Abstract Algebra Homework 2

Zachary Meyner

41. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup if $\mathbb{R}^*$ under the group operation of multiplication.

Proof. Let $n, m \in G$ *s.t.* $n = a + b\sqrt{2}$ and $m = c + d\sqrt{2}$.
(WTS: $n \cdot m \in G$ and $n^{-1} \in G$)
Multiplying $m \cdot n$ we have

$$\begin{aligned}
(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= ac + ad\sqrt{2} + bc\sqrt{2} + bd\sqrt{2}^2 && \text{(Distributive Property)} \\
&= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\
&= ac + \sqrt{2}(ad + bc) + 2bd && \text{(Distributive Property)} \\
&= (ac + 2bd) + (ad + bc)\sqrt{2} && \text{(Commutative and Associative Property)}
\end{aligned}$$

and $(ac + 2bd) + (ad + bc)\sqrt{2}$ is clearly an in G, so $n \cdot m$ must be in G. Now if we take n^{-1} we get

$$\begin{aligned}
\frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{(a - b\sqrt{2})}{(a - b\sqrt{2})} && \text{(Multiplying by 1)} \\
&= \frac{a - b\sqrt{2}}{(a + b\sqrt{2}) \cdot (a - b\sqrt{2})} \\
&= \frac{a - b\sqrt{2}}{a^2 - b\sqrt{2}^2} && \text{(Distributive Property)} \\
&= \frac{a + (-b)\sqrt{2}}{a^2 - 2b} && \text{(Simplifying)} \\
&= \frac{a}{a^2 - 2b} + \frac{-b}{a^2 - 2b}\sqrt{2} && \text{(Commutative and Associative Propety)}
\end{aligned}$$

Because a and b are in $\mathbb{Q}$ we know $\frac{a}{a^2-2b}$ and $\frac{-b}{a^2-2b}$ must also be in $\mathbb{Q}$, so n^{-1} must be in G.
$\therefore$ By the 2 step test G is a subgroup of $\mathbb{R}^*$ under the operation of multiplication. ■

45. Prove that the intersection of two subgroups of a group G is also a subgroup of G.

Proof. Let $P \leq G$ and $H \leq G$. We know that at least the identity element $e \in P \cap H$ Let $a, b \in P \cap H$ (WTS: $ab^{-1} \in P \cap H$). Because $a, b \in P \cap H$ we know

$$\begin{aligned} & a \in P \cap H \\ \implies & a \in P \text{ and } a \in H \\ & b \in P \cap H \\ \implies & b \in P \text{ and } b \in H \end{aligned}$$

Since P and H are subgroups of G we have

$$\begin{aligned} & ab^{-1} \in P \text{ and } ab^{-1} \in H \\ \implies & ab^{-1} \in P \cap H \end{aligned}$$

Thus $P \cap H$ is also a subgroup of G. ■

5. Find the order of every element in $\mathbb{Z}_{18}$.

$$\begin{aligned} |1| &= 18 \\ |2| &= 9 \\ |3| &= 6 \\ |4| &= 9 \\ |5| &= 18 \\ |6| &= 3 \\ |7| &= 18 \\ |8| &= 9 \\ |9| &= 2 \\ |10| &= 9 \\ |11| &= 18 \\ |12| &= 3 \\ |13| &= 18 \\ |14| &= 9 \\ |15| &= 6 \\ |16| &= 9 \\ |17| &= 18 \end{aligned}$$

23. Let $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.

Proof. Let $a^n = e$, then

$$\begin{aligned} e &= (aa^{-1})^n \\ &= a^n(a^{-1})^n \\ &= e(a^{-1})^n \\ &= (a^{-1})^n \end{aligned}$$

So $|a^{-1}| \leq n$. Now we let $(a^{-1})^m = e$, similarly we have

$$\begin{aligned} e &= (aa^{-1})^m \\ &= a^m(a^{-1})^m \\ &= a^m e \\ &= a^m \end{aligned}$$

So $|a| \leq m$. Thus we have both $|a^{-1}| \leq n \implies m \leq n$,
and $|a| \leq m \implies n \leq m$. Therefore $m = n$ and $|a| = |a^{-1}|$ ∎

(b) For all $g \in G, |a| = |g^{-1}ag|$

Proof. Let $|a| = n$, then $a^n = e$. Furthermore

$$\begin{aligned} (g^{-1}ag)^n &= g^{-1}agg^{-1}ag \ldots g^{-1}ag \\ &= g^{-1}ag && \text{(Cancelling } g^{-1}g\text{)} \\ &= g^{-1}eg \\ &= g^{-1}g \\ &= e \end{aligned}$$

So $|g^{-1}ag| \leq n$. Now let $c = g$. The same steps can be used to show that $|cg^{-1}agc^{-1}| \leq |g^{-1}ag|$. But $cg^{-1}agc^{-1} = gg^{-1}agg^{-1} = a$. Thus $|a| \leq |g^{-1}ag|$ or $n \leq |g^{-1}ag| \leq n$. Therefore $|g^{-1}ag| = n = |a|$. ∎

(c) The order of ab is the same as the order of ba.

Proof. Let $|ab| = n$, then $(ab)^n = e$. We show

$$\begin{aligned} (ba)^n &= (ba)^n e \\ &= (ba)^n bb^{-1} \\ &= bababa \ldots babb^{-1} \\ &= b(ab)^n b^{-1} && \text{(Associative Property)} \\ &= beb^{-1} \\ &= bb^{-1} \\ &= e \end{aligned}$$

So $|ba| \leq n$. Next we let $|ba| = m$, then $(ba)^m = e$. We can show again that

$$\begin{aligned}
(ab)^m &= (ab)^m e \\
&= (ab)^m a a^{-1} \\
&= ababab \ldots abaa^{-1} \\
&= a(ba)^m a^{-1} && \text{(Associative Property)} \\
&= aea^{-1} \\
&= aa^{-1} \\
&= e
\end{aligned}$$

So $|ab| \leq m$. From here we know $m \leq n$ and $n \leq m$.
Thus $n = m$ and $|ab| = |ba|$. ■