Class Groups with Binary Quadratic Forms

Mark Wang

November 6, 2017

We will now prove associativity for the composition of equivalence classes of binary quadratic forms. Namely, for primitive quadratic forms $f_1, f_2, f_3$ with discriminant $D = \Delta$, we prove that $(f_1 \circ f_2) \circ f_3 \sim f_1 \circ (f_2 \circ f_3)$. For the proof, we will first show the lemma that we can find pairwise relatively prime numbers: $a_1, a_2, a_3$ s.t. $a_1, a_2, a_3$ s.t. $f_1 \sim (a_1, B, a_2a_3C), f_2 \sim (a_2, B, a_1a_3C), \text{ and } f_3 \sim (a_3, B, a_1a_2C)$.

**Lemma 1.** Let $f_1, f_2, f_3$ represent primitive binary quadratic forms with the same discriminant $D = \Delta$. Then, for any $f_1, f_2, f_3$ we can find pairwise relatively prime integers: $a_1, a_2, a_3$ s.t. $f_1 \sim (a_1, B, a_2a_3C), f_2 \sim (a_2, B, a_1a_3C), \text{ and } f_3 \sim (a_3, B, a_1a_2C)$ s.t. $B, C \in \mathbb{Z}$.

**Proof.** The proof utilizes two different propositions which were defined and proved in previous lectures.

**Proposition 1.** Given any integer $m$ and a primitive form $Q$, there exists an $a_j$ relatively prime to $m$ such that $Q$ properly represents $a_j$.

**Proposition 2.** If $Q$ represents $a_j$, then $Q$ is equivalent to $Q' = a_jx^2 + b_jxy + c_jy^2$ for some integers $b_j, c_j$

Let us have $(a_1, b_1, c_1)$ represent $f_1$. From proposition 1, we can set $m = a_1$, and see that given $f_2$, there exists a number, which we call $a_2$ relatively prime to $m$ such that $f_2$ represents $a_2$. We then apply proposition 2 to see that there is form $f_2' = (a_2, b_2, c_2) \sim f_2$ for some integers $b_2, c_2$. Now, let us set $m = a_1, a_2$. We see that given $f_3$, there exists a number, which we call $a_3$ relatively prime to $m$ such that $f_3$ represents $a_3$. We then apply proposition 3 to see there is form $f_3' = (a_3, b_3, c_3) \sim f_3$ for some integers $b_3, c_3$.

We now need to find a way to make these forms nice. In order to show this we can use another result proven in a previous lecture.

**Proposition 3.** If $(a_1, b_1, c_1)$ and $(a_2, b_2, c_2)$ are united, then there are integers $B$ and $C$ such that $(a_1, b_1, c_1) \sim (a_1, B, a_2C), (a_2, b_2, c_2) \sim (a_2, B, a_1C)$

In particular, recall that for the proof of proposition 3, we transformed $(a_1, b_1, c_1)$ by the matrix $\begin{bmatrix} 1 & r_1 \\ 0 & 1 \end{bmatrix}$ and transformed $(a_2, b_2, c_2)$ by the matrix $\begin{bmatrix} 1 & r_2 \\ 0 & 1 \end{bmatrix}$ We see that since the transformation matrix has determinant one, then the resulting transformed binary quadratic forms would be equivalent. Recall that the transformation ”M” is applied on quadratic form ”Q” by
the formula $M^{TQM}$. The transformation maps $(a_1, b_1, c_1)$ to $(a_1, b_1 + 2a_1 r_1, a_1 r_1^2 + b_1 r_1 + c_1)$ and maps $(a_2, b_2, c_2)$ to $(a_2, b_2 + 2a_2 r_2, a_2 r_2^2 + b_2 r_2 + c_2)$. Thus we see that $B = b_1 + 2a_1 r_1 = b_2 + 2a_2 r_2$, which can be rearranged to $(b_1 - b_2)/2 = a_2 r_2 - a_1 r_1$. Since the GCD of $a_1$ and $a_2$ must be equal to 1 (by definition), then by Bezout’s theorem, we know that there is a solution for $r_1, r_2$. Since $a_1$ and $a_2$ are relatively prime, then $B = B_0 + 2a_1 a_2 \ast k$, where $B_0$ represents an initial solution and $k$ represents an integer. Meanwhile, we see that if we applied transformation matrix \[
\begin{bmatrix} 1 & r_3 \\ 0 & 1 \end{bmatrix}
\] to $(a_3, b_3, c_3)$, we get $(a_3, b_3 + 2a_3 r_3, a_3 r_3^2 + b_3 r_3 + c_3)$. Thus we want to find $k$ and $r_3$ such that $B_0 + 2a_1 a_2 \ast k = b_3 + 2a_3 r_3$. Rearranging, we get $(B_0 - b_3)/2 = a_3 r_3 - a_1 a_2 \ast k$. Since $a_1, a_2, a_3$ are pairwise relatively prime, then $a_1 a_2$ is relatively prime to $a_3$. Thus we can apply Bezout’s theorem again, to see that a solution for $k, r_3$ must exist.

