Chapter 6
AUTOMORPHISMS OF FORMS

We begin by recalling some notation. If \( F = [a, b, c] \), the matrix form of \( F \) is \( [F] = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \). If \( S \) is the substitution \( S: X \to rX + tY, \ Y \to sX + uY \), the matrix form of \( S \) is \( [S] = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \). Recalling that \( SF \) is the form resulting from applying \( S \) to \( F \), Lemma 1.2(g) says \( [S][F][S]^T = [SF] \). Thus having \( SF = F \) is equivalent to having \( [S][F][S]^T = [F] \).

Definitions: The substitution \( S \) is an automorphism of the form \( F \) if \( SF = F \). An automorphism \( S \) of \( F \) is either proper or improper, depending on whether \( S \) is a proper or improper substitution. The sets of automorphisms, proper automorphisms, and improper automorphisms of \( F \) will be denoted \( \text{Aut}(F) \), \( \text{Aut}^+(F) \), and \( \text{Aut}^-(F) \), respectively.

Recall that to complete the proof of Gauss' duplication theorem, we must find the size of \( \text{AMB}(\Delta) \). Now \( \text{PEC}(F) \in \text{AMB}(\Delta) \) IFF \( F \) is improperly equivalent to itself IFF \( \text{Aut}^-(F) \) is not empty. To understand \( \text{Aut}^-(F) \), we must first understand \( \text{Aut}^+(F) \).

It is easily seen that \( \text{Aut}^+(F) \) is a subgroup of \( \text{SL}_2(\mathbb{Z}) \). The goal of this chapter is to show that if \( F \) is primitive, then \( \text{Aut}^+(F) \) is isomorphic to \( \mathbb{Z}_{\Delta+1} \) (with \( \Delta = \Delta F \)).

In this chapter, we will do slightly more than is strictly necessary.

6.1 Exercise. Let \( F \) and \( G \) be properly equivalent forms. Then \( \text{Aut}^+(F) \) and \( \text{Aut}^+(G) \) are both subgroups of \( \text{SL}_2(\mathbb{Z}) \). Show that they are conjugate to each other.

Notation: In this chapter, \( R \) will be the matrix \( \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \). Also, if \( F = [a, b, c] \), then \( L_F = 2[F]R = \begin{bmatrix} -b & 2a \\ -2c & b \end{bmatrix} \).
6.2 Lemma: \[\begin{bmatrix} ef \\ gh \end{bmatrix} \mathbb{R} = \mathbb{R} \begin{bmatrix} h - g \\ -f \end{bmatrix}\]

Proof: Calculate.

6.3 Lemma: With \(I\) the \(2\times2\) identity matrix, \(L_F^2 = \Delta I\).

Proof: Calculate.

Definition: We define a map \(\Gamma_F : Q[\sqrt{\Delta}] \rightarrow M_2(Q)\) as follows.

For \(\gamma = v + w\sqrt{\Delta}\), let \(\Gamma_F(\gamma) = vI + wL_F = \begin{bmatrix} v - bw & 2aw \\ -2cw & v + bw \end{bmatrix}\).

(Note that \(\Gamma_F(1) = I\) and \(\Gamma_F(\sqrt{\Delta}) = L_F\).)

6.4 Lemma: \(\Gamma_F\) is an injective homomorphism. Also, the determinant of \(\Gamma_F(\gamma)\) equals \(N(\gamma)\).

Proof: The final statement is an easy calculation. That \(\Gamma_F\) preserves addition is trivial. That it preserves multiplication follows easily from Lemma 6.3. Since \(\Delta\) nonsquare implies \(a \neq 0\), showing our map is injective is straightforward.

6.5 Lemma: a) \(\Gamma_F(\mathbb{R}_\Delta) \subseteq M_2(\mathbb{Z})\) (the set of \(2\times2\) matrices with integral entries).

b) Suppose \(F\) is primitive. Then \(\Gamma_F(\mathbb{R}_\Delta) = \Gamma_F(Q[\sqrt{\Delta}]) \cap M_2(\mathbb{Z})\).

