Math 103B HW 1 Solutions to Selected Problems

7. Let $|a| = 30$. How many cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.

Solution: We know that $|\langle a^4 \rangle| = |\langle a^{4,30} \rangle| = |\langle a^2 \rangle|$, and this is just $|a^2|$, which is 15. Thus, Lagrange’s theorem tells us that there are 2 cosets. $\langle a^4 \rangle$ is one coset, of course, but what is the other one? Since cosets are disjoint, and in general for an element $g$ and a subgroup $H$ $g$ is an element of the coset $gH$ (since $e \in H$), we need only find an element that is not in $\langle a^4 \rangle$. But $a$ itself certainly is not in $\langle a^4 \rangle$ (otherwise we would have $\langle a^4 \rangle = \langle a \rangle$), so $a \langle a^4 \rangle$ is the other coset. One can check that is none other that the odd powers of $a$.

9. Let $H = \{ (1), (12)(34), (13)(24), (14)(23) \}$. Find the left cosets of $H$ in $A_4$. How many left cosets of $H$ in $S_4$ are there? (Determine this without listing them.)

Solution: Since $|A_4| = 12$, Lagrange’s theorem predicts that there will be 3 cosets. Since $(123) \not\in H$ but (as mentioned in the previous problem) is in $(123)H$, $(123)H \neq H$. By the same token $(321)H \neq H$. However, $(321)^{-1}(123) = (123)(123) = (321)$ is not in $H$ either, so $(321)H \neq (123)H$. This gives all 3 cosets. We could also write down all the cosets explicitly:

$$H = \{ (1), (12)(34), (13)(24), (14)(23) \}$$
$$ (123)H = \{ (123), (413), (243), (214) \}$$
$$ (321)H = \{ (321), (431), (234), (124) \}$$

and verify that this yields all the elements of $A_4$.

$S_4$ has order 24, so using Lagrange’s theorem again says that there are 6 cosets of $H$ in $S_4$.

10. Let $a$ and $b$ be elements of a group $G$ and $H$ and $K$ be subgroups of $G$. If $aH = bK$, prove that $H = K$.

Solution: $aH = bK$ is equivalent to $H = a^{-1}bK$. Since $kK = K$ for any element $k$ of $K$, it’s then enough to show $a^{-1}b \in K$. Why is this? As usual, $a$ is an element of $aH$, so we can find $k_0 \in K$ such that $a = bk_0$. But then $a^{-1}b = k_0^{-1}$, so it is in $K$, and we are done.
21. Suppose $G$ is a finite group of order $n$ and $m$ is relatively prime to $n$. If $g \in G$ and $g^m = e$, prove that $g = e$.

Solution: $g^m = e$, so we know that the order of $g$—call it $d$—satisfies $d$ must also divide $n$ by Lagrange’s theorem. The only common divisor of $n$ and $m$ is $1$, so $g$ is an element of order $1$; i.e., $g = e$.

24. Let $p$ be a prime and $k$ a positive integer such that $a^k \mod p = a \mod p$ for all integers $a$. Prove that $p-1$ divides $k-1$.

Solution: $0^k \equiv 0 \mod p$ whenever $k > 0$ (since they are equal), so the real content here is that for any $a \in \mathbb{Z}_p^\times$, $a^k \equiv a \mod p$. For a invertible modulo $p$, this is the same as $a^{k-1} \equiv 1 \mod p$ for all $a \in \mathbb{Z}_p^\times$. We want to show $p-1$ divides $k-1$. This is hard to prove unless we know that $\mathbb{Z}_p^\times$ is cyclic (of order $p-1$): in fact, the two statements can be shown to be equivalent. Since we’ll (almost certainly) prove this fact later, we assume it for this problem. Now the proof is easy: take $g \in \mathbb{Z}$ whose equivalence class modulo $p$ generates $\mathbb{Z}_p^\times$. Then $g^{k-1} = 1$ implies $|g|$ divides $k-1$. But $|g| = p-1$, which gives the desired result.