Now, we must verify whether the third terms of each BQF are divisible by the first term of the other two BQF. We know that since the discriminant of all the binary quadratic equations are equal and using the fact that the middle term is the same for all BQF, then $4 \ast (a_1) \ast (a_1 r_1^2 + b_1 r_1 + c_1) = 4 \ast (a_2) \ast (a_2 r_2^2 + b_2 r_2 + c_2) = 4 \ast (a_3) \ast (a_3 r_3^2 + b_3 r_3 + c_3)$. Since $a_1, a_2, a_3$ are pairwise relatively prime, then this means that $a_1 r_1^2 + b_1 r_1 + c_1$ is divisible by $a_2$ and $a_3, a_2 r_2^2 + b_2 r_2 + c_2$ is divisible by $a_1$ and $a_3$, and $a_3 r_3^2 + b_3 r_3 + c_3$ is divisible by $a_1$ and $a_2$. Thus we can divide each term by $4a_1 a_2 a_3$ to receive:

\[
\frac{a_1 r_1^2 + b_1 r_1 + c_1}{(a_2 a_3)} = \frac{(a_2 r_2^2 + b_2 r_2 + c_2)}{(a_1 a_3)} = \frac{(a_3 r_3^2 + b_3 r_3 + c_3)}{(a_1 a_2)} = C
\]

Thus the forms would be $(a_1, B, a_2 a_3 C), (a_2, B, a_1 a_3 C), (a_3, B, a_1 a_2 C)$.

\[
\square
\]

Lemma 2. $(f_1 \circ f_2) \circ f_3 \sim f_1 \circ (f_2 \circ f_3)$

Proof. Using Lemma 1, we know that we can find equivalent forms:

$(a_1, B, a_2 a_3 C), (a_2, B, a_1 a_3 C), (a_3, B, a_1 a_2 C)$ such that: $(a_1, B, a_2 a_3 C) \sim f_1, (a_2, B, a_1 a_3 C) \sim f_2, (a_3, B, a_1 a_2 C) \sim f_3$. Then applying the law of compositions directly, we have that:

$(f_1 \circ f_2) \circ f_3 = ((a_1, B, a_2 a_3 C) \circ (a_2, B, a_1 a_3 C)) \circ (a_3, B, a_1 a_2 C) = (a_1 a_2, B, a_3 C) \circ (a_3, B, a_1 a_2 C) = (a_1 a_2 a_3, B, C)$

Meanwhile, we also have:

$f_1 \circ (f_2 \circ f_3) = (a_1, B, a_2 a_3 C) \circ ((a_2, B, a_1 a_3 C) \circ (a_3, B, a_1 a_2 C)) = (a_1, B, a_2 a_3 C) \circ (a_2 a_3, B, a_1 C) = (a_1 a_2 a_3, B, C)$

\[
\square
\]