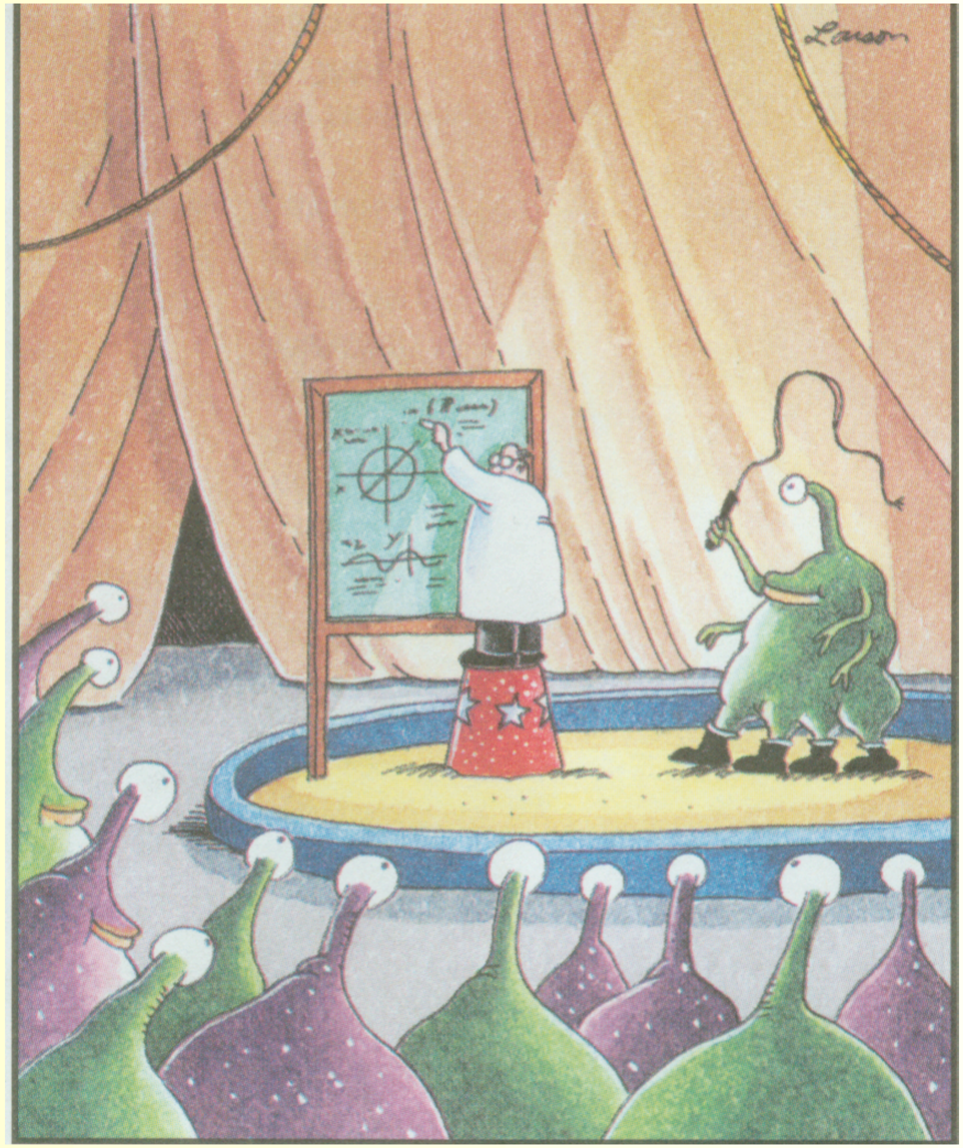
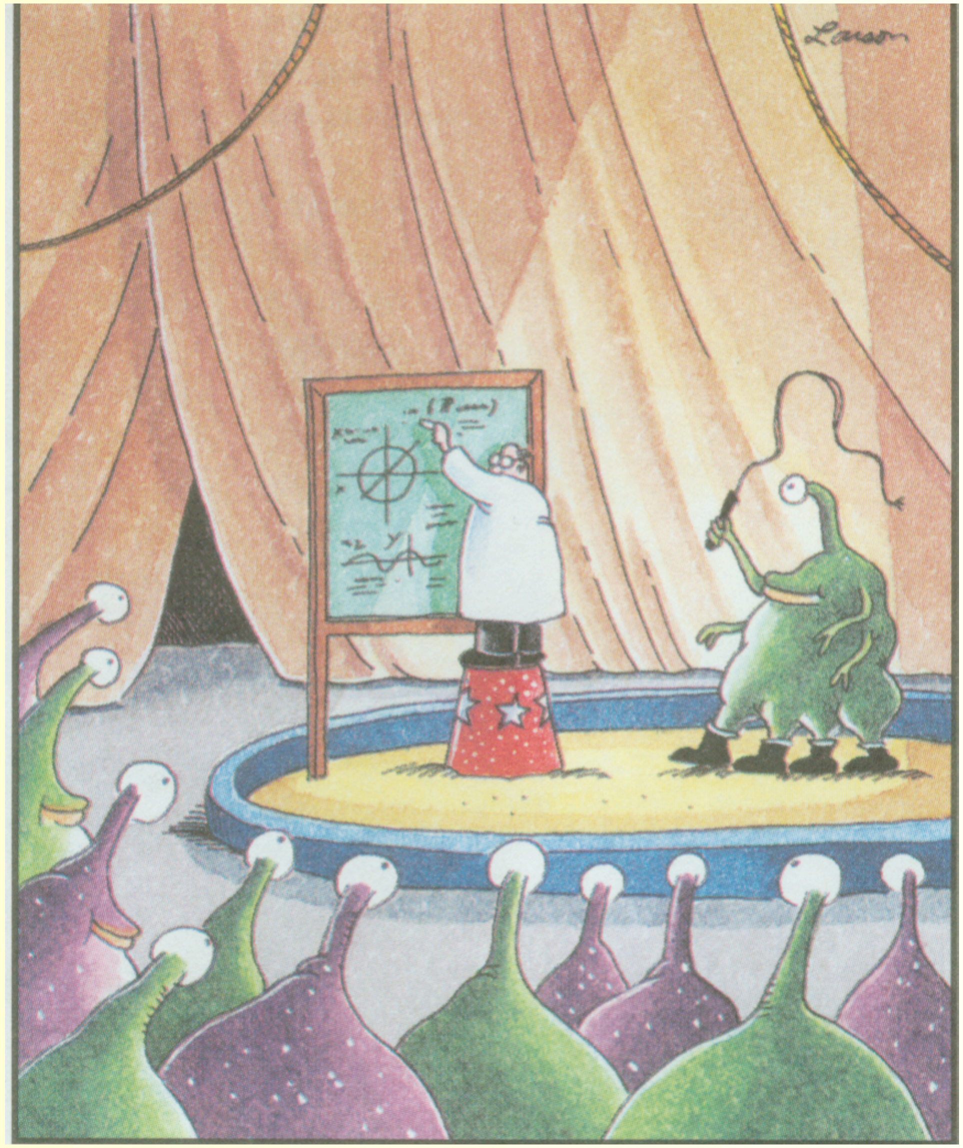
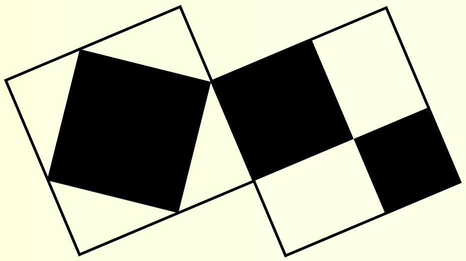