38. Prove that if $G$ is a finite group, the index of $Z(G)$ cannot be prime.

Solution: Suppose the index is some prime $p$. Then $p > 1$, so $G \neq Z(G)$. Now take $g \notin Z(G)$. Let $C(g)$ be the centralizer of $g$ in $G$. It follows from the definitions that $Z(G)$ is a subgroup of $C(g)$, (if an element commutes with everything, it commutes with $g$), but they are not equal since $g \in C(g)$. Thus $[C(g) : Z(G)] \neq 1$. On the other hand, by problem 33 \footnote{which is easy to prove: just use the formula in Lagrange’s theorem twice} $p = [G : Z(G)] = [G : C(g)][C(g) : Z(G)]$. $p$ is prime, so $[C(g) : Z(G)]$ being a divisor of $p$ greater than $1$ means that $[C(g) : Z(G)]$, and hence that $[G : C(g)] = 1$. But this implies $G = C(g)$, meaning that every element of $G$ commutes with $g$—a contradiction as $g \notin Z(G)$. Therefore, $[G : Z(G)]$ cannot be prime.

41. Let $G$ be a group of order $100$ that has a subgroup $H$ of order $25$. Prove that every element of $G$ of order $5$ is in $H$.

Solution: Let $g$ be an element of $G$ of order $5$. Then

$$|\langle g \rangle H| = \frac{|\langle g \rangle||H|}{|\langle g \rangle \cap H|} = \frac{1 \cdot 25}{5 \cdot 25} = \frac{|\langle g \rangle \cap H|}{125} = |\langle g \rangle \cap H|$$

But $\langle g \rangle H$ is a subset of $G$, so its size is bounded above by $|G| = 100$. This forces $|\langle g \rangle \cap H| > 1$, which means (by Lagrange’s theorem, since $|\langle g \rangle|$ is prime and $\langle g \rangle \cap H$ is a subgroup of $\langle g \rangle$), that it must be $5$. Therefore $\langle g \rangle \cap H = \langle g \rangle$, so in particular $g \in H$. 

Page 2
46. **Prove that a group of order 12 must have an element of order 2.**

**Solution:** Let $G$ be such a group. In general, if $g \in G$ has order $n$ divisible by 2, then $g^{n/2}$ has order 2. Thus, the only way $G$ could have no elements of order 2 is if every element of $G$ has order not divisible by 2. Suppose this is the case. By Lagrange’s theorem, the only possible orders for elements of $G$ are the divisors of 12: 1, 2, 3, 4, 6, and 12, and we can rule out each of those except for 1 and 3 since the others are divisible by 2. This means we have one element of order 1 (the identity), and 11 of order 3. However, if $g$ has order 3, then so does $g^2 = g^{-1}$ (which is not equal to $g$), meaning we can pair up each element of order 3 with its inverse. This means that the number of elements of order 3 is even, a contradiction, so $G$ must have an element of order 2 after all.

50. **Prove that $A_5$ has a subgroup of order 12.**

**Solution:** $A_5$ permutes the set $\{1, 2, 3, 4, 5\}$, and we claim that the orbit of any $i \in \{1, 2, 3, 4, 5\}$ is the whole set. To see this, we just note that the (even) permutation $(ij)(k\ell)$ (for $k, \ell \neq i$ or $j$) takes $i$ to $j$, for any $i$ and $j$. But then by the Orbit-Stabilizer theorem

$$|\text{stab}_G(i)| = \frac{|A_5|}{|\text{orb}_G(i)|} = \frac{60}{5} = 12$$

Thus for any $i$, $\text{stab}_G(i)$ will give us a subgroup of order 12.

**Remark:** We could also have just noticed that $A_4$, which has order 12, is a subgroup. However, $\text{stab}_G(5)$ is just $A_4$, so this argument is a slight generalization of the easier one. In fact, these are the only subgroups of order 12.

56. **Why does the fact that $A_4$ has no subgroup of order 6 imply that $|Z(A_4)| = 1$?**

**Solution:** Suppose $\alpha \in Z(A_4)$. If $\alpha$ is not the identity, it is either a product of disjoint 2-cycles (so has order 2), or a 3-cycle (so has order 3). If the former, then if we take any 3-cycle $\beta$, $|\alpha\beta| = \text{lcm}(|\alpha|, |\beta|) = 6$ since $\alpha$ and $\beta$ commute. If $|\alpha| = 3$ instead, the same argument, using an element $\beta$ of order 2, shows that either way we have an element of order 6 in $A_4$. This generates a subgroup of order 6, impossible, so $\alpha$ can only be the identity, and $|Z(A_4)| = 1$. 