Proof: a) We do the case that \(\Delta\) is odd, the other being easier. Let \(\alpha = x + y\delta \in \mathbb{R}_\Delta\) (\(x, y \in \mathbb{Z}\)). Now \(\alpha = x + y(1/2 + \sqrt{\Delta}/2) = v + w\sqrt{\Delta}\) with \(v = x + y/2\) and \(w = y/2\). The entries of \(\Gamma_F(\alpha)\) are \(2aw\), \(-2cw\), and \(v \pm bw\) and we must show these are integers. Clearly \(2aw = ay\) and \(-2cw = -cy\) are integers. Now \(v \pm bw = (x + y/2) \pm by/2\). If \(y\) is even, both are integers.
Suppose $y$ is odd. Since $\Delta$ is odd, we know $b$ is also odd, and again both those entries are integers.

b) Again we do the case that $\Delta$ is odd. One containment follows from part (a). For the other, suppose $\Gamma_F(v + w\sqrt{\Delta}) \in M_2(\mathbb{Z})$. We must show $v + w\sqrt{\Delta} \in R_{\Delta}$. As $\delta = 1/2 + \sqrt{\Delta}/2$, $v + w\sqrt{\Delta} = (v - w) + 2w\delta$. We need $v - w$ and $2w$ to be integers. We know the entries of $\Gamma_F(v + w\sqrt{\Delta})$ (i.e., $2aw$, $-2cw$, $v \pm bw$) are all integers. Since $v \pm bw$ are both integers, $2bw \in \mathbb{Z}$, as are $2aw$ and $2cw$. As $F$ is primitive, $\gcd(a, b, c) = 1$, from which we see $2w \in \mathbb{Z}$ (as desired). Now $v \pm bw$ integers also gives $2v \in \mathbb{Z}$. Write $v = n/2$ and $w = m/2$ ($n, m \in \mathbb{Z}$). Now $v - bw = (n - mb)/2$ is an integer, so $n$ and $mb$ have the same parity. But $b$, like $\Delta$, is odd. Thus $n$ and $m$ have the same parity, so $v - w = (n - m)/2$ is an integer. (When $\Delta$ is even, use that $bw \in \mathbb{Z}$.)

6.6 Lemma: Let $F$ and $G$ be forms of discriminant $\Delta$. Let $S$ be a proper substitution. The following are equivalent.

(i) $SF = G$.

(ii) $[S]L_F[S]^{-1} = L_G$.

(iii) For all $\gamma \in \mathbb{Q}[\sqrt{\Delta}]$, $[S]\Gamma_F(\gamma)[S]^{-1} = \Gamma_G(\gamma)$. (In other words, the composition of $\Gamma_F$ and conjugation by $[S]$ equals $\Gamma_G$.)

Proof: ii) $\iff$ iii): This follows easily from the facts that $\Gamma_F$ and $\Gamma_G$ are determined by $\Gamma_F(\sqrt{\Delta}) = L_F$ and $\Gamma_G(\sqrt{\Delta}) = L_G$, and that conjugation by $[S]$ is an automorphism of $M_2(\mathbb{Q})$.

If (i) holds, we have $[S][F][S]^T = [G]$. Now $L_G = 2[G]R = 2[S][F][S]^T R$. Let $[S] = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$. By Lemma 6.2, $[S]^T R = \begin{bmatrix} r^t & s \\ t^u & u \end{bmatrix} = R \begin{bmatrix} u & -s \\ -t & r \end{bmatrix}$. Since $\det [S] = 1$, $\begin{bmatrix} u & -s \\ -t & r \end{bmatrix} = [S]^{-1}$, and so $L_G = 2[S][F]R[S]^{-1} = [S]L_F[S]^{-1}$, giving (ii). The reverse argument (and cancellation of $2R$) shows (ii) implies (i).
6.7 Corollary: If $\alpha \in \mathbb{U}_{\Delta,+1}$, then $\Gamma_F(\alpha) \in \text{Aut}^+(F)$.

Proof: By Lemmas 6.4 and 6.5, $\Gamma_F(\alpha)$ is an integral matrix with determinant 1, and so is the matrix form of a proper substitution $S$. Thus $\Gamma_F(\alpha) = [S]$. As $\Gamma_F$ is a ring homomorphism which sends 1 to 1, $\Gamma_F(\alpha^{-1}) = [S]^{-1}$. Now $\Gamma_F(\sqrt{\Delta}) = L_F$, and so $[S]L_F[S]^{-1} = \Gamma_F(\alpha)\Gamma_F(\sqrt{\Delta})\Gamma_F(\alpha^{-1}) = \Gamma_F(\alpha\sqrt{\Delta}\alpha^{-1}) = \Gamma_F(\sqrt{\Delta}) = L_F$. Lemma 6.6 shows SF must be F, so that $\Gamma_F(\alpha) = [S] \in \text{Aut}^+(F)$.

