The Class Number Problem

2. An Introduction to Algebraic Number Theory

Rajat Tandon

The second part gives an introduction to ‘algebraic number theory’, defines class numbers for finite extensions of the field of rational numbers and proves that in the context of quadratic fields, this definition coincides with the definition of class numbers via binary quadratic forms given in the first part.

We have seen in the first part of this article in the previous issue that some seemingly innocuous questions starting with the formula \( \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \) lead to fairly deep mathematics. This is typical of the subject. It is so important to ask the right question – “ask an impertinent question and you get a pertinent answer”.

The roots of \( aX^2 + bX + c = 0 \) are given by \( \frac{-b \pm \sqrt{\Delta}}{2a} \) where \( \Delta = b^2 - 4ac \) i.e., they are of the form \( x + y\sqrt{\Delta} \) with \( x \) and \( y \) rational. The set \( \mathbb{Q}(\sqrt{\Delta}) \) of elements of the form \( x + y\sqrt{\Delta} \) with \( x \) and \( y \) rational forms a subfield of the field of complex numbers, \( \mathbb{C} \). \( \mathbb{Q}(\sqrt{\Delta}) \) is also a vector space over the rationals if we define scalar multiplication by \( \lambda(x + y\sqrt{\Delta}) = \lambda x + \lambda y\sqrt{\Delta} \). \( \{1, \sqrt{\Delta}\} \) is a basis of \( \mathbb{Q}(\sqrt{\Delta}) \) over \( \mathbb{Q} \), and \( \mathbb{Q} \) is a subfield of \( \mathbb{Q}(\sqrt{\Delta}) \). This process can easily be generalised. For instance, let \( p \) be a prime and \( \zeta = e^{2\pi i / p} \). Let \( \mathbb{Q}(\zeta) \) be the set of complex numbers of the form \( x_0 + x_1\zeta + x_2\zeta^2 + \cdots + x_{p-2}\zeta^{p-2} \) with \( x_i \) rational. Note that \( 1 + \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{p-1} = 0 \) so \( \zeta^{p-1} \) can be written in terms of \( 1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{p-2} \). Check that \( \mathbb{Q}(\zeta) \) is a subfield of \( \mathbb{C} \) containing \( \mathbb{Q} \) and that \( 1, \zeta, \zeta^2, \ldots, \zeta^{p-2} \) is a basis of \( \mathbb{Q}(\zeta) \) over \( \mathbb{Q} \) with scalar multiplication being defined in the obvious way. These are examples of fields containing \( \mathbb{Q} \) which are finite dimensional as vector spaces over \( \mathbb{Q} \). Such fields are known as algebraic number fields and were the object of detailed study by Dedekind, Kronecker and Kummer in the 19th century. Amongst the

---

several motivations for studying such fields were three problems suggested by Greek geometers:
(i) To trisect any given angle
(ii) To construct a cube whose volume is twice that of a given cube.
(iii) To construct a square equal in area to a given circle.

These constructions were to be done by ‘ruler and compass only’ in the manner that we are taught at school. The second problem boils down to being able to construct by ruler and compass the real root of $X^3 - 2$. Galois and Abel looked at such problems and their work gave a huge impetus to the systematisation of algebra and algebraic number theory.

The examples given above, $\mathbb{Q}(\sqrt{\Delta})$ and $\mathbb{Q}(\zeta)$, have been generated by single elements ($\sqrt{\Delta}$ and $\zeta$) which satisfy some polynomial with rational (in fact, integral) coefficients ($X^2 - \Delta, X^p - 1$ respectively). Indeed, it can be shown that any subfield of $\mathbb{C}$ containing $\mathbb{Q}$ which is $n$-dimensional as a vector space over $\mathbb{Q}$ consists of elements of the form $x_0 + x_1 \alpha + x_2 \alpha^2 + \cdots + x_{n-1} \alpha^{n-1}$ where the $x_i$ are rationals and $\alpha$ is a complex number which satisfies a polynomial equation of degree $n$ with rational coefficients.

