The RLWE problem used by the CKKS encryption scheme considers the mathematical objects, \textit{rings}. To understand \textit{rings}, \textit{groups} must first be understood. A group $(\mathbb{G}, \bullet)$ is a set, $\mathbb{G}$, and an operator, $\bullet: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$, such that the following properties hold:

\begin{itemize}

\item \textbf{Closure}: $a \bullet b \in \mathbb{G}$ for all $a,b \in \mathbb{G}$.

\item \textbf{Associativity}: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c \in \mathbb{G}$.

\item \textbf{Neutral Element}: there exists an $e \in \mathbb{G}$ such that for all $a \in \mathbb{G}$, $a \bullet e = e \bullet a = a$.

\item \textbf{Inverse Element}: for each $a \in \mathbb{G}$ there exists some $b \in \mathbb{G}$ such that $a \bullet b = b \bullet a = e$.

\end{itemize}

If $a \bullet b = b \bullet a$ for all $a, b \in \mathbb{G}$, the group is called \textbf{commutative} (or \textbf{abelian}). If there is no inverse element for each element, $(\mathbb{G}, \bullet)$ is a \textbf{monoid} instead.

From this, a \textit{ring} is defined as $(\textbf{R}, \boxplus, \boxtimes)$, where $\textbf{R}$ is a set, $\boxplus: \textbf{R} \times \textbf{R} \rightarrow \textbf{R}$, and $\boxtimes: \textbf{R} \times \textbf{R} \rightarrow \textbf{R}$, such that

\begin{itemize}

\item $(\textbf{R}, \boxplus)$ is an abelian group.

\item $(\textbf{R}, \boxtimes)$ is a monoid.

\item $\boxplus$ and $\boxtimes$ are distributive – for all $a, b, c \in \textbf{R}$, $a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c)$ and $(a \boxplus b) \boxtimes c = (a \boxtimes c) \boxplus (b \boxtimes c)$.

\end{itemize}

If $a \boxtimes b = b \boxtimes a$ then it is a \textbf{commutative} ring, but this is not necessary for rings generally. One example of a ring is $(\mathbb{Z}[x], +, \times)$.