Larson



Abducted by an alien circus company, Professor Doyle is forced to write calculus equations in center ring.

Ideal Multiplication in Fields of Low Degree
A Preliminary Report



Alf van der Poorten

ceNTRe for Number Theory Research, Sydney

To Richard Brent on his 60th birthday

Computing by the Numbers   Berlin, July 21, 2006

Manjul Bhargava's work on higher composition laws amply deals with issues that arise in congenially detailing an algorithm for multiplication of ideals in quadratic fields. I briefly illustrate Bhargava's work by giving my take on its application to the well known quadratic case, hoping thereby to instance and hint at its generalisations to cubic, and quartic fields.

Manjul Bhargava's work on higher composition laws amply deals with issues that arise in congenially detailing an algorithm for multiplication of ideals in quadratic fields. I briefly illustrate Bhargava's work by giving my take on its application to the well known quadratic case, hoping thereby to instance and hint at its generalisations to cubic, and quartic fields.

'My take' is only little more than an explanation of sorts of Dan Shanks's infrastructural composition, see

Daniel Shanks, 'On Gauss and composition', in *Number Theory and Applications*, (NATO – Advanced Study Institute, Banff, 1988) Kluwer Academic Publishers Dordrecht, 1989, 163–204 .

Manjul Bhargava's work on higher composition laws amply deals with issues that arise in congenially detailing an algorithm for multiplication of ideals in quadratic fields. I briefly illustrate Bhargava's work by giving my take on its application to the well known quadratic case, hoping thereby to instance and hint at its generalisations to cubic, and quartic fields.

'My take' is only little more than an explanation of sorts of Dan Shanks's infrastructural composition, see

Daniel Shanks, 'On Gauss and composition', in *Number Theory and Applications*, (NATO – Advanced Study Institute, Banff, 1988) Kluwer Academic Publishers Dordrecht, 1989, 163–204 .

I first looked at a cubic analogue of these notions late in the past milennium. and again in 2001, then jointly with Renate Scheidler.

Manjul Bhargava's work on higher composition laws amply deals with issues that arise in congenially detailing an algorithm for multiplication of ideals in quadratic fields. I briefly illustrate Bhargava's work by giving my take on its application to the well known quadratic case, hoping thereby to instance and hint at its generalisations to cubic, and quartic fields.

'My take' is only little more than an explanation of sorts of Dan Shanks's infrastructural composition, see

Daniel Shanks, 'On Gauss and composition', in *Number Theory and Applications*, (NATO – Advanced Study Institute, Banff, 1988) Kluwer Academic Publishers Dordrecht, 1989, 163–204 .

I first looked at a cubic analogue of these notions late in the past millennium. and again in 2001, then jointly with Renate Scheidler. Inappropriately, we looked at composition of ternary cubic forms.

Composition of Quadratic Forms

Composition of Quadratic Forms

The product of two quadratic forms $\varphi = UX^2 + VXY + WY^2$ and $\varphi' = U'X'^2 + V'X'Y' + W'Y'^2$ is a nasty expression

$$UU'X^2X'^2 + UV'X^2X'Y' + UW'X^2Y'^2 + VU'XX'^2Y + \cdots \qquad \text{etc.}$$

Composition of Quadratic Forms

The product of two quadratic forms $\varphi = UX^2 + VXY + WY^2$ and $\varphi' = U'X'^2 + V'X'Y' + W'Y'^2$ is a nasty expression

$$UU'X^2X'^2 + UV'X^2X'Y' + UW'X^2Y'^2 + VU'XX'^2Y + \cdots \qquad \text{etc.}$$

Suppose, however, that it happens to happen that there is a bilinear substitution

$$x = A_xXX' + B_xXY' + C_xX'Y + D_xYY'$$
$$y = A_yXX' + B_yXY' + C_yX'Y + D_yYY'$$

whereby that product becomes $\Phi = ux^2 + vxy + wy^2$.

Composition of Quadratic Forms

The product of two quadratic forms $\varphi = UX^2 + VXY + WY^2$ and $\varphi' = U'X'^2 + V'X'Y' + W'Y'^2$ is a nasty expression

$$UU'X^2X'^2 + UV'X^2X'Y' + UW'X^2Y'^2 + VU'XX'^2Y + \cdots \qquad \text{etc.}$$

Suppose, however, that it happens to happen that there is a bilinear substitution

$$x = A_xXX' + B_xXY' + C_xX'Y + D_xYY'$$
$$y = A_yXX' + B_yXY' + C_yX'Y + D_yYY'$$

whereby that product becomes $\Phi = ux^2 + vxy + wy^2$.

Then we have a much more palatable "product" and, moreover, we may then report that the form Φ is a compound of the given forms φ and φ'.

All of this should be completely familiar.

All of this should be completely familiar. Everyone knows the evident instance

$(X^2+Y^2)({X'}^2+{Y'}^2)=x^2+y^2$ with $x=XX'-YY'$, $y=XY+X'Y$,

All of this should be completely familiar. Everyone knows the evident instance

$(X^2+Y^2)({X'}^2+{Y'}^2)=x^2+y^2$ with $x=XX'-YY'$, $y=XY+X'Y$,

More impressively, one reads in the literature that Fermat had noticed that the product of two primes represented by $2x^2+2xy+3y^2$ is represented by x^2+5y^2.

