MATH 257: Homework #3

Jesse Farmer

20 October 2004

1. *Prove that if $A \subset B$ then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subset B$ and $A \neq B$, but $\langle A \rangle = \langle B \rangle$.*

   Both $\langle A \rangle$ and $\langle B \rangle$ are groups under the same operation, so it suffices to show that $\langle A \rangle \subset \langle B \rangle$. Every element of $\langle A \rangle$ can be written as $a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$. By hypothesis, however, $a_i \in B$, and hence $a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} \in \langle B \rangle$.

   If there exists an element in $b \in B \setminus A$ such that $b = a_1 a_2$ for some $a_1, a_2 \in A$, then, even though $A \neq B$, $\langle A \rangle = \langle B \rangle$.

2. *A group H is called* finitely generated *if there is a finite set A such that $H = \langle A \rangle$.*

   (a) *Prove that every finite group is finitely generated.*
   If H is finite then certainly $H = \langle H \rangle$, and is therefore finitely generated.

   (b) *Prove that $\mathbb{Z}$ is finitely generated.*
   Clearly $(\mathbb{Z}, +) = \langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\}$.

   (c) *Prove that every finitely generated subgroup of the additive group of $\mathbb{Q}$ is cyclic.*
   Consider $H = \left\langle \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \right\rangle$. For any $a \in H$ there exist $m_1, \ldots, m_n$ such that

   $$a = \sum_{i=1}^{n} \frac{m_i p_i}{q_i} = \frac{\sum_{i=1}^{n} \left(m_i p_i \prod_{k \neq i} q_k \right)}{\prod_{k=1}^{n} q_k} = n \frac{1}{k}$$

   where n is the numerator of the above expression and k the denominator. Hence $H \leq \left\langle \frac{1}{k} \right\rangle$ (it is a group, and certainly a subset of the latter), and since the subgroup of a cyclic group is itself cyclic, H must be cyclic.

   (d) *Prove that $\mathbb{Q}$ is not finitely generated.*
   From the previous part we see it is sufficient to show that $\mathbb{Q}$ is not cyclic. This is clear since, if it were the case, every element could be written as $\frac{np}{q}$ for some $p, q, n \in \mathbb{Z}$. All that is necessary to construct an element not of this form is to pick two primes p_1, p_2 not equal to q or p. There exists no n such that $\frac{p_1}{p_2} = n \frac{p}{q}$.

3. *Let $A = \{\pi \in S_n \mid |\pi| = 2\}$. Show that $S_n = \langle A \rangle$.*

   Obviously $\langle A \rangle \subset S_n$, so it is sufficient to show that $S_n \subset \langle A \rangle$, i.e., every element of S_n can be written as the composition of 2-cycles. Since any permutation can be decomposed into

disjoint cycles, it is also sufficient to show that a single cycle can be written as the product of 2-cycles. Consider the cycle $(c_1 c_2 \cdots c_n)$. We claim

$$(c_1 c_2 \cdots c_n) = (c_1 c_2)(c_1 c_3) \cdots (c_1 c_i)(c_1 c_{i+1}) \cdots (c_1 c_n)$$

This 2-cycle representation is correct since $c_i \mapsto c_{i+1}$, $c_1 \mapsto c_2$, and $c_n \mapsto c_1$.

4. *Let G be a group and $a_1, \ldots, a_n \in G$ with $a_i a_j = a_j a_i$ for all i, j. Prove that $H = \langle a_1, \ldots, a_n \rangle = \{a_1^{m_1} \cdots a_n^{m_n} \mid m_i \in \mathbb{Z}\}$ and H is Abelian.*

   Because of commutability we can group element of the same base together, and add their exponents. Induction on n would perhaps be more rigorous.

5. *Let G be a group and $a, b \in G$ with $|a| = |b| = |ab| = 2$. Prove that $\langle a, b \rangle = \{1, a, b, ab\}$ is of order 4.*

   Every element g of $\langle a, b \rangle$ satisfies the property $g^2 = 1$, and so by the previous homework $\langle a, b \rangle$ is Abelian. Hence $g = a^n b^m$ for some $m, n \in \mathbb{N}$. However, since every power of a, b, or ab is either itself or the identity (because they are all of order 2), it follows that $a^n b^m$ is one of a, b, ab. Note that $a, b, e \neq ab$ since, if $ab = a$ or $ab = b$ then b or a would be of order 1, respectively, and if $ab = e$ then $a = b$.