6.8 Exercise: a) Suppose $S$ is an improper substitution. Show $[S]L_F[S]^{-1} = -L_{SF}$. (Use Lemma 6.2 and modify the argument in Lemma 6.6.)

b) Suppose $\alpha \in \mathbb{U}_{\Delta}$, and $N(\alpha) = -1$. Show $\Gamma_F(\alpha) = [S]$ for an improper substitution $S$, and $SF = -F$. (Use that $\Gamma_F$ is a homomorphism to show $L_F = -L_{SF}$.) (Note that contrary to what one might guess, $\Gamma_F(\alpha) \notin \text{Aut}^+(F)$.)

6.9 Lemma: Let $r$, $s$, $t$, and $u$ be rational numbers. The following are equivalent.

i) $\begin{bmatrix} rs \\ tu \end{bmatrix}$ is in the image of $\mathbb{Q}[\sqrt{\Delta}]$ under $\Gamma_F$.

ii) $ra + bs = ua$ and $at = -cs$.

iii) $\begin{bmatrix} rs \\ tu \end{bmatrix}[F] = [F]\begin{bmatrix} u - t \\ -s & r \end{bmatrix}$.

iv) $\begin{bmatrix} rs \\ tu \end{bmatrix}$ commutes with $L_F$.
Proof: i) \implies iv): Suppose (i) holds. Since \( L_F = \Gamma_F(\sqrt{\Delta}) \) and since \( \Gamma_F \) is a homomorphism, (iv) follows from the commutivity of \( Q[\sqrt{\Delta}] \).

iv) \implies iii): Suppose (iv) holds. Let \( N = \begin{bmatrix} rs \\ tu \end{bmatrix} \) and \( M = \begin{bmatrix} u - t \\ -s \end{bmatrix} \). We have \( NL_F = L_FN \). Thus \( N(2[F]R) = (2[F]R)N \). By Lemma 6.2 we see that \( MR = RN \), and so \( N(2[F]R) = 2[F]MR \). The 2 and R can be canceled.

iii) \implies ii): Using that \( [F] = \begin{bmatrix} a \\ b/2 \\ c \end{bmatrix} \), calculate the two products in (iii). Comparing the top rows of the two products, one sees that \( ra + bs/2 = ua - bs/2 \) and \( cs = -at \). (ii) follows.

ii) \implies i): (ii) implies \( ra + bs/2 = ua - bs/2 \) and \( cs = -at \). Recalling that \( \Delta \) nonsquare implies \( ac \) are nonzero, we divide the first equation by \( a \) to get \( r + bs/2a = u - bs/2a \). Call that number \( v \). From the second equality, we see \( s/2a = t/2c \). Call that number \( w \). It is now easily seen that \( \Gamma_F(v + w\sqrt{\Delta}) = vI + wL_F = \begin{bmatrix} v - bw & 2aw \\ -2cw & v + bw \end{bmatrix} = \begin{bmatrix} rs \\ tu \end{bmatrix} \).

6.10 Proposition: Let \( F \) be primitive. Then \( \text{Aut}^+(F) \) is isomorphic (as a multiplicative group) to \( \mathbb{I}_{\Delta,+1} \), (via \( \Gamma_F \)).

Proof: By Corollary 6.7, we know \( \Gamma_F \) carries \( \mathbb{I}_{\Delta,+1} \) into \( \text{Aut}^+(F) \). Lemma 6.4 tells us \( \Gamma_F \) is injective, and preserves multiplication.

It only remains to show that if \( [S] = \begin{bmatrix} rs \\ tu \end{bmatrix} \in \text{Aut}^+(F) \), then \( [S] = \Gamma_F(\alpha) \) for some \( \alpha \in \mathbb{I}_{\Delta,+1} \). (Here, \( r, s, t, \) and \( u \) are integers.)