All of this should be completely familiar. Everyone knows the evident instance

$(X^2+Y^2)({X'}^2+{Y'}^2)=x^2+y^2$ with $x=XX'-YY'$, $y=XY+X'Y$,

More impressively, one reads in the literature that Fermat had noticed that the product of two primes represented by $2x^2+2xy+3y^2$ is represented by x^2+5y^2. The 'why that is so' follows from the identity

$$\begin{aligned}&(2X^2+2XY+3Y^2)(2{X'}^2+2XY'+3{Y'}^2)\\&\qquad=(2XX'+XY'+X'Y-2YY')^2+5(XY'+XY'+YY')^2\,.\end{aligned}$$

All of this should be completely familiar. Everyone knows the evident instance

$(X^2+Y^2)(X'^2+Y'^2) = x^2+y^2$ with $x = XX'-YY'$, $y = XY+X'Y$,

More impressively, one reads in the literature that Fermat had noticed that the product of two primes represented by $2x^2+2xy+3y^2$ is represented by x^2+5y^2. The 'why that is so' follows from the identity

$$(2X^2+2XY+3Y^2)(2X'^2+2XY'+3Y'^2)$$
$$= (2XX'+XY'+X'Y-2YY')^2+5(XY'+XY'+YY')^2 .$$

In other words, x^2+5y^2 is a compound of $2x^2+2xy+3y^2$ with itself.

If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, I write $\Phi_M(x, y) = \Phi(ax + by, cx + dy)$, and recall that the discriminant of Φ_M is $(\det M)^2$ times that of Φ.

If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, I write $\Phi_M(x, y) = \Phi(ax + by, cx + dy)$, and recall that the discriminant of Φ_M is $(\det M)^2$ times that of Φ.

Now notice that

$$x = (A_xX'+B_xY')X+(C_xX'+D_xY')Y = (A_xX+C_xY)X'+(B_xX+D_xY)Y'$$

$$y = (A_yX'+B_yY')X+(C_yX'+D_yY')y = (A_yX+C_yY)X'+(B_yX+D_yY)Y' .$$

If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, I write $\Phi_M(x,y) = \Phi(ax+by, cx+dy)$, and recall that the discriminant of Φ_M is $(\det M)^2$ times that of Φ.

Now notice that

$$x = (A_xX'+B_xY')X+(C_xX'+D_xY')Y = (A_xX+C_xY)X'+(B_xX+D_xY)Y'$$

$$y = (A_yX'+B_yY')X+(C_yX'+D_yY')y = (A_yX+C_yY)X'+(B_yX+D_yY)Y'.$$

Hence we have the identities

$$\varphi(X,Y)\varphi'(X',Y') = \Phi(x,y) = \Phi_{\left(\begin{smallmatrix} A_xX'+B_xY' & C_xX'+D_xY' \\ Ax'+By' & Cx'+Dy' \end{smallmatrix}\right)}(X,Y)$$

and

$$\varphi(X,Y)\varphi'(X',Y') = \Phi(x,y) = \Phi_{\left(\begin{smallmatrix} A_xX+C_xY & B_xX+D_xY \\ A_yX+C_yY & B_yX+D_yY \end{smallmatrix}\right)}(X',Y'),$$

illustrating first that φ and φ' each have discriminant a square of a rational times that of Φ.

It follows that there is no effective loss of generality in our supposing henceforth that all three forms φ, φ', and Φ have the same discriminant.

It follows that there is no effective loss of generality in our supposing henceforth that all three forms φ, φ', and Φ have the same discriminant. Second, we see that

$$\varphi'(x',y')^2 = \begin{vmatrix} A_xX'+B_xY' & C_xX'+D_xY' \\ A_yX'+B_yY' & C_yX'+D_yY' \end{vmatrix}^2$$

and

$$\varphi(x,y)^2 = \begin{vmatrix} A_xX+C_xY & B_xX+D_xY \\ A_yX+C_yY & B_yX+D_yY \end{vmatrix}^2 .$$

It follows that there is no effective loss of generality in our supposing henceforth that all three forms φ, φ', and Φ have the same discriminant. Second, we see that

$$\varphi'(x', y')^2 = \begin{vmatrix} A_x X' + B_x Y' & C_x X' + D_x Y' \\ A_y X' + B_y Y' & C_y X' + D_y Y' \end{vmatrix}^2$$

and

$$\varphi(x, y)^2 = \begin{vmatrix} A_x X + C_x Y & B_x X + D_x Y \\ A_y X + C_y Y & B_y X + D_y Y \end{vmatrix}^2 .$$