The first thing we would want to know about such fields is whether they have a subring in them in much the same way that $\mathbb{Q}$ contains $\mathbb{Z}$ and every element of $\mathbb{Q}$ is a ratio of two (one non-zero) elements of $\mathbb{Z}$. One ‘natural’ possibility in $\mathbb{Q}(\sqrt{\Delta})$ could be $\mathbb{Z} + \mathbb{Z}\sqrt{\Delta}$, i.e., elements of the form $a + b\sqrt{\Delta}$ with $a$ and $b$ integers or in other words $\mathbb{Z}$-linear combinations of the basis $1, \sqrt{\Delta}$. Similarly one could consider $\mathbb{Z} + \mathbb{Z}\zeta + \mathbb{Z}\zeta^2 + \mathbb{Z}\zeta^3 + \cdots + \mathbb{Z}\zeta^{p-2}$ in $\mathbb{Q}(\zeta)$. But immediately one would recognise a difficulty in basing a definition which depends on the choice of a basis. For instance, $\mathbb{Q}(\sqrt{\Delta}) =$ $\mathbb{Q}(\sqrt{4\Delta})$ but $\mathbb{Z} + \mathbb{Z}\sqrt{\Delta} \neq \mathbb{Z} + \mathbb{Z}\sqrt{4\Delta}$ or observe that if $p = 3$ then $\zeta = e^{2\pi i/3} = -\frac{1 + \sqrt{-3}}{2}$ so $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$ but $\mathbb{Z} + \mathbb{Z}\zeta \neq \mathbb{Z} + \mathbb{Z}\sqrt{-3}$. To get around the problem of square factors of $\Delta$ we will henceforth assume that $\Delta$ is a fundamental discriminant see Part I of this article. Hence the only square factor $\Delta$ can have is $4$. 
We have already seen that the fields above are generated by elements which satisfy a monic (leading coefficient 1) polynomial with rational coefficients. In fact, every element $a + b\sqrt{\Delta}$ in $\mathbb{Q}(\sqrt{\Delta})$ satisfies the polynomial $X^2 - 2aX + (a^2 - b^2\Delta) = 0$. This suggests an alternative. Why not consider those elements of $\mathbb{Q}(\sqrt{\Delta})$ (or $\mathbb{Q}(\zeta)$) which satisfy a monic polynomial with coefficients in $\mathbb{Z}$? Such elements are called **algebraic integers** (in the given field). Do such elements form a subring $I$, i.e., are they closed under addition and multiplication? The answer is ‘yes’. Observe that $a + b\sqrt{\Delta}$ will be an element of the given type provided $2a \in \mathbb{Z}$ and $a^2 - b^2\Delta \in \mathbb{Z}$. Suppose then that $a + b\sqrt{\Delta}$ and $c + d\sqrt{\Delta}$ are such that $2a, 2c \in \mathbb{Z}$ and $a^2 - b^2\Delta, c^2 - d^2\Delta \in \mathbb{Z}$. Observe that $2(a + c) \in \mathbb{Z}$ and $(a + c)^2 - (b + d)^2\Delta = (a^2 - b^2\Delta) + (c^2 - d^2\Delta) + 2ac - 2bd\Delta$. We say that a rational number is a half integer if it is of the form $\frac{l}{2}$ where $l$ is odd. We make the following observations which can easily be proved by the reader: for $a, b \in \mathbb{Q}$, $2a$ and $a^2 - b^2\Delta$ are integers implies

(i) $2b \in \mathbb{Z}$ since $\Delta$ has no square free factor other than possibly 4;

(ii) if $\Delta$ is even then $a$ must be an integer and $b$ either an integer or half integer;

(iii) if $\Delta$ is odd $a$ and $b$ must be either both integers or both half integers.

In all cases it can then be seen that if $2a, 2c \in \mathbb{Z}$ and $a^2 - b^2\Delta, c^2 - d^2\Delta \in \mathbb{Z}$ then $2ac - 2bd\Delta \in \mathbb{Z}$ and therefore that $(a + c)^2 - (b + d)^2\Delta \in \mathbb{Z}$. On the other hand

\[
(a + b\sqrt{\Delta}) (c + d\sqrt{\Delta}) = ac + bd\Delta + (ad + bc)\sqrt{\Delta} \\
(ac + bd\Delta)^2 - (ad + bc)^2\Delta = (a^2 - b^2\Delta) (c^2 - d^2\Delta)
\]

are both in $\mathbb{Z}$. Hence $I$ is indeed closed under addition and multiplication.

