SOLUTIONS FOR PROBLEM SET 4

A. Suppose that G is a group and that H is a subgroup of G such that $[G : H] = 2$. Suppose that $a, b \in G$, but $a \notin H$ and $b \notin H$. Prove that $ab \in H$.

Solution. Since $[G : H] = 2$, it follows that H is a normal subgroup of G. Consider the quotient group G/H. It is a group of order 2. The identity element in that group is H. The other element (the element which is not the identity) in that group is of order 2. If $a \in G$, but $a \notin H$, then aH is that other element in G. Thus, we have $(aH)^2 = H$. However, if $b \in G$, but $b \notin H$, then bH is also that other element. That is, we have $bH = aH$.

Therefore, we have $(aH)(bH) = (aH)(aH) = (aH)^2 = H$. Now, $(aH)(bH) = abH$. Thus, we have $abH = H$. This means that $ab \in H$, which is what we wanted to prove.

B: This problem concerns the group $G = \mathbb{Q}/\mathbb{Z}$. The group operation will be written as $+$.

(a) Prove that every element of G has finite order.

Solution. We will prove that every element of G has finite order. If $g \in G$, then $g = r + \mathbb{Z}$, where $r \in \mathbb{Q}$. There exists a positive integer n such that $nr \in \mathbb{Z}$. (For example, one could write r in reduced form and let n be the denominator of r.) We then have

$$ng = n(r + \mathbb{Z}) = nr + \mathbb{Z} = \mathbb{Z},$$

the last equality following from the fact that $nr \in \mathbb{Z}$. The second equality is a consequence of the definition of addition in the quotient group $\mathbb{Q}/\mathbb{Z}$. We have proved that ng is the identity element in G and therefore g has finite order. Thus, every element of G indeed has finite order.

(b) Prove that every finite subgroup of G is a cyclic group.

Solution. We will prove that every finite subgroup of G is a cyclic group. Suppose H is a finite subgroup of G. Let $|H| = t$. Then

$$H = \{h_1, ..., h_t\}, \quad \textit{where } h_i = r_i + \mathbb{Z} \ \textit{ and } \ r_i \in \mathbb{Q}$$

for $1 \leq i \leq t$. We can write the rational numbers $r_1, ..., r_t$ in the following way

$$r_i = \frac{n_i}{m}$$

where m is a positive integer and $n_i \in \mathbb{Z}$ for $1 \leq i \leq t$. To do this, we can take m to be any positive integer which is a multiple of the denominators of all the rational numbers $r_1, ..., r_t$, i.e., a common denominator for those rational numbers. Let

$$a \;=\; \frac{1}{m} + \mathbb{Z} \;\in\; G$$

Then we have

$$n_i a \;=\; n_i\left(\frac{1}{m} + \mathbb{Z}\right) \;=\; \frac{n_i}{m} + \mathbb{Z} \;=\; r_i + \mathbb{Z} \;=\; h_i$$

for $1 \leq i \leq t$. Therefore, $h_i \in \langle a \rangle$ for $1 \leq i \leq t$, where $\langle a \rangle$ is the cyclic subgroup of G generated by a. Therefore, H is a subgroup of $\langle a \rangle$. Since H is a subgroup of a cyclic group, we can conclude that H itself is a cyclic group. We are using one of the propositions we have proved about cyclic groups.

(c) Give a specific example of a proper subgroup H of G which is not finite.

Solution. Let

$$H \;=\; \{g \in G \mid |g| = 2^m, \;\; \textit{where } m \textit{ is a nonnegative integer } \}$$

To verify that H is a subgroup of G, note that the identity element has order $1 = 2^0$ and so is in H. Also, if $h \in H$, then its inverse $-h$ has the same order as h and so the inverse $-h$ is in H. Also, if $h_1, \; h_2 \in H$, then let their orders be $2^{m_1}, \; 2^{m_2}$, respectively. Let $m = max\{m_1, \; m_2\}$. Note that both 2^{m_1} and 2^{m_2} divide 2^m. Therefore, $2^m h_1 = e$ and $2^m h_2 = e$, where e is the identity element of G. Since G is an abelian group, we have

$$2^m(h_1 + h_2) \;=\; 2^m h_1 + 2^m h_2 \;=\; e + e \;=\; e$$

and so the order of $h_1 + h_2$ must divide 2^m. It follows (from number theory) that the order of $h_1 + h_2$ is a power of 2 and therefore $h_1 + h_2 \in H$. Thus, H is closed under the group operation for G. We have verified that H is a subgroup of G.

