MATH 402A - Solutions for Assignment 2.

Page 47, problem 9: Assume that G is a group and that $a^2 = e$ for all $a \in G$. Suppose that a and b are arbitrary elements of G. Then ab is in G too. Hence, the assumption about G implies that $(ab)^2 = e$. That is, $(ab)(ab) = e$. We also have $a^2 = e$ and $b^2 = e$. Using these equations, we obtain the following equations:

$$e = (ab)(ab) = a(ba)b \qquad \textit{and} \qquad e = ee = a^2b^2 = (aa)(bb) = a(ab)b \quad .$$

It follows that $a(ba)b = a(ab)b$. We have used the associative law several times to derive some of the above equations. Now

$$a(ba)b = a(ab)b \quad \Longrightarrow \quad (ba)b = (ab)b \quad \Longrightarrow \quad ba = ab \quad .$$

We have used the cancellation law to derive these implications. It follows that $ab = ba$ for all choices of a and b in G. This proves that G is abelian.

Page 47, problem 13: We start with some general remarks. Let G be a group and let e denote the identity element of G. We have $ea = a$ and $ae = a$ for all $a \in G$. Thus, $ea = ae$ for all $a \in G$. Furthermore, suppose that $a, b \in G$ and $ab = e$. We have

$$ab = e \quad \Longrightarrow \quad ab = aa^{-1} \quad \Longrightarrow \quad b = a^{-1} \quad \Longrightarrow \quad ba = a^{-1}a = e \quad .$$

We have used the cancellation law to derive the second implication. Therefore, if $ab = e$, then it follows that $ba = e$ and hence that $ab = ba$.

Now suppose that G is a group of order 4. For all $a \in G$, we have $ea = ae = a$. Hence e commutes with every element of G. Now suppose that the other three elements of G are denoted by a, b and c. Thus, e, a, b, and c are all distinct and $G = \{e, a, b, c\}$.

Obviously, $aa = aa$. Hence a commutes with itself.

Now consider ab. We have $ab \in \{e, a, b, c\}$. We cannot have $ab = b$ or $ab = a$. To explain this, notice that

$$ab = b \implies ab = eb \implies a = e, \qquad ab = a \implies ab = ae \implies b = e \quad .$$

However, $a \neq e$ and $b \neq e$. It therefore follows that $ab \neq b$ and $ab \neq a$. This leaves two possibilities: either $ab = e$ or $ab = c$.

If we reverse the role of a and b in the previous paragraph, then we find that there are two possibilities for ba, namely either $ba = e$ or $ba = c$.

If $ab = e$, then we showed above that $ba = e$ and hence $ab = ba$. Similarly, reversing the role of a and b, if we have $ba = e$, then it follows that $ab = e$ and hence that $ab = ba$. There is only one case not yet covered, the case where ab and ba are both equal to c. But in that remaining case, we have $ab = c$ and $ba = c$ and so we have $ab = ba$. Hence a and b commute with each other in that case too.

The above argument can be applied to the pair of elements a and c. It shows that $ac = ca$. The argument applies to the pair b and c, showing that $bc = cb$. It follows that G is indeed an abelian group.

Now if $|G| = 1, 2$ or 3, a similar (and easier argument) works. Obviously, e commutes with all other elements of G. Thus, if $G = \{e\}$, nothing more needs to be proved. If $|G| = 2$, suppose $a \in G$ is the non-identity element. Now $ae = ea = a$ and $aa = aa$ and so a commutes with all elements of G, settling the case where $|G| = 2$. Finally, if $|G| = 3$, suppose $G = \{e, a, b\}$. The only non-obvious thing to prove is that $ab = ba$. Note that

$$ab = a \implies ab = ae \implies b = e, \qquad ab = b \implies ab = eb \implies a = e.$$

But $a \neq e$ and $b \neq e$. Therefore, $ab = e$. Similarly, $ba = e$. Hence $ab = ba$, finishing the case where $|G| = 3$.

Page 47, problem 15: As proven in class, $(a * b)^{-1} = (b^{-1}) * (a^{-1})$.

Page 47, problem 16: Suppose that $a,\ b \in G$, that $a = a^{-1},\ b = b^{-1}$, and that $ab = (ab)^{-1}$. According to problem 15 (although we omit the $*$), we have $(ab)^{-1} = b^{-1}a^{-1}$. Hence

$$ba = b^{-1}a^{-1} = (ab)^{-1} = ab \quad .$$

Under the assumptions of the problem, this argument applies to all pairs of elements $a, b \in G$. Thus $ab = ba$ for all $a, b \in G$. Hence G is abelian.