**Exercise:** Show that

(i) in $\mathbb{Q}(\sqrt{-1})$ we have $I = \{a + b\sqrt{-1} | a, b \in \mathbb{Z}\}$

(ii) in $\mathbb{Q}(\sqrt{-3})$ $I = \{\frac{a + b\sqrt{-3}}{2} | a, b \in \mathbb{Z} \ \equiv \ b \pmod{2}\} = \mathbb{Z} + \mathbb{Z}\zeta$ where $\zeta = \frac{-1 + \sqrt{-3}}{2}$ is a cube root of unity.

Would every element of $\mathbb{Q}(\sqrt{\Delta})$ be a ratio of two elements of
We note that $Z + Z\sqrt{\Delta} \subseteq I$ and $\frac{a}{b} + \frac{c}{d}\sqrt{\Delta} = \frac{ad + bcv\sqrt{\Delta}}{bd}$ so this is trivially true. What other properties of $Z$ would we like $I$ to have? The best would be unique factorisation. In $Z$ we have the notion of a prime number and we know that every number can be written up to sign uniquely as a product of distinct prime powers viz $n = \pm p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r}$ where the $p_i$ are distinct primes and, moreover, if $n$ is also equal to $\pm q_1^{f_1}q_2^{f_2} \cdots q_s^{f_s}$ then after changing the order of the $q_i$'s, if necessary, we have $r = s, p_i = q_i$ and $e_i = f_i$ for all $i$.

Imagine the usefulness of having such a property in $I$. For instance consider $Q(\zeta)$ as above and the ring of integers $I$ in $Q(\zeta)$, i.e., the set of all elements in $Q(\zeta)$ which satisfy a monic polynomial in $Z[X]$, the ring of polynomials in one variable with integer coefficients. Suppose there exist non-zero integers $x, y, z$ such that $xP + yP = zP$. Then

$$xP = zP - yP = (z - y)(z - \zeta y)(z - \zeta^2 y) \cdots (z - \zeta^{p-1} y). \quad (*)$$

It is easy to see that $x \in I$ and $z - \zeta^i y \in I$. If we have unique factorisation in $I$ there is just a chance that $(*)$ may give us a contradiction to unique factorisation (or allow us to use the method of descent) and we may prove Fermat's last theorem! It is just possible that Fermat had some such proof in mind when he wrote in the margin ... 

We would first need the notion of a prime element in $I$. This is accomplished more or less as in $Z$ — negatives allowed. So we consider $-2, -3, -5, \ldots$ also as primes.

**Definition 1:** An integer $n$ is a prime if whenever $n$ is written as a product $ab$ of two integers then either $a$ or $b$ must be $\pm 1$. Note that $\pm 1$ are the only units in $Z$, i.e. elements in $Z$ with a multiplicative inverse.

There is another way of defining a prime number.

**Definition 1':** An integer $p \neq \pm 1$ is a prime if and only if whenever $p$ divides a product of integers $ab$ then $p$ must divide either $a$ or $b$.

Recall if $n$ is an integer then $nZ$, the set of multiples of $n$, forms an ideal in $Z$ (an ideal $J$ in a commutative ring $R$ is
an additive subgroup of $R$ which has the property: $x \in J$, $r \in R$ implies $rx \in J$). If an ideal $I$ in a ring satisfies the property: $ab \in I$ implies either $a \in I$ or $b \in I$ it is called a prime ideal. So the integer $p$ is a prime number is the same thing as saying that $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. It is easy to see that the two definitions we have given are equivalent in $\mathbb{Z}$.

Based on the above we could define in an arbitrary commutative ring with unity $R$ (all our rings will be so) an element $\pi$ to be prime either by requiring that whenever $\pi = ab$ either $a$ or $b$ must be a unit in $R$ or by requiring that the ideal $\pi R$, consisting of all multiples of $\pi$, is a prime ideal. Unfortunately in an arbitrary ring the two definitions are not equivalent. An element $\pi$ which satisfies the first property is said to be irreducible whereas if $\pi R$ is a prime ideal we call $\pi$ a prime. In integral domains (commutative rings with no zero divisors) all primes are irreducible but not vice versa. (Exercise: Prove this.)

A domain in which every non-zero non-unit can be written as a product of irreducibles in an essentially unique way, that is up to order and multiplication by units ($6 = 2 \cdot 3 = 3 \cdot 2 = (-2)(-3) = (-3)(-2)$) is called a unique factorisation domain (UFD). Clearly, $\mathbb{Z}$ is a UFD and it is easy to check that $J = \mathbb{Z} + \mathbb{Z}i$ is also a UFD.

