MATH 375.11

Class 11: Selected Answers

1. **a)** Let G be a finite group of order n. Let $a \in G$. Show that $|a| \leq n$. **Solution:** Let $|a| = m$. Consider the set of $n+1$ elements $\{e = a^0, a = a^1, a^2, \ldots, a^n\} \subset G$. Since $|G| = n$, not all of the elements are distinct. So there exist elements $a^k = a^j$ such that $k \neq j$ in the set (with $0 \leq 1 \leq n$). WMA that $k > j$. So then $a^k = a^j \Rightarrow a^{k-j} = a^{j-j} = e$. Note that $0 < k - j \leq n$. But then by by an earlier Corollary, $|m| \mid (k-j)$, so $m \leq (k-j) \leq n$.

b) Let G be a finite group of order n. Prove that there is some positive integer M so that for every $a \in G$, we have $a^M = e$. **Solution:** By the previous part, the order of any element in G is not greater thant $n = |G|$. Therefore, since $n!$ is the product of all posiive integers less than or equal to n, if a is any element of G, then $|a| \mid n!$. So $M = n!$ will work.

2. **a)** Determine the subgroup lattice for Z_{15}. **Solution:**

$$\begin{tikzcd}
 & <1> \arrow[dl] \arrow[dr] & \\
<3> \arrow[dr] & & <5> \arrow[dl] \\
 & <0> &
\end{tikzcd}$$

b) Notice that $15 = 3 \cdot 5$ is the product of two primes. If p and q are distinct primes, determine the subgroup lattice for Z_{pq}. **Solution:**

$$\begin{tikzcd}
 & <1> \arrow[dl] \arrow[dr] & \\
<p> \arrow[dr] & & <q> \arrow[dl] \\
 & <0> &
\end{tikzcd}$$

3. Gallian page 81 #36.

$*$	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

Solution: Note this is **not** a subgroup problem because the operation is different than in $\mathbf{Z}_{20}$ (multiplication, not addition) and the elements are not even in $U(20)$. So check the four group properties. The operation is closed. The identity is 16. Inverses: $4^{-1} = 4, 8^{-1} = 12, 12^{-1} = 8$, $16^{-1} = 16$. Finally, the operation is associative because multiplication mod 20 is associative.

4. Gallian page 81 #42. **Solution:** Note that since $6 \mid |G|$ and $G = < a >$ is cyclic, then the Fundamental theorem applies. There is only one subgroup of order 6 and it is generated by $a^{n/6}$ where $n = |G|$. If we let $x = a^{n/6}$ then the subgroup is $< x > = \{e, x, x^2, x^3, x^4, x^5\}$. Written this way, the elements of order 6 are obvious: x and x^5 since only their powers are relatively prime to 6. In the original format, the two elements would have been $a^{n/6}$ and its inverse $a^{-n/6} = x^5$.

5. Let $G =< x >$ be cyclic. If $|x| = n$, show that $< x^r >=< x^s > \iff \gcd(n, r) = \gcd(n, s)$. **Solution:** First, Sam's theorem says

$$\gcd(n, r) = \gcd(n, s) \iff \frac{n}{\gcd(n, r)} = \frac{n}{\gcd(n, s)} \iff |x^r| = |x^s| \iff |< x^r >| = |< x^s >|.$$

Notice what this says: If the gcds are the same, then the *orders* of the cyclic subgroups are the same. Sam's theorem does not say the the cyclic subgroups are the same, just that there are orders are. But the Fundamental Theorem of Cyclic Groups (FTCG) says that: There is only one subgroup of a cyclic group of a particular order. Finish the proof now by observing

$$|< x^r >| = |< x^s >| \iff < x^r >=< x^s >$$

from the FTCG. So you need both theorems.

6. Extra Credit: Gallian page 81 #50. **Solution**: If $U(49)$ is cyclic and has order 42, then if g is any generator, then by Sam's theorem the other generators have the form g^n where $1 < n < 42$ and $\gcd(42, n) = 1$. Thus $n = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41$. So there are 12 generators. Note that the numbers listed are *not* the generators themselves, they are the *powers* of any generator we eventually select. If you look in your text, the number integers les than n relatively prime to n is called $\phi(n)$. It is an important function.

7. Several of you tried to show that an infinite group must have an infinite number of subgroups. Here's another hint: Split it into two cases: G has at least one element x with infinite order; (2) All elements of G have finite order.