Math 103A: Homework 4 solutions

1. Solution to I.6, Q18
   There are $\frac{42}{gcd(30,42)} = 7$ elements in the subgroup. In fact, $< 30 >= \{30, 18, 6, 36, 24, 12, 0\}$.

2. Solution to I.6 Q23
   For a finite cyclic subgroup of order n, there is exactly one subgroup for each divisor of n. (This is from *Theorem 6.14* and the discussion following the theorem). So we have nine distinct subgroups generated by the elements $1, 2, 3, 4, 6, 9, 12, 18$ and $36(0)$. Check out *Example 6.17* for what the subgroup diagram should look like.

3. Solution to I.6 Q27
   Similar to the previous problem, we find all the subgroups of $\mathbb{Z}_{12}$. These are subgroups generated by $1, 2, 3, 4, 6$ and $12(0)$. The subgroup generated by 2, for example, has order $\frac{12}{gcd(2,12)} = 6$. By similar computations, the subgroups generated by $1, 3, 4, 6$ and $12(0)$ have orders $12, 4, 3, 2$ and 1 respectively.

4. Solution to I.6 Q32
   a. True. This is *Theorem 6.1*.
   b. False. The Klein 4-group from *Example 5.9* is abelian but not cyclic.
   c. False. Any $\frac{a}{b}$ cannot generate $\mathbb{Q}$ because $\frac{a}{2b}$ is not an integral multiple of $\frac{a}{b}$.
   d. False. As we saw on the first problem above, 30 does not generate $\mathbb{Z}_{42}$.
   e. True. $\mathbb{Z}_n$.
   f. False. Again, the Klein 4-group has order 4 but is not cyclic.
   g. False. 9 is not prime but generates $\mathbb{Z}_{20}$ as gcd(9,20) = 1.
   h. False. What even is the group operation in $(\mathbb{Z}_5, +) \cap (C^*, .)$?
   i. True. This follows from the definition of a subgroup and *Exercise 54* in section 5.
   j. True. If a generates a group, then a^{-1} generates the group as well (why?).

5. Solution to I.6 Q33
   As we mentioned in the previous problem, the Klein 4-group from *Example 5.9* is finite of order 4, but is not cyclic.

6. Solution to I.6 Q44
   Let $\phi : G \to G'$ and $\psi : G \to G'$ be two isomorphisms such that $\phi(a) = \psi(a)$, where a generates G. We need to show $\phi(x) = \psi(x)$ for all $x \in G$. Note that $\phi(a^2) = \phi(a.a) = \phi(a).\phi(a) = \phi(a)^2$ since ϕ is an isomorphism, and we can extend that by simple induction to $\phi(a^n) = \phi(a)^n$. Since G is cyclic, any $x \in G$ can be written as $x = a^m$ for some $m \in \mathbb{Z}$. So $\phi(x) = \phi(a^m) = \phi(a)^m$. Similarly, $\psi(x) = \psi(a^m) = \psi(a)^m$. Now $\phi(a) = \psi(a) \implies \phi(a)^m = \psi(a)^m \implies \phi(x) = \psi(x)$.

7. Solution to I.6, Q45
Given $n, r \in \mathbb{Z}^+$, let $H = \{nr + ms | n, m \in \mathbb{Z}\}$. We can show that H satisfies the subgroup axioms. Given $nr + ms, pr + qs \in H$, clearly $(n + p)r + (m + q)s \in H$. So H is closed. Taking $n = 0$ and $m = 0$, $0.r + 0.s = 0 \in H$. So H has the identity element. Finally, given $nr + ms \in H$, it's inverse $(-n)r + (-m)s$ is also in H. Hence H is a subgroup.

8. Solution to I.6, Q46
Assume ab has finite order n, i.e. n is the smallest integer such that $(ab)^n = e$. Note that $(ba)^{n+1} = b(ab)^n a = ba$ since $(ab)^n = e$. Multiplying both sides by the inverse of ba, we get $(ba)^n = e$. So $\text{ord}(ba) \leq n$. In fact the order of ba has to equal n. If $\text{ord}(ba) = m < n$, by symmetry of the above argument, $\text{ord}(ab) <= m < n$, which gives a contradiction.

9. Solution to I.6 Q50
Let a be the unique element in G of order 2. Let $x \in G$ be an arbitrary element. Note that $(xax^{-1})^2 = (xax^{-1})(xax^{-1}) = xa^2x^{-1} = xx^{-1} = e$ since by assumption $a^2 = e$. So xax^{-1} has order 2. (It cannot have order 1 as that would make a the identity.) But a is the unique element of order 2. So $xax^{-1} = a \implies xa = ax$.

10. Solution to I.6 Q51
We need to find the number of positive integers less than pq that are relatively prime to pq. We can actually list the elements that do not satisfy the requirement: $p - 1$ multiples of q and $q - 1$ multiples of p that are less than pq. So the number of generators is $pq - 1 - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1)$. (This is actually the Euler's totient function: $\phi(pq) = \phi(p)\phi(q) = (p - 1)(q - 1)$).

11. Solution to I.6 Q52
Similar to the previous problem, we need to find the number of positive integers less than p^r that are relatively prime to p^r, i.e. not divisible by p. The elements that do not satisfy the requirement are the $p^{r-1} - 1$ multiples of p. So the number of generators is $p^r - 1 - (p^{r-1} - 1) = p^{r-1}(p - 1)$. (Again, this number is $\phi(p^r) = p^{r-1}(p - 1)$.)

12. Solution to I.6 Q55
Let H be a proper nontrivial subgroup of $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is cyclic, H is cyclic. Let a be a generator of H.Then the order of H equals $\frac{p}{gcd(a,p)} = \frac{p}{1} = p$. Therefore H contains p elements, i.e. $H = \mathbb{Z}_p$, which is a contradiction.

13. Solution to I.6 Q56
(a) Let a and b be elements of orders r and s respectively such that $H =< a >$ and $K =< b >$. We claim that the order of ab is rs, and thus $< ab >$ is a subgroup of order rs.
Note that, since G is abelian, $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e^s e^r = e$. Now let n be the

order of ab: $(ab)^n = e \implies a^n b^n = e \implies a^n = b^{-n}$. Since $b^{-n} \in K$ and $a^n = b^{-n}$, $a^n \in K$, but also $a^n \in H$. Because H and K have only e in common (as their orders are relatively prime), $a^n = b^{-n} = e$. Finally, since the order of a is r, r divides n, and since the order of b is s, s divides n. But rs is the least common multiple of r and s, and we already showed $(ab)^{rs} = e$. Therefore, the order of ab is rs, and $< ab >$ is the desired subgroup.

(b) Again, let a and b be elements of orders r and s respectively such that $H =< a >$ and $K =< b >$. Let d be the gcd of r and s. Writing $r = dq$, we note that $\gcd(q, s) = 1$ and $\mathrm{lcm}(r, s) = \frac{rs}{d} = qs$. Consider the subgroup of H generated by a^d, $L =< a^d >$, which has order q. Since $\gcd(q, s) = 1$, we can apply part (a) for L and K to get a cyclic subgroup of order qs which is the least common multiple of r and s.