Suppose m is any positive integer. Let $h_m = \dfrac{1}{2^m} + \mathbb{Z}$. Then

$$2^m h_m \;=\; 2^m\left(\frac{1}{2^m} + \mathbb{Z}\right) = 1 + \mathbb{Z} \;=\; \mathbb{Z} \;=\; e, \qquad 2^{m-1} h_m \;=\; 2^{m-1}\left(\frac{1}{2^m} + \mathbb{Z}\right) \;=\; \frac{1}{2} + \mathbb{Z} \;\neq\; e \;.$$

Hence the order of h_m divides 2^m, but does not divide 2^{m-1}. It follows that the order of h_m is equal to 2^m. Thus, the cyclic subgroup $\langle h_m \rangle$ of H has order 2^m. Since m can be chosen as large as we wish, and H contains a subgroup of order 2^m, it is clear that H cannot be finite.

To show that $H \neq G$, consider the element $g = \frac{1}{3} + \mathbb{Z} \in G$. Clearly, $g \neq e$ and $3g = e$. Thus, g has order 3 and so $g \notin H$. Hence $H \neq G$.

(d) Prove that no proper subgroup of G can have finite index.

Solution. Suppose that H is a subgroup of G of finite index. Since G is abelian, H will be a normal subgroup of G. The quotient group G/H is finite, by assumption. Let $n = |G/H|$. Then every element of G/H has order dividing n. This means that, for every $g \in G$, $n(g + H)$ is the identity element of G/H, which is the coset H. Thus, $n(g + H) = H$. But, $n(g + H) = ng + H$. It follows that $ng \in H$ for all $g \in G$.

Let nG denote $\{ng \mid g \in G\}$. We have proved that $nG \subseteq H \subseteq G$. We will now prove that $nG = G$. To see this, suppose that $f \in G$. Write $f = r + \mathbb{Z}$, where $r \in \mathbb{Q}$. Let $s = \frac{1}{n}r$. Then $s \in \mathbb{Q}$. Let $g = s + \mathbb{Z}$. Then

$$ng = n(s + \mathbb{Z}) = ns + \mathbb{Z} = r + \mathbb{Z} = f.$$

Since $f \in G$ is arbitrary, we have proved that $nG = G$. Since $nG \subseteq H \subseteq G$, we can now conclude that $H = G$. Thus, if H is a subgroup of G of finite index, then $H = G$ and hence H is not a proper subgroup of G.

C: Suppose that G is a group and that N and M are normal subgroups of G.

TRUE OR FALSE: *If* $G/M \cong G/N$*, then* $M \cong N$*.*

If this statement is true, give a proof. If it is false, give a specific counterexample.

Solution The statement is false. Here is a counterexample. Let $G = D_4$, the group of symmetries of a square. We can regard D_4 as a subgroup of S_4. Suppose that N is the Klein 4-group. That is,

$$N = \{ e.\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3) \}\ .$$

As discussed in class one day, N is a subgroup of D_4. We have $[G : N] = |G|/|N| = 8/4 = 2$. Since the index is 2, it follows that N is a normal subgroup of G. Furthermore, G/N is a group of order 2. It must be a cyclic group of order 2. Note that every element of N has order 1 or 2. Thus, N has no element of order 4.

On the other hand, let M be the subgroup of D_4 consisting of the rotations. Then M is a cyclic group of order 4. It has two elements of order 4. Furthermore, we have $[G : M] = |G|/|M| = 8/4 = 2$. Thus M is a normal subgroup of G and G/M is a group of order 2. Thus, G/M is a cyclic group of order 2.

Thus, both G/N and G/M are cyclic groups of order 2 and are therefore isomorphic to each other. However, N and M are not isomorphic to each other. The group M has elements of order 4, but the group N has no such elements.

D: If G is an abelian group, then every subgroup of G is a normal subgroup. Is the converse of that fact true? If true, give a proof. If false, give a counterexample.

Solution. The converse is false. The group $G = Q_8$ is a counterexample. This group is nonabelian. However, every subgroup of G is a normal subgroup of G. This is obvious for G itself and for the trivial subgroup $\{1\}$. It is also true for any subgroup H of G such that $|H| = 4$. This is so because if $|H| = 4$, then $[G : H] = 2$. Therefore, such a subgroup H will be a normal subgroup of G.

It remains to consider subgroups H of G such that $|H| = 2$. However, there is only one such subgroup, namely $H = \{1, -1\}$. But this subgroup is actually the center of G, and is therefore a normal subgroup of G.

E: Suppose that G is a finite group and that N is a normal subgroup of G. Suppose also that G/N has an element of order m, where m is a positive integer. Carefully prove that G has an element of order m.

Solution. Suppose that G is a finite group, that N is a normal subgroup of G, and that G/N has an element of order m, where m is a positive integer.

The elements of G/N are of the form aN, where $a \in G$. Suppose that a is chosen so that aN is an element of G/N which has order m. The rest of this proof will concern the element a.