6. *Prove that up to isomorphism there are exactly two groups of order 4.*

   Any group of order 4 can be written as $\{e, a, b, c\}$. The order of any element must divide the order of the group, hence the orders of a, b, c must be some combination of 2 and 4, respectively (since only the identity has order 1). If two distinct non-identity elements a, b have order 2 then $a \neq b^{-1}$ since this implies $a = b$. The contrapositive of this shows that if $a = b^{-1}$ then a, b do not have order 2, i.e., they must have order 4. Hence there must be an even number of elements of order 4, which means there are either none or there are two. This completely determines the structure of the group since the identity has order 1, and therefore there are at most two distinct groups of order 4, up to isomorphism. It is easy to check that two such groups exist and that they are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

7. *Find the number of subgroups of order n of S_n when n is prime and when $n = 4$.*

   Up to isomorphism the answer is 1 and 2, respectively. However, not counting isomorphic groups, there are $(n-2)!$ subgroups of order n when n is prime. This is because we know each non-identity element of the subgroup must have order n and hence be composed of commuting n-cycles, and hence has one cycle of length n. Fixing the first element of that cycle and permuting the others determines all the other members of the group, but for each of these $(n-1)!$ subgroups, there are $n-1$ permutations that result in the same group (e.g., $\{e, (123), (132)\}$ is the same group, not simply isomorphic to, $\{e, (132), (123)\}$), so there are $(n-2)!$ actual subgroups.

   When $n = 4$ there are two possibilities for the orders of the elements, but from previous problems we know that the elements must have orders of the form $1, 2, 2, 2$ or $1, 2, 4, 4$. There are three of the former and one of the later, making for 4 in total.

8. *Let $H \leq G$ and $g \in G$. Prove that if the right coset equals some left coset of H in G then it equals the left coset gH and $g \in N_G(H)$.*

   Clearly if $gH = Hg$ then $g \in N_G(H)$, since every element of h can be written as $gh'g^{-1}$ for some $h' \in H$. It suffices to prove that if $gH = Hx$ then $gH = Hg$.

$g \in gH$ since $e \in H$, and therefore $g \in Hx$. Hx and Hg are either disjoint or coincide, and since they share at least one element, namely g, they must coincide. Therefore $gH = Hx = Hg$.

9. *Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = \{e\}$.*

   Since $H \cap K \leq K$ and $H \cap K \leq H$, the order of $H \cap K$ must divide both $|H|$ and $|K|$, but since these two integers are relatively prime the largest integer to do so is 1 and $|H \cap K|$ must be 1.

10. *Let G be a group and H_1, H_2 be subgroups of G of finite index. Prove that $H_1 \cap H_2$ is a subgroup of H_1 of finite index and $[H_1 : H_1 \cap H_2] \leq [G : H_2]$. Deduce that $[G : H_1 \cap H_2]$ is finite.*

    Let $h_1, h_2 \in H_1 \cap H_2$. Then $h_1^{-1}h_2 \in H_1$ and $h_1^{-1}h_2 \in H_2$ since H_1 and H_2 are groups, which implies $h_1^{-1}h_2 \in H_1 \cap H_2$. That is, $H_1 \cap H_2 \leq H_1$. Now consider $H_1/H_1 \cap H_2$. The smallest $H_1 \cap H_2$ could be is if it were $\{e\}$, in which case $H_1/H_1 \cap H_2 \cong H_1$. Similarly, the largest it could be is if $H_1 = H_2$, in which case $H_1/H_1 \cap H_2 \cong \{e\}$. Therefore $[H_1 : H_1 \cap H_2] \leq |H_1| < \infty$. And this is not true, since $|H_1|$ is not necessarily finite, but I misread the problem and it's late now.

    By Proposition 13 in Chapter 3,

$$[H_1 : H_1 \cap H_2] = \frac{|H_1|}{|H_1 \cap H_2|} = \frac{|H_1 H_2|}{|H_2|} \leq \frac{|G|}{|H_2|} = [G : H_2]$$

    Since $H_1 \cap H_2 \leq H_1$, it must be that $|H_1 \cap H_2| \leq |H_1|$ and hence

$$[G : H_1 \cap H_2] = \frac{|G|}{|H_1 \cap H_2|} \leq$$