$\mathbb{Z}$ has another property which is somewhat stronger – every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$ where $n$ is an integer. A domain $D$ which has the property that every ideal in it is of the form $xD$ for some $x$ in $D$ is called a Principal Ideal Domain (PID) and every PID is a UFD. If we could show that the ring of integers $I$ in an algebraic number field is always a PID then we could use the argument given above for FLT. Unfortunately $I$ is not always a PID. For instance, consider $\mathbb{Q}(\sqrt{-20})$; then $I = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ and we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. It is easy to check that $2, 3, 1 \pm \sqrt{-5}$ are all irreducible elements in $I$. We remark that the ring of integers of an algebraic number field is a UFD if and only if it is a PID.
Recall that if \( A \) and \( B \) are two ideals in a ring \( R \) then we define their product \( A \cdot B = \{ \sum_{i=1}^{n} a_i b_i | a_i \in A, b_i \in B, \text{ for some } n \} \). This is also an ideal. Though \( I \) is not always a PID it is true that every ideal in \( I \) can be written uniquely, except for order, as a product of prime ideals. This gives us the first hint that the concept of an ideal may be at least as important as the notion of an element. Note that in a PID the two notions are almost the same as every ideal is generated by a single element which is uniquely determined up to units.

So if \( I \) is not always a PID then how 'bad' is it? The set \( I \) of ideals in \( I \) under the product defined above form a semigroup (\( I \) itself is the identity). We define an equivalence relation on this set \( I \) as follows: \( A \sim B \) if there exist \( \alpha, \beta \in I \) such that \( \alpha I \cdot A = \beta I \cdot B \). It is easy to check that this gives us an equivalence relation on \( I \) and the product on \( I \) induces a product on the set of equivalence classes \( I/\sim: [A] \cdot [B] = [A \cdot B] \). The crucial point here is to check that \( \cdot \) as defined above is well defined, i.e., if \( A \sim A' \) and \( B \sim B' \) then \( A \cdot B \sim A' \cdot B' \). The set of equivalence classes \( I/\sim \) with this product is actually a group. It is one of the fundamental theorems of algebraic number theory that this group is finite – not just for quadratic extensions of \( \mathbb{Q} \) but for any finite extension of \( \mathbb{Q} \). The order of this group is called the class number of the extension. The class number of \( \mathbb{Q}(\sqrt{\Delta}) \) will be denoted by \( h'(\Delta) \). Note that the class number is one if and only if \( I \) is a PID.

Let now \( \Delta \) be a negative fundamental discriminant, i.e., a negative integer \( \Delta \) which is congruent to 0 or 1 modulus 4 and which cannot be written in the form \( \Delta_0 n^2 \) where \( \Delta_0 \) is another discriminant and \( n \) is an integer. Hence 4 is the only possible square factor of \( \Delta \). Recall that we have defined \( h(\Delta) \) to be the number of equivalence classes of primitive binary integral quadratic forms. Remarkably:

**THEOREM:** \( h(\Delta) = h'(\Delta) \).

In order to prove this we first observe that if \( \alpha = a + b\sqrt{\Delta} \) is in the ring of integers \( I \) of \( \mathbb{Q}(\sqrt{\Delta}) \) then so also is \( \overline{\alpha} = \)
\(a - b\sqrt{\Delta}\). Hence so also is \(a\alpha\) which is an integer. Hence if \(A\) is any non-zero ideal of \(I\) then \(A \cap \mathbb{Z} \neq (0)\). Clearly \(A \cap \mathbb{Z}\) is an ideal in \(\mathbb{Z}\) so \(A \cap \mathbb{Z} = a\mathbb{Z}\) for some integer \(a > 0\). Observe also that any non-zero ideal of \(I\) cannot be contained in \(\mathbb{Z}\).

