Class Groups with Binary Quadratic Forms

Mike Wang

November 8, 2017

Today, we will be talking about composition of equivalence classes of quadratic binary forms, and how this forms an abelian group. Specifically, I will review what an abelian group is, and prove that the composition operator of quadratic binary form that we have defined satisfies the identity, invertability, and commutativity properties of an abelian group. Mark will show that the operator also satisfies associativity. First, recall these definitions.

**Definition 1.** A group is a set of elements $S$ and operation $\ast$, that satisfies **identity**, **invertability**, and **associativity** conditions.

For the **identity** condition, there is an element $i \in S$ such that $\forall s \in S, s \ast i = i \ast s = s$.

For the **invertability** condition, $\forall s \in S, \exists -s \in S$ such that $s \ast -s = i$, the identity.

For the **associativity** condition, for any $a, b, c \in S$, $(a \ast b) \ast c = a \ast (b \ast c)$.

**Definition 2.** An abelian group over elements $S$ and operation $\ast$ also satisfies **commutativity**, which means that for any $a, b \in S$, $a \ast b = b \ast a$.

**Definition 3.** Recall that the composition of two binary quadratic forms is equivalent to the composition of two equivalent **nice** binary quadratic forms $Q_1 = (a_1, B, a_2 C)$ and $Q_2 = (a_2, B, a_1 C)$, where $Q_1 \circ Q_2 = (a_1 a_2, B, C)$. It was shown that any two primitive binary quadratic forms have equivalence **nice** forms.

The next theorem is the main result that we will prove today.

**Theorem 1.** Let $Q_\Delta$ be the set of equivalence classes of primitive binary quadratic forms with discriminant $\Delta$. Then, $Q_\Delta$ with the composition operator is an abelian group.

We will prove the identity, invertability, and commutavity properties in this lecture.

**Lemma 1 (Identity).** $q_i \in Q_\Delta$, the identity for the composition operator, is $[(1, \ast, \ast)]$

We will prove this lemma in 2 steps - first, we will show that for any BQF $(a, b, c)$, we can find another BQF $(1, \ast, \ast)$ such that $(a, b, c) \circ (1, \ast, \ast) = (a, b, c)$. Second, we will show that all BQF’s of the form $(1, \ast, \ast)$ makes up an equivalence class. We will prove this second statement as another lemma.
Lemma 2. Let \((1, b_1, c_1)\) and \((1, b_2, c_2)\) be BQF’s with the same discriminant. These BQF’s must be equivalent.

Proof. Notice that \(b_1\) and \(b_2\) must have the same parity, since \(b_1^2 - 4c_1 = b_2^2 - 4c_2\) implies that \(b_1 \equiv b_2 \mod 2\). Then, the matrix \[
\begin{bmatrix}
1 & \frac{b_2 - b_1}{2} \\
\frac{b_1}{2} & c_1
\end{bmatrix}
\] would transform the first form into the second form.

\[
\begin{bmatrix}
1 & 0 \\
\frac{b_1}{2} & c_1
\end{bmatrix}
\begin{bmatrix}
1 & \frac{b_2 - b_1}{2} \\
0 & 1
\end{bmatrix}
= \begin{bmatrix}
1 & \frac{b_1}{2} \\
0 & 1
\end{bmatrix}
\begin{bmatrix}
\frac{b_2}{4} + c_1 & \frac{b_2 - b_1}{2} \\
\frac{b_1}{2} & 1
\end{bmatrix}
= \begin{bmatrix}
1 & \frac{b_2}{2} \\
\frac{b_1}{2} & \text{something}
\end{bmatrix}
\]

Notice that because the determinants of the two forms are the same, we do not need to calculate \text{something}.

Proof of lemma 1. Consider any quadratic binary form \((a, b, c)\). Notice that \((1, b, ac)\) is nice with this binary quadratic form. Thus, the composition of the two forms is \((a, b, c)\).

From lemma 2, we have shown that all binary quadratic forms that begin with 1 (of the form \((1, *, *)\)) are equivalent. This shows that the equivalence class of the form \((1, *, *)\) is the identity element.

Lemma 3 (Invertability). For any equivalence class \(q_1 = [(a, b, c)]\), we could find an inverse equivalence class \(q_2 = [(c, b, a)]\) such that \(q_1 \circ q_2 = q_i\).

Proof. Consider the quadratic binary form \((a, b, c)\). Notice that the quadratic binary form \((c, b, a)\) is nice with this form. Therefore, the composition of the two forms is \((ac, b, 1)\). Notice that the matrix \[
\begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix}
\] transforms \((ac, b, 1)\) to \((1, -b, ac)\), which is the identity.

Lemma 4 (Commutativity). For any two equivalence classes \(q_1, q_2 \in Q_\Delta\), then \(q_1 \circ q_2 = q_2 \circ q_1\).

Proof. From last week, we know that there is a BQF in \(q_1\) and a BQF in \(q_2\) such that the BQF’s are nice. Let the two binary quadratic forms be \((a_1, B, a_2C)\) \(\in q_1\) and \((a_2, B, a_1C)\) \(\in q_2\) for some \(a_1, a_2, B, C \in \mathbb{Z}\). Then, we can easily see that \(q_1 \circ q_2 = q_2 \circ q_1 = [(a_1a_2, B, C)]\)