Math 110A HW §3.2 – Solutions

4. An element x in a multiplicative group G is called idempotent if $x^2 = x$. Prove that the identity element e is the only idempotent element in a group G.

   Proof. Let G be a a group. Let $x \in G$ such that $x^2 = x$. Since $x = xe$, we have that $x^2 = xe$. In other words, $xx = xe$. Since G is a group, cancellation holds. Thus, cancelling x, we get $x = e$. Thus the only idempotent in G is e. □

9. Let G be a group.

   (a) Define the relation R on G by xRy if and only if there exists $a \in G$ such that $y = a^{-1}xa$. Prove R is an equivalence relation.

   Proof. Let $x, y, z \in G$ and let e be the identity in G. Then $x = e^{-1}xe$. Thus xRx.
   Assume xRy. So there exists $a \in G$ such that $y = a^{-1}xa$. Multiplying on the left by a we get $ay = xa$. Multiplying on the right by a^{-1}, we get $aya^{-1} = x$. Now, since $(a^{-1})^{-1} = a$, we have that $aya^{-1} = x$ implies $(a^{-1})^{-1}y(a^{-1}) = x$. However, since $a \in G$, $a^{-1} \in G$. Thus yRx.
   Assume xRy and yRz. So there exists $a, b \in G$ such that $y = a^{-1}xa$ and $z = b^{-1}yb$. Substituting, we get

   $$z = b^{-1}yb = b^{-1}(a^{-1}xa)b = (b^{-1}a^{-1})x(ab) = (ab)^{-1}x(ab)$$

   Since $a, b \in G$, $ab \in G$. Hence zRx.
   Thus R is an equivalence relation. □

   (b) Let $x \in G$. Find $[x]$, if G is abelian.
   Let $y \in [x]$, then $y = a^{-1}xa$. Since G is abelian, $y = a^{-1}xa$ implies $y = a^{-1}ax$. So $y = x$. Thus the only element in $[x]$ is x. In other words, $[x] = \{x\}$.

13. Prove that if $x = x^{-1}$ for all x in the group G, then G is abelian.

    Proof. Assume $x = x^{-1}$ for all $x \in G$. Let $a, b \in G$. Then $ab \in G$, thus $(ab)^{-1} = ab$. By the reverse order law of inverses, $(ab)^{-1} = b^{-1}a^{-1}$. Therefore we have $b^{-1}a^{-1} = ab$. Finally since $a^{-1} = a$ and $b^{-1} = b$, we have $ba = ab$. Thus G is abelian. □

15. Let G be a group. Prove that G is abelian if and only if $(xy)^2 = x^2y^2$ for all x and y in G.

    Proof.

    ($\Rightarrow$) Assume G is abelian. Let $x, y \in G$. Then $(xy)^2 = xyxy = xxyx$ since G is abelian, and of course $xxyy = x^2y^2$. Thus $(xy)^2 = x^2y^2$.

    ($\Leftarrow$) Assume $(xy)^2 = x^2y^2$ for all $x, y \in G$. Then we have the following.

    $$\begin{aligned}(xy)^2 &= x^2y^2\\ xyxy &= xxyy\\ x^{-1}xyxy &= x^{-1}xxyy\\ yxy &= xyy\\ yxyy^{-1} &= xyyy^{-1}\\ yx &= xy\end{aligned}$$

    Thus G is abelian.

$\square$

20. Prove or disprove that every group of order 3 is abelian.

Proof. Since G has order 3, let $G = \{e, a, b\}$, where e is the identity. Clearly $ea = a = ae$ and $eb = b = be$. Now let's consider what ab could equal. If $ab = a$, then $ab = ae$ and by cancellation, $b = e$ which is a contradiction. Similarly, if $ab = b$, then $ab = eb$ and by cancellation $a = e$, which is a contradiction. Thus ab must equal e. We can use the same argument to show that $ba = e$. Thus $ab = ba$. Hence in all products, order does not matter. Therefore G is abelian. $\square$

23. Suppose that G is a nonempty set that is closed under an associative binary operation $*$ and that the following two conditions hold:

    (a) There exists a left identity e in G such that $e * x = x$ for all $x \in G$.

    (b) Each $a \in G$ has a left inverse $a_l \in G$ such that $a_l * a = e$.

Prove G is a group.

Proof. We need only show that e is the identity and the inverse of a is a_l.

$$\begin{aligned}
(a_l * a) * e &= a_l * (a * e) \quad \text{by associativity.}\\
e * e &= a_l * (a * e) \quad \text{since } a_l * a = e.\\
e &= a_l * (a * e) \quad \text{since } e \text{ is a left identity.}\\
a_l * a &= a_l * (a * e) \quad \text{since } a_l * a = e.\\
a_{ll} * (a_l * a) &= a_{ll} * \big(a_l * (a * e)\big) \quad \text{where } a_{ll} \text{ is the left inverse of } a_l.\\
(a_{ll} * a_l) * a &= (a_{ll} * a_l) * (a * e) \quad \text{by asociativity.}\\
e * a &= e * (a * e) \quad \text{since } a_{ll} \text{ is the left inverse of } a_l.\\
a &= a * e \quad \text{since } e \text{ is a left identity.}
\end{aligned}$$

Thus we have shown that $a * e = a$, and we already knew $e * a = a$. Thus e is the identity.

Now let's show a_l is a right inverse of a. So we need to show that $a * a_l = e$.

$$\begin{aligned}
a * a_l &= a * (e * a_l) \quad \text{since } e \text{ is the identity.}\\
a * a_l &= a * \big((a_l * a) * a_l\big) \quad \text{since } a_l \text{ is the left inverse of } a.\\
a * a_l &= (a * a_l) * (a * a_l) \quad \text{by associativity.}\\
(a * a_l) * e &= (a * a_l) * (a * a_l) \quad \text{since } e \text{ is the identity.}\\
a' * \big((a * a_l) * e\big) &= a' * \big((a * a_l) * (a * a_l)\big) \quad \text{where } a' \text{ is the left inverse of } a * a_l.\\
(a' * (a * a_l)) * e &= (a' * (a * a_l)) * (a * a_l) \quad \text{by associativity.}\\
e * e &= e * (a * a_l) \quad \text{since } a' \text{ is the left inverse of } a * a_l.\\
e &= a * a_l \quad \text{since } e \text{ is the identity.}
\end{aligned}$$

Thus we have shown that $a * a_l = e$, and we already knew $a_l * a = e$. Thus a_l is the inverse of a.

Therefore G is a group.

$\square$