Now \( [S] \in \text{Aut}^+(F) \) is equivalent to \( [S][F][S]^T = [F] \), and hence to \( [S][F] = [F][S]^T \). As \( \text{Det} [S] = 1 \), that equation is \( [rs] [F] = [F] [u - t] \). By Lemmas 6.9 and 6.5(b), \( [S] \in \Gamma_F(Q[\sqrt{\Delta}]) \cap M_2(\mathbb{Z}) = \Gamma_F(R_{\Delta}) \). Thus for some
\( \alpha \in \mathbb{R}_\Delta, \Gamma_F(\alpha) = [S] \). By Lemma 6.4, \( N(\alpha) = \det [S] = 1 \), and so 
\( \alpha \in \mathfrak{f}_\Delta + 1 \). as desired.

6.11 Exercise: Suppose \( F \) is primitive. Show \( \Gamma_F(\mathbb{Q}[\sqrt{\Delta}]) \cap \text{GL}_2(\mathbb{Z}) = \{[S] \mid \text{either } S \text{ is a proper substitution and } SF = F, \text{ or } S \text{ is an improper substitution and } SF = -F \} \). (See Exercise 6.8(b).) Note that \( \text{Aut}^-(F) \) is disjoint from \( \Gamma_F(\mathbb{Q}[\sqrt{\Delta}]) \).

6.12 Corollary: Let \( F \) be a Gaussian form of non-square discriminate \( \Delta \).

i) If \( \Delta > 0 \), then \( \text{Aut}^+(F) \) is isomorphic to \( \mathbb{Z}_2 \oplus \mathbb{Z} \).

ii) If \( \Delta = -3 \), then \( \text{Aut}^+(F) \) is isomorphic to \( \mathbb{Z}_6 \).

iii) If \( \Delta = -4 \), then \( \text{Aut}^+(F) \) is isomorphic to \( \mathbb{Z}_4 \).

iv) If \( \Delta < -4 \), then \( \text{Aut}^+(F) \) is isomorphic to \( \mathbb{Z}_2 \).

Proof: Combine Proposition 6.10 with Corollary 5.7(b) (for \( \Delta > 0 \)) and Exercise 5.4 (for \( \Delta < 0 \)).

6.13 Remark: Having determined \( \text{Aut}^+(F) \), we now consider \( \text{Aut}(F) \) (which we see is a subgroup of \( \text{GL}_2(\mathbb{Z}) \)). It might well happen that \( \text{Aut}(F) = \text{Aut}^+(F) \). This will be the case when there are no improper automorphisms of \( F \), or equivalently, when \( \text{PEC}(F) \) is not in \( \text{AMB}(\Delta) \). One example is \([2, 1, 5]\). In Example 3.9 we saw \([2, 1, 5]\) and \([2, -1, 5]\) are not properly equivalent. As they are improperly equivalent, \([2, 1, 5]\) cannot be improperly equivalent to itself.

Suppose there is an improper automorphism \( T \) of \( F \). Then it is easily seen that the set of all improper automorphisms of \( F \) is exactly \( \{TS \mid S \text{ is a proper automorphism of } F \} \). It follows that in this case, \( \text{Aut}^+(F) \) is a normal subgroup of index 2 in \( \text{Aut}(F) \).
As an example, let $F = [1, 0, -2]$. Now $\Delta = 8$ and $\tau_\Delta = 3 + 2\sqrt{2} = 3 + \sqrt{\Delta}$. Thus $\Gamma_F(\tau_\Delta) = 3I + L_F = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}$ is a proper automorphism of $F$. Now $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ is an improper automorphism of $F$. Those two automorphisms do not commute.

There is one surprise concerning improper automorphisms of $F$, but we leave it for the next section, where we use it.

6.14 Exercise: Let $F = aX^2 + bXY + cY^2$ be a primitive form of discriminant $\Delta$. Use Proposition 6.10 and Exercise 5.13 to show that $\text{Aut}^+(F)$ equals the set of all matrices of the form

$$
\begin{bmatrix}
\frac{u-bv}{2} & av \\
-cv & \frac{u+bv}{2}
\end{bmatrix},
$$

where $(u, v)$ ranges over all solutions of $X^2 - \Delta Y^2 = 4$. 