Math 103 HW 6 Solutions to Selected Problems

14. **Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is a prime?**

    Solution: Let g be a generator of G, of order n, and let g^k be a generator of the subgroup of order H (such a generator must exist, since a subgroup of a cyclic group is cyclic). Notice that $(g^k)^n = (g^n)^k = e$, so 7 must at least divide n. This means that $|g^7| = \frac{n}{(n,7)} = \frac{n}{7}$. On the other hand, by assumption the subgroup $< g^7 >$ has order $1, 7$, or n, so these are the only choices for $\frac{n}{7}$. The third case is ruled out immediately (n can never equal $\frac{n}{7}$). The first implies that $n = 7$, contradicting the fact that G has a *proper* subgroup of order 7. The only choice left is $\frac{n}{7} = 7$, or $n = 49$. The same proof, replacing 7 everywhere with any prime p, shows that if we start with p instead we get $|G| = p^2$.

19. **If a cyclic group has an element of infinite order, how man elements of finite order does it have.**

    Solution: Suppose $G =< g >$ is cyclic of infinite order. To begin with, this forces g to have infinite order. If some power g^k has finite order—n, say—then $g^{kn} = e$, and g has order dividing kn (a contradiction, since then g has finite order) unless $k = 0$. Thus $g^0 = e$ is the only element of finite order in G.

24. **For any element a in any group G, prove that $< a >$ is a subgroup of $C(a)$ (the centralizer of a).**

    Solution: $< a >$ is already a group under the multiplication in G, so we just need to show it is a subset of $C(a)$. This is easy: $a \cdot a = a \cdot a$, so $a \in C(a)$. As $C(a)$ is a group (in particular, closed under multiplication and inversion), we must have that any a^n is also in $C(a)$. This is precisely what it means for $< a > \subseteq C(a)$, so we are done.

30. **Suppose G is a group with more than one element. If the only subgroups of G are $\{e\}$ and G, prove that G is cyclic and has prime order.**

Solution: Take any $g \neq e$ (this is possible since G has more than one element. Then $< g > \neq \{e\}$, so $< g >= G$, hence G is cyclic. Consider the subgroup $< g^2 >$. If this is $\{e\}$, then g has order 2, so we are finished. Otherwise $< g^2 >= G$, and we can write $g = g^{2k}$ for some $k \in \mathbb{Z}$. But then $e = g^{2k-1}$, so g (hence G) has finite order.

Now let $|G| = n$. Because $n > 1$, by unique factorization there exists a prime p dividing n. We want to show that $n = p$. If $< g^p >= \{e\}$ (ie, $g^p = e$), then n divides p, which combined with $p|n$ implies $p = n$. Otherwise, $< g^p >= G$, meaning g^p is a generator of G. But this is only true if n and a nontrivial divisor of n, p, are coprime; impossible. Therefore $n = p$, as desired.

38. **Let m and n be elements of the group $\mathbb{Z}$. Find a generator for the group $< m > \cap < n >$.**

Solution: We can be sure that some generator exists because $\mathbb{Z}$ is cyclic, so the subgroup $< m > \cap < n >$ must also be. This is just the common multiples of m and n, so one guesses that $< m > \cap < n >=< \ell >$, where ℓ is the least common multiple of m and n (that is, the smallest positive common multiple). ℓ is clearly an element of $< m > \cap < n >$, so we need only show that if $a \in< m > \cap < n >$, the ℓ divides a. Let $a = q\ell + r$, with $q, r \in \mathbb{Z}$ and $0 \leq r < \ell$. Since m and n divide a (a is an element of $< m > \cap < n >$) and divides ℓ, they must both divide $r = a - q\ell$. But ℓ is the least common multiple, so $r = 0$, and ℓ divides a. This shows that $< m > \cap < n >=< \ell >$.

50. **Prove that an infinite group must have an infinite number of subgroups.**

Solution: Let G be such a group. Suppose G has an element g of infinite order. Then for any $j > k > 0$, $< g^j >$ cannot equal $< g^k >$. This is true because otherwise, we would have $g^j = g^{kn}$ and $g^k = g^{jm}$ for some $n, m \in \mathbb{Z}$, meaning $g^{j-kn} = e = g^{k-jm}$. Since g has infinite order, the only way this can happen is if $j = kn$ and $k = jm$. But then k and j both divide each other, so they are equal. We thus conclude that the $< g^k >$ for $k > 0$ provide an infinite number of (distinct for each k) subgroups.

The only other option is that every element of G has finite order. In this case, we can construct an infinite sequence of subgroups as follows. Start with any element g_1 of G. Now assume we have picked $g_1, \cdots, g_n$ such that none of the g_i are equal for $1 \leq i \leq n$. Since each g_i has finite order, the set of powers $S_n = \{g_i^k | k \in \mathbb{Z}, 1 \leq i \leq n\}$ is finite. As G is infinite, $G - S_n$ is nonempty, so if we pick $g_{n+1} \in G - S_n$, by definition g_{n+1} cannot be an element of $< g_i >$ for any smaller i. Thus $< g_{n+1} > \neq < g_n > \neq \cdots \neq < g_1 >$. This process then yields an infinite sequence $< g_i >$ of distinct subgroups of G.

62. **Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $< a > \cap < b >= \{e\}$.**

Solution: Let $|a| = n$, $|b| = m$. Clearly $e \in < a > \cap < b >$, so we must show the other containment. To this end, suppose $g \in < a > \cap < b >$. Then $g = a^k = b^\ell$ for some $k, \ell \in \mathbb{Z}$. Since g is a power of a, we know that $|g|$ divides n. g is a power of b as well, so $|g|$ divides m—ie, it is a common divisor of m and n. But n and m are relatively prime, so $(m, n) = 1$ implies $|g| = 1$, and $g = e$.

68. **Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $< x^r > \subseteq < x^s >$.**

Solution: $< x^s >$ is closed under multiplication and inversion, so $< x^r > \subseteq < x^s >$ if and only if $x^r \in < x^s >$, which is true if and only if $x^r = x^{sk}$ for some k. But this (multiplying/dividing both sides by $(x^r)^{-1}$) happens if and only if $e = x^{sk-r}$. By Theorem 4.1, it is thus necessary and sufficient that $r \equiv sk \pmod{n}$ for some $k \in \mathbb{Z}$—in other words, that $< r > \subseteq < s >$ in Z_n.