MATH 371
HOMEWORK SET 3
DUE 28.11.2012, WEDNESDAY

Remember: x, y, z, etc. a, b, etc., A, B, etc. stand for integers! p stand ALWAYS for a prime number; $\mathbf{Z}$ denotes the set of integers.

(1) Let f be a binary quadratic form. Show that the set of automorphisms of f, $\mathrm{Aut}(f)$, is in fact a group.

Solution 1. The automorphisms is as we have defined, a subset of $\mathrm{PGL}_2(\mathbf{Z})$. For $f = (A, B, C)$, let $M_f = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$. There are three things to check:

a. identity: (this will also show that $\mathrm{Aut}(f) \neq \emptyset$)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \text{ clear.}$$

b. closed under group operation: Say $U, V \in \mathrm{Aut}(f)$. Then

$$\begin{aligned} (UV)\cdot f &= (UV)^t M_f (UV) \\ &= V^t \underbrace{U^t M_f U}\, V \\ &= V^t \quad M_f \quad V \\ &= M_f. \end{aligned}$$

c. inverses: Let $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{Aut}(f)$. For simplicity say $\det(U) = 1$. As U is an automorphism we have

$$U \cdot f = U^t M_f U = M_f.$$

So

$$\left(U^t\right)^{-1} U^t M_f U = \left(U^t\right)^{-1} M_f \Leftrightarrow M_f = \left(U^t\right)^{-1} M_f U^{-1}. \tag{1}$$

It is now enough to note that $\left(U^t\right)^{-1} = \left(U^{-1}\right)^t$.

(2) Show that $U = \begin{pmatrix} 391 & 1155 \\ 630 & 1861 \end{pmatrix}$ is an automorphism of the form $f = (5, 14, -11)$.

Solution 2. This is simple computation.

(3) Let $f = (A, B, C)$ be an arbitrary binary quadratic form and $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{Aut}(f)$. Show that $A|r$.

Solution 3. As we did in class, we use the equality $M_f U = \left(U^t\right)^{-1} M_f$, as in Equation 1:

$$\begin{aligned} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} &= \begin{pmatrix} s & -r \\ -q & p \end{pmatrix}\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \\ \begin{pmatrix} Ap + Br/2 & Aq + Bs/2 \\ Bp/2 + Cr & Bq/2 + Cs \end{pmatrix} &= \begin{pmatrix} As - Br/2 & Bs/2 - Cr \\ -Aq + Bp/2 & -Bq/2 + Cp \end{pmatrix}. \end{aligned}$$

Now, we have:

$$Ap + Br/2 = As - Br/2 \tag{2}$$
$$Aq + Bs/2 = Bs/2 - Cr \tag{3}$$
$$Bp/2 + Cr = -Aq + Bp/2 \tag{4}$$
$$Bq/2 + Cs = -Bq/2 + Cp. \tag{5}$$

Both Equation 3 and Equation 4 gives us $Aq = -Cr$ and Equation 2 gives $A(s - p) = Br$. Assume now that $(A, C) = d$ and write $A = da$. Since we know that f is primitive, d cannot divide B. In this case, $d|r$ by Equation 2. a does not divide C, so by Equation 3 $a|r$, hence $da|r$, i.e. $A|r$.

(4) Show that $\begin{pmatrix} 13 & 24 \\ 72 & 133 \end{pmatrix} \in \mathrm{Aut}(f)$; where $f = (3, 5, -1)$. Can you find any other matrix in $\mathrm{Aut}(f)$?

Solution 4. The first part is also a simple computation. As for finding another matrix in the automorphism group, let $U = \begin{pmatrix} 13 & 24 \\ 72 & 133 \end{pmatrix}$. In Question 1, you have proven that $\mathrm{Aut}(f)$ is a group. Hence any power of U should be an element of $\mathrm{Aut}(f)$. Thus any matrix U^n for $n \in \mathbf{Z}$ is an automorphism of the binary quadratic form. In fact, $\mathrm{Aut}(f) \cong \mathbf{Z} \leq \mathrm{PSL}_2(\mathbf{Z})$.