In order to make life a bit easier we will assume in what follows that \(\Delta\) is odd and hence that \(I = \mathbb{Z} + \mathbb{Z} \frac{1 + \sqrt{\Delta}}{2}\) (proof?). Let \(A\) be an ideal in \(I\). Define

\[J = \{r \in \mathbb{Z}| r \cdot \frac{1 + \sqrt{\Delta}}{2} + s \in A\}\]

for some \(s \in \mathbb{Z}\). Then \(J\) is an ideal in \(\mathbb{Z}\) and since \(A \not\subseteq \mathbb{Z}, J\) is non-zero. Let \(J = t\mathbb{Z}, t > 0\). Then there exists an \(s \in \mathbb{Z}\) such that \(t\frac{1 + \sqrt{\Delta}}{2} + s \in A\). We claim that \(A = a\mathbb{Z} + \frac{(t+2s)+t\sqrt{\Delta}}{2}\mathbb{Z}\). Clearly the right hand side is contained in \(A\). Let \(\alpha = u + v\frac{1 + \sqrt{\Delta}}{2} \in A\). Then \(v \in J\) so \(v = tv'\) for some \(v' \in \mathbb{Z}\). Therefore

\[\alpha - v'(t + 2s) + t\sqrt{\Delta} = \frac{u + tv'(1 + \sqrt{\Delta}) - v'(t + 2s) + t\sqrt{\Delta}}{2} = u - sv' \in A \cap \mathbb{Z} = a\mathbb{Z}.
\]

Therefore \(\alpha \in a\mathbb{Z} + \frac{(t+2s)+t\sqrt{\Delta}}{2}\mathbb{Z}\). Hence every ideal \(A\) in \(I\) is of the form \(a\mathbb{Z} + \frac{b+c\sqrt{\Delta}}{2}\mathbb{Z}\) for some \(a > 0, c > 0\). For this to be an ideal it must be closed under multiplication by \(\frac{1 + \sqrt{\Delta}}{2}\). Hence

\[a \cdot \frac{1 + \sqrt{\Delta}}{2} \in a\mathbb{Z} + \frac{b+c\sqrt{\Delta}}{2}\mathbb{Z},\]

i.e., there exist integers \(m, n\) such that \(a \cdot \frac{1 + \sqrt{\Delta}}{2} = ma + n \cdot \frac{b+c\sqrt{\Delta}}{2} \Rightarrow a = nc\) and \(1 = 2m + b\) i.e., \(c\) divides \(a\), \(c\) divides \(b\) and \(\frac{b}{c}\) is odd. Let \(a = tc, b = uc, u\) odd. Then \(a\mathbb{Z} + \frac{b+c\sqrt{\Delta}}{2}\mathbb{Z} = tc\mathbb{Z} + \frac{uc+c\sqrt{\Delta}}{2}\mathbb{Z} = c[t\mathbb{Z} + \frac{u+y\sqrt{\Delta}}{2}\mathbb{Z}].\)

Hence, every ideal \(A\) in \(I\) is of the form \(c[t\mathbb{Z} + \frac{u+y\sqrt{\Delta}}{2}\mathbb{Z}]\), with \(c > 0, t > 0\) and \(u\) odd. Further, again since \(A\) is closed under multiplication by \(\frac{1 + \sqrt{\Delta}}{2}\), \(c \cdot \frac{u+y\sqrt{\Delta}}{2} = c[t\mathbb{Z} + \frac{u+y\sqrt{\Delta}}{2}\mathbb{Z}].\)

Hence there exist integers \(h, k\) such that \(\frac{(u+\Delta)+(1+y)\sqrt{\Delta}}{4} = ht + k\frac{u+y\sqrt{\Delta}}{2}\). Therefore, \(k = \frac{1+u}{2}\) and \(\frac{u+\Delta}{4} = ht + \frac{k}{2} = ht + \frac{u(1+u)}{4}\). Hence \(\Delta = u^2 + 4ht\). We have proved:
Proposition: Every ideal in $I$ is of the form $t(aZ + \frac{b+\sqrt{\Delta}}{2}Z)$ for some integers $a, b, t$ with $t > 0, a > 0$ and such that there exists an integer $c$ with $\Delta = b^2 - 4ac$.

Proof of the THEOREM: We denote by $[aX^2 + bXY + cY^2]$ the equivalence class of the form $aX^2 + bXY + cY^2$ in $S_1(\Delta)$. We denote by $[A]$ the equivalence class of the ideal $A$ in $I$. Define

$$\epsilon : S_1(\Delta)/\sim \longrightarrow I/\sim$$

$$[aX^2 + bXY + cY^2] \longrightarrow [aZ + \frac{b+\sqrt{\Delta}}{2}Z].$$

Then the proposition we have proved above shows that $\epsilon$ is surjective. We need, of course, to show that $\epsilon$ is well defined. For this we must show that if

$$A(aX^2 + bXY + cY^2) = a'X^2 + b'XY + c'Y^2$$

where $A$ is either $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ then $aZ + \frac{b+\sqrt{\Delta}}{2}Z \sim a'Z + \frac{b'+\sqrt{\Delta}}{2}Z$.

