

# ALGEBRAIC NUMBER THEORY

## HOMEWORK 5

- (1) Show that  $\text{Im}(Mz) = \frac{\text{Im}(z)}{|cz+d|^2}$  for  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ .

Note that, for complex numbers  $z$ , we have  $\text{Re } z = \frac{z+\bar{z}}{2}$  and  $\text{Im } z = \frac{z-\bar{z}}{2i}$ . Thus we get

$$\begin{aligned} \text{Im } Mz &= \text{Im} \frac{az+b}{cz+d} = \text{Im} \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} \\ &= \frac{1}{|cz+d|^2} \text{Im} [(ac+bd) + adz + bc\bar{z}] \\ &= \frac{ad-bc}{|cz+d|^2} \text{Im } z = \frac{\text{Im}(z)}{|cz+d|^2} \end{aligned}$$

because  $ad - bc = 1$ .

- (2) Show that  $\text{SL}_2(\mathbb{Z})$  acts on the upper half plane, i.e., that  $(MN)z = M(Nz)$  for  $z \in \mathcal{H}$ . Let  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and  $N = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  be elements in  $\text{SL}_2(\mathbb{Z})$ . Then

$$\begin{aligned} Nz &= \frac{ez+f}{gz+h}, \\ M(Nz) &= \frac{aN(z)+b}{cN(z)+d} = \frac{a(ez+f)+b(gz+h)}{c(ez+f)+d(gz+h)} \\ &= \frac{(ae+bg)z+af+bh}{(ce+dg)z+cf+dh} = (MN)(z). \end{aligned}$$

- (3) Show that  $Q \sim Q|_M$  for  $M \in \text{SL}_2(\mathbb{Z})$  defines an equivalence relation on the set of binary quadratic forms of fixed discriminant  $\Delta$ .

- (a)  $Q \sim Q$  is trivial: put  $M = I$ .
- (b)  $Q \sim Q'$  implies  $Q' \sim Q$ : in fact, if  $Q' = Q|_M$ , then  $Q = Q'|_N$  for  $N = M^{-1} \in \text{SL}_2(\mathbb{Z})$ .
- (c)  $Q \sim Q'$  and  $Q' \sim Q''$  implies  $Q \sim Q''$ . In fact, if  $Q' = Q|_M$  and  $Q'' = Q'|_N$ , then  $Q'' = Q|_{MN}$ . This last equation can be checked directly; it also follows from the next problem: If  $Q$  corresponds to  $z$ , then  $Q'$  corresponds to  $M^{-1}z$  and  $Q''$  to  $N^{-1}M^{-1}z = (MN)^{-1}z$ , hence we must have  $Q'' = Q|_{MN}$ .

- (4) Show that if a positive definite binary quadratic form  $Q$  corresponds to  $z \in \mathcal{H}$ , then for  $M \in \text{SL}_2(\mathbb{Z})$ , the form  $Q|_M$  corresponds to  $M^{-1}z$ .

Write  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ; then  $M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ . For  $Q = (A, B, C)$  we have  $z = \frac{-B+\sqrt{\Delta}}{2A}$ . Now  $Q|_M = (A', B', C')$  with  $A' = Ar^2 + Brt + Ct^2$ ,  $B' =$

$2(Ars + Ctu) + B(ru + st)$ , and  $C' = As^2 + Bsu + Cu^2$ . Write  $z = \frac{-B + \sqrt{\Delta}}{2A}$ ; then  $z + \bar{z} = -\frac{B}{A}$ ,  $z - \bar{z} = \frac{\sqrt{\Delta}}{A}$ , and  $z\bar{z} = \frac{C}{A}$ .

Now  $Q|_M$  corresponds to  $\frac{-B' + \sqrt{\Delta}}{2A'}$ ; on the other hand,

$$\begin{aligned} M^{-1}z &= \frac{uz - s}{-tz + r} = \frac{(uz - s)(-t\bar{z} + r)}{(-tz + r)(-t\bar{z} + r)} \\ &= -\frac{rs + tuz\bar{z} - ruz - st\bar{z}}{(-tz + r)(-t\bar{z} + r)}. \end{aligned}$$

Now

$$\begin{aligned} ruz + st\bar{z} &= \frac{1}{2}(ru + st)(z + \bar{z}) + \frac{1}{2}(ru - st)(z - \bar{z}) \\ &= (ru + st)\frac{B}{2A} + \frac{\sqrt{\Delta}}{2}, \end{aligned}$$

hence

$$\begin{aligned} M^{-1}z &= -\frac{rs + tu\frac{C}{A} + (ru + st)\frac{B}{2A} - \frac{1}{2}\sqrt{\Delta}}{r^2 + rt\frac{B}{A} + t^2\frac{C}{A}} \\ &= -\frac{2Ars + 2Ctu + B(ru + st) - \sqrt{\Delta}}{2(Ar^2 + Brt + Ct^2)} = \frac{-B' + \sqrt{\Delta}}{A'} \end{aligned}$$

- (5) Show that the two binary quadratic forms  $(1, 0, 3)$  and  $(1, 1, 1)$  represent the same integers, but that they are not equivalent.

Let  $Q(x, y) = x^2 + 3y^2$  and  $R(x, y) = x^2 + xy + y^2$ . These are not equivalent since their discriminants are  $-12$  and  $-3$ , respectively. On the other hand, assume that  $n = x^2 + 3y^2$ . Then  $n = x^2 - 3y^2 = (y - x)^2 + (y - x)(y + x) + (y + x)^2 = X^2 + XY + Y^2$  for  $X = y - x$  and  $Y = y + x$ . Thus every integer represented by  $Q$  is also represented by  $R$ .

Conversely, assume that  $n = x^2 + xy + y^2$ . If  $x$  and  $y$  have the same parity, substitute  $x = Y - X$  and  $y = Y + X$  (in other words: put  $X = \frac{y-x}{2}$  and  $Y = \frac{y+x}{2}$ .) Then  $n = X^2 + 3Y^2$ . If, on the other hand,  $x$  and  $y$  have different parity (as e.g. in  $1 = R(1, 0)$ ), then we may assume that  $x$  is even (otherwise we switch  $x$  and  $y$ ) and observe that  $R(x, y) = R(-x, x + y)$ ; to the last representation we can apply the argument above.

- (6) Compute all reduced forms of discriminant  $\Delta = -31$ .

There are three reduced forms, the principal form  $(1, 1, 8)$  corresponding to the unit ideal, and the two forms  $(2, \pm 1, 4)$  corresponding to the two prime ideals of norm 2 in  $\mathbb{Q}(\sqrt{-31})$ .