Note that this problem is virtually the same as problem 9. If G is a group and $a \in G$, then the equation $a^2 = e$ is equivalent to the equation $a^{-1} = a$. Thus, a group with the property stated in problem 9 is also a group with the property stated in this problem, and vice versa.

Page 54, problem 1: Let $C = A \cap B$. Let e denote the identity element of G. We assume that A and B are subgroups of G. First of all, we have $e \in A$ and $e \in B$. Hence $e \in C$.

Secondly, we show that C is closed under the operation of G. Suppose that $u, v \in C$. Then $u, v \in A$ and therefore, since A is closed, we have $uv \in A$. Similarly, $u, v \in B$ and therefore, since B is closed, we have $uv \in B$. Therefore, $uv \in C$.

Finally, suppose that $u \in C$. Let u^{-1} be the inverse of u in G. Then, $u \in A$ and since A is a subgroup of G, $u^{-1} \in A$. Similarly, $u \in B$ and since B is a subgroup of G, $u^{-1} \in B$. Therefore, $u^{-1} \in C$.

We have proved the three things that are needed to verify that C is a subgroup of G.

Page 54, problem 2: The subgroup of $\mathbf{Z}$ generated by -1 is the entire group $\mathbf{Z}$ itself. For if $n \in \mathbf{Z}$, then we can write $n = (-n)(-1)$, an integral multiple of -1. Since the operation is $+$, we have proved that -1 generates $\mathbf{Z}$.

Page 54, problem 4: First of all, $Z(G)$ contains e. This is so because $ea = a = ae$ for all $a \in G$. Hence $ea = ae$ for all $a \in G$ and that means that $e \in Z(G)$.

Secondly, suppose that $u, v \in Z(G)$. This means that $ua = au$ and $va = av$ for all $a \in G$. Therefore,

$$(uv)a = u(va) = u(av) = (ua)v = (au)v = a(uv)$$

for all $a \in G$. This means that $uv \in Z(G)$. Hence $Z(G)$ is closed under the operation for G.

Now assume that $u \in Z(G)$. This means that $ua = au$ for all $a \in G$. Let u^{-1} be the inverse of u in G. Let b be an arbitrary element of G and let $a = b^{-1}$, an element of G. Hence

$$u^{-1}b = u^{-1}a^{-1} = (au)^{-1} = (ua)^{-1} = a^{-1}u^{-1} = bu^{-1}$$

and hence u^{-1} commutes with b for all $b \in G$. Thus, $u^{-1} \in Z(G)$.

We have proved the three things that are needed to verify that $Z(G)$ is a subgroup of G.

Page 55, problem 6: Suppose that $a \in Z(G)$. Hence, for all $b \in G$, we have $ab = ba$. Therefore, for all $b \in G$, we have $b \in C(a)$. Therefore, $C(a) = G$.

Conversely, suppose $C(a) = G$. Then, if $b \in G$, we have $b \in C(a)$ and that means that $ba = ab$. Therefore, for all $b \in G$, we have $ba = ab$. Therefore, $a \in Z(G)$.

Page 55, problem 8: Let e denote the identity element of G. The subset H is defined by

$$H = \{a \in G \mid a^2 = e\}$$

First of all, $e^2 = ee = e$ and hence $e \in H$. Secondly, if $a, b \in H$, then

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2 = ee = e$$

and therefore $ab \in H$. We have used the associative law (many times), the fact that $ab = ba$ (which is true because G is assumed to be abelian), and the assumption that $a, b \in H$ (so that $a^2 = b^2 = e$). Therefore, $a, b \in H \implies ab \in H$. That is, H is closed under the group operation for G.

Finally, suppose that $a \in H$. Since $a^2 = e$, we have $aa = e$. That is, $a^{-1} = a$. Therefore, $a^{-1} \in H$.

We have proved the three things that are needed to verify that H is a subgroup of G.

Page 55, problem 9: One example is $G = S_3$. The identity element e for G is the identity map i. Consider the two elements

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad g' = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

which are in G. It is easy to verify that $g^2 = i$ and $(g')^2 = i$. Thus, both g and g' are in the subset H defined in problem 8. However,

$$gg' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

and

$$(gg')^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq i.$$

Thus, $gg' \notin H$. Therefore, H is not closed under the group operation for G and therefore is not a subgroup of G