(5) Let $\mathcal{T} := \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \leq \mathrm{PGL}_2(\mathbf{Z})$.

i. Show that $\mathcal{T} = \left\{ \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \mid s \in \mathbf{Z} \right\}$.

ii. For any $t = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in \mathcal{T}$ and and binary quadratic form $f = (A.B, C)$ compute $t \cdot f$.

iii. Show that $f = (A, B, C)$ and $f' = (A', B', C')$ are in the same $\mathcal{T}$-orbit (i.e. the *sets* $\mathcal{T} \cdot f$ and $\mathcal{T} \cdot f'$ are equal) if

a. $\Delta(f) = \Delta(f')$

b. $A = A'$

c. $B' = B + 2As$ for some $s \in \mathbf{Z}$

Hint: It is enough to compare the last components! In fact, converse to the above statement is also true. Can you prove?

iv. Write two binary quadratic forms $f = (A, B, C)$ and $f' = (A', B', C')$ with $\Delta(f) = \Delta(f')$ and $A = A'$ but f and f' are not in the same $\mathcal{T}$ orbit.

Solution 5. Throughout let t_s stand for the matrix $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$.

i. This can be proven using two inductions(one for $s \in \mathbf{Z}_{>0}$, one for $s \in \mathbf{Z}_{<0}$).

ii. $t_s \cdot f = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} A & As + B/2 \\ B/2 & Bs/2 + C \end{pmatrix} = \begin{pmatrix} A & As + B/2 \\ As + B/2 & As^2 + Bs + C \end{pmatrix}$

iii. Assume the conditions a., b., and c. holds. It is enough to show that s_o given in condition c. satisfies $t_{s_o} \cdot f = f'$. By part ii. we know that

$$t_{s_o} \cdot f = (A, 2As_o + B, As_o^2 + Bs_o + C).$$

Then by b. and c. it is enough to compute the last coefficients. Equality of the last coefficients follows when one considers the equality of the discriminants(a.). Note: Diğdem has a nice proof of the converse. Contact her.

iv. Let $f = (6, 7, -1)$ and $f' = (6, 5, -2)$. They both have the same discriminant: 73. But they cannot be in the same $\mathcal{T}$ orbit because there is no $k \in \mathbf{Z} \setminus \{0\}$ so that $5 = 7 + 2 \cdot 6k$ or $7 = 5 + 2 \cdot 6k$

(6) For any given integers x_o and y_o which are relatively prime, show that there are integers x'_o and y'_o such that the matrix

$$\begin{pmatrix} x_o & x'_o \\ y_o & y'_o \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{Z}).$$

Show that these integers are *not* unique!

Solution 6. As $(x_o, y_o) = 1$, there are integers x'_o and y'_o such that $x_o x'_o + y_o(-y'_o) = 1$ Hence the matrix $\begin{pmatrix} x_o & x'_o \\ y_o & y'_o \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{Z})$. However, the integers x'_o and y'_o are not unique by the simple observation that for any $k \in \mathbf{Z}$ we have $x_o(x'_o + k \cdot y_o) + y_o(-y'_o - k \cdot x_o) = x_o x'_o + y_o(-y'_o) = 1$.

(7) Let x and y be two non-zero relatively prime integers. Show that for any $U_o = \begin{pmatrix} x & r_o \\ y & s_o \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{Z})$ we have

$$\left\{ \begin{pmatrix} x & r \\ y & s \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{Z}) \mid r, s \in \mathbf{Z} \right\} = \mathcal{T} \cdot U_o.$$

Show also that the same claim holds even if x and y are not relatively prime.

Solution 7. Fix $U_o = \begin{pmatrix} x & r_o \\ y & s_o \end{pmatrix}$ and let $U = \begin{pmatrix} x & r \\ y & s \end{pmatrix}$ be an element of the set $\left\{ \begin{pmatrix} x & r \\ y & s \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{Z}) \mid r, s \in \mathbf{Z} \right\}$. Note that there is a $t \in \mathbf{Z}$ with the property that $s = s_o + ty$. Let us assume for simplicity that $\det(U) = +1$ so that $xs - yr = 1$. Then using the fact that $xs_o - yr_o = 1$ we conclude that $r = xt + r_o$. In other words

$$U = U_o \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

That is $U \in U_o \cdot \mathcal{T}$. Conversely, we have $\begin{pmatrix} x & r_o \\ y & s_o \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & r \\ y & s \end{pmatrix}$. The second part of the question does NOT make sense simply because x and y have to be relatively prime. Otherwise the matrix U_o cannot belong to $\mathrm{PGL}_2(\mathbf{Z})$.