k$. Hence we have $\Phi(n)\Phi(m) = \Phi(n + m)$ and Φ is an isomorphism.

3. Find all subgroups of order 4 in $\mathbf{Z}_4 \oplus \mathbf{Z}_2$.

Solution: We have seen that an abelian group of order 4 is either cyclic (if it contains an element of order 4), or it is isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ (if it does not contain an element of order 4). Let us determine the elements (a, b) of order 4. By a theorem in class, we have

$$ord((a, b)) = lcm(ord(a), ord(b)) = 4.$$

As the order of b can be at most 2, it follows that the order of a must be 4, and b can have order 1 or 2. Hence the elements of order 4 are

$$\{(1, 0), (1, 1), (3, 0), (3, 1)\}.$$

Each element of order 4 generates a cyclic subgroup of order 4. However, this subgroup contains two elements of order 4, the chosen generating one and its inverse. Hence we have two cyclic subgroups of order 4, namely $\{(0, 0), (1, 0), (2, 0), (3, 0)\}$ and

$\{(0,0),(1,1),(2,0),(3,1)\}$. Moreover, as we have four elements of order 4 and one element of order 1 (the identity $(0,0)$), there are three remaining elements of order 2, namely $\{(2,0),(2,1),(0,1)\}$. These elements together with the identity form another subgroup of order 4. Answer: Three subgroups of order 4.

4. Let G be a finite group with $|G| = 21$ and let H be a normal subgroup with $|H| = 7$.
   (a) Let $a \in G$, $a \notin H$. What is the order of aH in the factor group G/H? To which group is the factor group G/H isomorphic?
   (b) Let $\tilde{a} \in aH$. Which numbers can be the order of $\tilde{a}$. Why?
   (c) Give an example of G, H and a as in (a) and elements $\tilde{a} \in aH$ for all possible orders of $\tilde{a}$, as determined in (b).

Solution : We have $\frac{|G|}{|H|} = 21/7 = 3$ cosets of H in G (recall that left and right cosets are the same for a normal subgroup). Hence G/H is a group of order 3, and it must be isomorphic to $\mathbf{Z}_3$ (as 3 is a prime number). So, in particular, as aH is not the identity element H in G/H, the order of aH must be 3, which shows (a).

By a theorem in class, the order of aH must divide the order of a. Hence the order of a must be a multiple of 3 for a as in part (a). On the other hand, the order of a must divide the order of G, which is $21 = 3 \cdot 7$. Hence the only possibilities for the order of a are 3 and 21.

To find an example for (c), take $G = \mathbf{Z}_{21}$, $H = \langle 3 \rangle = \{0,3,6,9,12,15,18\}$ and $a = 1$. Then $|H| = 7$ and H is normal, as G is abelian. Moreover, ord(1)=21. But we also have $7 = 1 + 2 \cdot 3 \in 1 + H$ (here we use additive notation) and the order of 7 is equal to 3. These are all the possibilities in (b).