Quiz 4

Allen Williams

February 14th, 2018

1. Prove that $G = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}, a, b \text{ not both zero}\}$ is a subgroup of $\mathbb{R}^*$, the multiplicative group of non-zero real numbers. Let $x, y \in G$ then $x = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$ and $y = a' + b'\sqrt{3}$ for some $a', b' \in \mathbb{Q}$. Then $y^{-1} = \frac{1}{a'+b'\sqrt{3}}$, so $x \cdot y^{-1} = \frac{a+b\sqrt{3}}{a'+b'\sqrt{3}} = \frac{a+b\sqrt{3}}{a'+b'\sqrt{3}} \cdot \frac{a'-b'\sqrt{3}}{a'-b'\sqrt{3}}$ $= \frac{aa'-3bb'}{(a')^2-3(b')^2} + \frac{a'b-ab'}{(a')^2-3(b')^2}\sqrt{3}$. So when $x, y \in G$, $x \cdot y^{-1} \in G$ which is a necessary and sufficient condition for G being a subgroup of $\mathbb{R}^*$.

2. Prove the $SL_2(\mathbb{Z})$ is a subgroup of $SL_2(\mathbb{R})$. Clearly $SL_2(\mathbb{Z})$ is a subset of $SL_2(\mathbb{R})$ since $\mathbb{Z}$ is a subset of $\mathbb{R}$. Let $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $Y = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be elements of $SL_2(\mathbb{Z})$, that is $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ and $\det(X) = \det(Y) = 1$. Then $XY^{-1} = \frac{1}{\det(Y)} X \cdot adj(Y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} = \begin{pmatrix} ad' - bc' & a'b - ab' \\ cd' - c'd & a'd - b'c \end{pmatrix}$. Since the entries in X and Y^{-1} are integers, the entries in XY^{-1} are also integers. Also since $\det(Y) = 1$, $\det(Y^{-1}) = \frac{1}{1} = 1$, so $\det(XY^{-1}) = \det(X)\det(Y^{-1}) = 1 \cdot 1 = 1$, so $XY^{-1} \in SL_2(\mathbb{Z})$ when $X, Y \in SL_2(\mathbb{Z})$, meaning $SL_2(\mathbb{Z})$ is a subgroup of $SL_2(\mathbb{R})$.

3. $< \mathbb{Q}, + >$ the additive group of rational numbers is not cyclic. First note that if $\mathbb{Q}$ were generated by one of its elements, that element could not be 0, since 0 is the identity element in $< \mathbb{Q}, + >$ so $< 0 >= \{0\}$. Now Assume for contradiction that $\mathbb{Q} =< a >$ for some $a \in \mathbb{Q}$ with $a \neq 0$, that is for all $q \in \mathbb{Q}$, there exists an integer k, such that $q = ka$. Since a is itself rational, $\frac{a}{2}$ must also be rational. Consider $q = \frac{a}{2}$, then $a = 2ka$. Since $a \neq 0$, $2k = 1$ so $k = \frac{1}{2}$, which contradicts the fact that k is an integer, so $< \mathbb{Q}, + >$ cannot be cyclic.

4. What is the order of [4] in $U(21)$? Find the subgroup of $U(21)$ generated by [4]. The order of [4] in $U(21)$ is 3 since $[4]^3 = [4 * 4 * 4] = [64] = [1]$. $< [4] >= \{[4], [16], [1]\}$.

5. $U(5)$ is a cyclic group and its generators are [2] and [3]. $U(5)$ consists of the elements $\{[1], [2], [3], [4]\}$. Also $[2] \cdot [3] = [6] = [1]$ so $[2] = [3]^{-1}$ so the

subgroups $<[2]>$ and $<[3]>$ will be the same.

$$\begin{aligned}
[2]^1 &= [2] \\
[2]^2 &= [4] \\
[2]^3 = [8] &= [3] \\
[2]^4 = [16] &= [1]
\end{aligned}$$

So $<[2]>=<[3]>=U(5)$. [1] is the identity element in $U(5)$ so it cannot generate $U(5)$, and [4] is its own inverse so it cannot generate $U(5)$ so [2] and [3] are the only generators for $U(5)$. Since [4] is its own inverse, $<[4]>=\{[4],[1]\}$ which is a non-trivial subgroup of $U(5)$.

6. Find all non-trivial cyclic subgroups of $<\mathbb{Z}_8,+>$. [0] is the identity on $<\mathbb{Z}_8,+>$ so $<[0]>$ is the trivial group. Also since $[1]=[7]^{-1}$, $[2]=[6]^{-1}$, and $[3]=[5]^{-1}$, and an element generates the same cyclic subgroup as its inverse, it is enough to find $<[1]>, <[2]>, <[3]>$, and $<[4]>$.

$$\begin{aligned}
[1] &= [1] \\
[1]+[1] &= [2] \\
[1]+[1]+[1] &= [3] \\
[1]+[1]+[1]+[1] &= [4] \\
[1]+[1]+[1]+[1]+[1] &= [5] \\
[1]+[1]+[1]+[1]+[1]+[1] &= [6] \\
[1]+[1]+[1]+[1]+[1]+[1]+[1] &= [7] \\
[1]+[1]+[1]+[1]+[1]+[1]+[1]+[1] = [8] &= [0]
\end{aligned}$$

So $<[1]>=\{[0],[1],[2],[3],[4],[5],[6],[7]\}$

$$\begin{aligned}
[2] &= [2] \\
[2]+[2] &= [4] \\
[2]+[2]+[2] &= [6] \\
[2]+[2]+[2]+[2] = [8] &= [0]
\end{aligned}$$

So $<[2]>=\{[0],[2],[4],[6]\}$

$$\begin{aligned}
[3] &= [3] \\
[3]+[3] &= [6] \\
[3]+[3]+[3] = [9] &= [1] \\
[3]+[3]+[3]+[3] = [12] &= [4] \\
[3]+[3]+[3]+[3]+[3] = [15] &= [7] \\
[3]+[3]+[3]+[3]+[3]+[3] = [18] &= [2] \\
[3]+[3]+[3]+[3]+[3]+[3]+[3] = [21] &= [5] \\
[3]+[3]+[3]+[3]+[3]+[3]+[3]+[3] = [24] &= [0]
\end{aligned}$$

So $< [3] >= \{[0],[1],[2],[3],[4],[5],[6],[7]\}$

$$[4] = [4]$$
$$[4] + [4] = [8] = [0]$$

So $< [4] >= \{[4],[0]\}$