If $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ then $a' = a$ and $b' = b + 2a$ which implies that $aZ + \frac{b+\sqrt{\Delta}}{2}Z = a'Z + \frac{b'+\sqrt{\Delta}}{2}Z$.

If $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ then $a' = c$ and $b' = -b$ so

$$a'Z + \frac{b'+\sqrt{\Delta}}{2}Z = cZ + \frac{-b+\sqrt{\Delta}}{2}Z = \frac{b^2 - \Delta}{4a}Z + \frac{-b + \sqrt{\Delta}}{2}Z.$$

Therefore $a(a'Z + \frac{b'+\sqrt{\Delta}}{2}Z) = \frac{(-b + \sqrt{\Delta})}{2}(aZ + \frac{b+\sqrt{\Delta}}{2}Z)$ and we have proved what was required.

In order to prove our theorem we must show that $\epsilon$ is a bijection. Only the injectivity of $\epsilon$ is left. Before proving injectivity we make two remarks:

(a) If $A$ and $B$ are two ideals in $I$ then they are equivalent if there exists $\alpha, \beta \in I$ such that $\alpha.A = \beta.B$. But this is equivalent to $\alpha\bar{\alpha}A = \bar{\alpha}\beta B$ and $\alpha\bar{\alpha}$ is a positive integer.
Hence \( A \sim B \) if and only if there exists an integer \( t > 0 \) and \( \beta \in I \) such that \( t \cdot A = \beta \cdot B \).

(b) If \( \alpha, \beta \in I \) and \( \alpha \mathbb{Z} + \beta \mathbb{Z} = \gamma \mathbb{Z} + \delta \mathbb{Z} \) then there exists an integral \( 2 \times 2 \) matrix \( A \) of determinant \( \pm 1 \) such that
\[
A \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}
\]

Suppose now that
\[
\epsilon([aX^2 + bXY + cY^2]) = \epsilon([a'X^2 + b'XY + c'Y^2])
\]
i.e.,
\[
a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2} \mathbb{Z} \sim a'\mathbb{Z} + \frac{b' + \sqrt{\Delta}}{2} \mathbb{Z}.
\]

Hence there exists an integer \( t' > 0 \) and \( \alpha = \frac{p+q\sqrt{\Delta}}{2} \) in \( I \)
such that \( \alpha \cdot (a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2} \mathbb{Z}) = t' \cdot (a'\mathbb{Z} + \frac{b' + \sqrt{\Delta}}{2} \mathbb{Z}) = A \) (say).

We must show that
\[
a'X^2 + b'XY + c'Y^2 = A \cdot (aX^2 + bXY + cY^2)
\]
for some \( A \) in \( \text{SL}(2, \mathbb{Z}) \).

Case 1: Let \( q = 0 \) and \( t = p/2 \). Then \( at\mathbb{Z} = a't'\mathbb{Z} = A \cap \mathbb{Z} \).

We may without loss of generality assume that \( at = a't' \) and hence \( t > 0 \).

There exist integers \( m, n \) such that \( t = \frac{b + \sqrt{\Delta}}{2} = ma't' + nt' \cdot \frac{b' + \sqrt{\Delta}}{2} \) which implies that \( t = nt' \) and hence \( a' = na \).

There also exist integers \( k, l \) such that \( t'\frac{b' + \sqrt{\Delta}}{2} = kta + lt\frac{b + \sqrt{\Delta}}{2} \).

Hence \( ln = 1 \) or \( n = 1, t = t', a = a' \) and \( b' = b + 2ak \).