Since $a \in G$ and G is finite, it follows that the subgroup $\langle a \rangle$ of G is a finite group. Thus a has finite order. Let n be the order of a. In particular, $a^n = e$, where e is the identity element of G.

Since $a^n = e$, it follows that $(aN)^n = a^n N = eN = N$. Now we chose a at the beginning of this proof so that aN is an element in the group G/N of order m. Therefore, the fact that $(aN)^n = e$ implies that m divides n.

The subgroup $\langle a \rangle$ of G which is generated by a has order n. It is a cyclic group of order n. We proved in class that if m is a positive integer which divides n, then a cyclic group of order n must contain a subgroup H of order m and that subgroup must be cyclic. If $H = \langle b \rangle$, then b must have order m. Obviously, $b \in \langle a \rangle \subseteq G$. Hence G contains the element b and b has order m, as we wanted.

F: Suppose that A and B are groups. Let $G = A \times B$. Let e be the identity element of A and let f be the identity element of B. Then $(e,\ f)$ is the identity element in G. Let

$$H = \{ \ (a,\ f) \bigm| a \in A \ \} \quad .$$

Prove that H is a normal subgroup of G. Furthermore, prove that $H \cong A$ and that $G/H \cong B$.

Solution. To prove that H is a subgroup of G, observe that H obviously contains $(e,\ f)$ which is the identity element in G. Also, consider two elements $(a_1,\ f)$ and $(a_2,\ f)$ in H. Their product is $(a_1a_2,\ ff) = (a_1a_2,\ f)$ which is clearly in H. Finally, the inverse of an element $(a,\ f)$ in H is $(a^{-1},\ f)$, which is also in H. These remarks show that H is indeed a subgroup of G.

It will be useful to recall the following fact. If $a \in A$, then $aA = A$. We also have $Aa = A$. Now consider an element $(a,\ b) \in G$. Here $a \in A$ and $b \in B$. By definition, $H = \{ \ (c,\ f) \bigm| c \in A \ \}$. We have

$$\begin{aligned} (a,\ b)H \ &= \ \{ \ (a,\ b)(c,\ f) \bigm| c \in A \ \} \ = \ \{ \ (ac,\ bf) \bigm| c \in A \ \} \\ &= \ \{ \ (ac,\ b) \bigm| c \in A \ \} \ = \ \{ \ (k,\ b) \bigm| k \in A \ \} \quad . \end{aligned}$$

We have used the fact that $\{ac \ |c \in A\} = aA = A = \{k | k \in A\}$. Thus, the above left coset is just the set of elements in G whose second entry is equal to b. Similarly,

$$\begin{aligned} H(a,\ b) \ &= \ \{ \ (c,\ f)(a,\ b) \bigm| c \in A \ \} \ = \ \{ \ (ca,\ fb) \bigm| c \in A \ \} \\ &= \ \{ \ (ca,\ b) \bigm| c \in A \ \} \ = \ \{ \ (k,\ b) \bigm| k \in A \ \} \quad . \end{aligned}$$

We have used the fact that $Aa = A$. It follows that $(a,\ b)H = H(a,\ b)$ for all elements $(a,\ b) \in G$. Therefore, H is a normal subgroup of G.

To prove that H and A are isomorphic, consider the map $\varphi : A \to H$ defined by

$$\varphi(a) \ = \ (a,\ f)$$

for all $a \in A$. The map φ is clearly a bijection from A to H. Furthermore, if $a_1,\ a_2 \in A$, then we have

$$\varphi(a_1a_2) \ = \ (a_1a_2,\ f) \ = \ (a_1,\ f)(a_2,\ f) \ = \ \varphi(a_1)\varphi(a_2)$$

and hence the bijection φ is indeed an isomorphism from A to H.

Finally, we will prove that G/H and B are isomorphic. Note that the left coset $(a,\ b)H$ depends only on b , and not on a. Thus $(a,\ b)H = (e,\ b)H$. Thus, the elements of G/H are all of the form $(e,\ b)H$ for some $b \in B$. Furthermore, if $b_1,\ b_2 \in B$, we have $(e,\ b_1)H = (e,\ b_2)H$ if and only if $b_1 = b_2$. Define a map $\psi : B \to G/H$ by

$$\psi(b) \ = \ (e,\ b)H$$

for all $b \in B$. The above remarks show that ψ is bijective. Furthermore, for $b_1,\ b_2 \in B$, we have

$$\psi(b_1 b_2) \ = \ (e,\ b_1 b_2)H \ = \ (e,\ b_1)(e,\ b_2)H \ = \ (e,\ b_1)H(e,\ b_2)H \ = \ \psi(b_1)\psi(b_2) \ .$$

Thus, ψ is an isomorphism from B to G/H and hence those two groups are indeed isomorphic.