It is now easy to see that
\[
a'X^2 + b'XY + c'Y^2 = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot (aX^2 + bXY + cY^2).
\]

Case 2: \( (q \neq 0) \) In view of case 1 we may assume that \( (p, q) = 1 \). By the proposition above and remark (b) there exists an integral matrix \( A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \) of determinant \( \pm 1 \)
such that
\[
A \begin{pmatrix} \frac{p+q\sqrt{\Delta}}{2} \\ \frac{b+\sqrt{\Delta}}{2} \end{pmatrix} \begin{pmatrix} \frac{p+q\sqrt{\Delta}}{2} \\ \frac{b+\sqrt{\Delta}}{2} \end{pmatrix} = \begin{pmatrix} t'a' \\ t'\frac{b' + \sqrt{\Delta}}{2} \end{pmatrix}
\]
or, in fact, by multiplying by the matrix \( \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \), if necessary, we can assume that \( A \) is in \( SL(2,\mathbb{Z}) \) and

\[
A \cdot \left( \frac{a\frac{p+q\sqrt{\Delta}}{2}}{(b+\frac{\sqrt{\Delta}}{2}) \cdot (\frac{p+q\sqrt{\Delta}}{2})} \right) = \left( \frac{\pm t'a'}{t' \cdot \frac{b'+\sqrt{\Delta}}{2}} \right).
\]

Therefore, \( xa^p+q\sqrt{\Delta} + y\left(\frac{bp+q\Delta}{4}\right) + \left(\frac{p+\sqrt{\Delta}}{4}\right) = \pm t'a' \) which implies that \( xa^p + y\left(\frac{bp+q\Delta}{4}\right) = \pm t'a' \) and \( xa^q + y\frac{p+q\Delta}{4} = 0 \). Hence \( 2xaq = -y(p+ bq) \). Let \( e \) be the positive g.c.d. of \( 2a \) and \( p + bq \). Then \( x\frac{2aq}{e} = -y\frac{p+aq}{e} \) so \( 
\frac{2aq}{e} \) divides \( y \) and \( y = \frac{2aq}{e} \cdot r \) for some integer \( r \). Then \( x = -r\frac{p+aq}{e} \). Since \( (x, y) = 1 \) we get \( r = \pm 1 \). A simple calculation now shows that \( xa^2 + y\left(\frac{bp+q\Delta}{4}\right) = \pm t'a' = -\frac{2a}{e} \alpha \bar{\alpha} \). Hence, keeping in view the various signs, we get \( t'a' = \frac{2a}{e} \alpha \bar{\alpha} \). Furthermore, since \( wx - yz = 1 \), substituting the values of \( x \) and \( y \) given above we get \( w(p + bq) + 2aqz = -re \). We further get from \((*) \) that \( 2\frac{a^p+q\sqrt{\Delta}}{2} + w\left(\frac{p+q\Delta}{2}\right) = t' \cdot \frac{b'+\sqrt{\Delta}}{2} \) which implies that \( 2zap + w(bp+q\Delta) = 2t'b' \) and \( 2zaq + w(p+aq) = 2t' \), i.e., \( -re = 2t' \). Hence \( 2zap + w(bp+q\Delta) = -reb' \).

It is now easy to check that \( A^t \cdot (aX^2 + bXY + cY^2) = a'X^2 + b'XY + c'Y^2 \). For instance, the coefficient of \( X^2 \), if we replace \( X \) by \( X^2 + zY \) and \( Y \) by \( yX + wY \) in the expression \( aX^2 + bXY + cY^2 \), is \( ax^2 + bxy + cy^2 \). Substituting \( x = -r\frac{p+aq}{e} \) and \( y = \frac{2aq}{e} \cdot r \) and using the fact that \( t'a' = \frac{2a}{e} \alpha \bar{\alpha} \) and \( 2t' = -re \) we get \( ax^2 + bxy + cy^2 = a' \). Similarly, the coefficient of \( XY \) on the required transformation is \( 2axz + bzx + byz + 2cyw \) which on substitution is just \( b' \). Therefore \( A^t \cdot (aX^2 + bXY + cY^2) = a'X^2 + b'XY + c'Y^2 \) and \( e \) is injective.

This is a beautiful example in mathematics where two apparently unrelated objects turn out to be equal. Maybe the reader can discover some more.

---

Suggested Reading


Address for Correspondence
Rajat Tandon
Department of Mathematics
University of Hyderabad
Central University P.O.
Hyderabad 500 046, India

---

"Bhabha is a great lover of music, a gifted artist, a brilliant engineer and an outstanding scientist... He is the modern equivalent of Leonardo da Vinci."

G V Raman

---

RESONANCE | July 1998