Thus, up to choices of sign tantamount to our defining direct rather than indirect composition, necessarily

It follows that there is no effective loss of generality in our supposing henceforth that all three forms φ, φ', and Φ have the same discriminant. Second, we see that

$$\varphi'(x',y')^2 = \begin{vmatrix} A_xX' + B_xY' & C_xX' + D_xY' \\ A_yX' + B_yY' & C_yX' + D_yY' \end{vmatrix}^2$$

and

$$\varphi(x,y)^2 = \begin{vmatrix} A_xX + C_xY & B_xX + D_xY \\ A_yX + C_yY & B_yX + D_yY \end{vmatrix}^2 .$$

Thus, up to choices of sign tantamount to our defining direct rather than indirect composition, necessarily

$$\varphi(x,y) = \begin{vmatrix} A_x & B_x \\ A_y & B_y \end{vmatrix} x^2 + \left(\begin{vmatrix} A_x & D_x \\ A_y & D_y \end{vmatrix} - \begin{vmatrix} B_x & C_x \\ B_y & C_y \end{vmatrix}\right) xy + \begin{vmatrix} C_x & D_x \\ C_y & D_y \end{vmatrix} y^2$$

It follows that there is no effective loss of generality in our supposing henceforth that all three forms φ, φ', and Φ have the same discriminant. Second, we see that

$$\varphi'(x',y')^2 = \begin{vmatrix} A_xX'+B_xY' & C_xX'+D_xY' \\ A_yX'+B_yY' & C_yX'+D_yY' \end{vmatrix}^2$$

and

$$\varphi(x,y)^2 = \begin{vmatrix} A_xX+C_xY & B_xX+D_xY \\ A_yX+C_yY & B_yX+D_yY \end{vmatrix}^2 .$$

Thus, up to choices of sign tantamount to our defining direct rather than indirect composition, necessarily

$$\varphi(x,y) = \begin{vmatrix} A_x & B_x \\ A_y & B_y \end{vmatrix} x^2 + \left(\begin{vmatrix} A_x & D_x \\ A_y & D_y \end{vmatrix} - \begin{vmatrix} B_x & C_x \\ B_y & C_y \end{vmatrix}\right)xy + \begin{vmatrix} C_x & D_x \\ C_y & D_y \end{vmatrix} y^2$$

and

$$\varphi'(x,y) = \begin{vmatrix} A_x & C_x \\ A_y & C_y \end{vmatrix} x^2 + \left(\begin{vmatrix} A_x & D_x \\ A_y & D_y \end{vmatrix} + \begin{vmatrix} B_x & C_x \\ B_y & C_y \end{vmatrix}\right)xy + \begin{vmatrix} B_x & D_x \\ B_y & D_y \end{vmatrix} y^2 ,$$

It follows that there is no effective loss of generality in our supposing henceforth that all three forms φ, φ', and Φ have the same discriminant. Second, we see that

$$\varphi'(x',y')^2 = \begin{vmatrix} A_xX' + B_xY' & C_xX' + D_xY' \\ A_yX' + B_yY' & C_yX' + D_yY' \end{vmatrix}^2$$

and

$$\varphi(x,y)^2 = \begin{vmatrix} A_xX + C_xY & B_xX + D_xY \\ A_yX + C_yY & B_yX + D_yY \end{vmatrix}^2 .$$

Thus, up to choices of sign tantamount to our defining direct rather than indirect composition, necessarily

$$\varphi(x,y) = \begin{vmatrix} A_x & B_x \\ A_y & B_y \end{vmatrix} x^2 + \left(\begin{vmatrix} A_x & D_x \\ A_y & D_y \end{vmatrix} - \begin{vmatrix} B_x & C_x \\ B_y & C_y \end{vmatrix}\right) xy + \begin{vmatrix} C_x & D_x \\ C_y & D_y \end{vmatrix} y^2$$

and

$$\varphi'(x,y) = \begin{vmatrix} A_x & C_x \\ A_y & C_y \end{vmatrix} x^2 + \left(\begin{vmatrix} A_x & D_x \\ A_y & D_y \end{vmatrix} + \begin{vmatrix} B_x & C_x \\ B_y & C_y \end{vmatrix}\right) xy + \begin{vmatrix} B_x & D_x \\ B_y & D_y \end{vmatrix} y^2 ,$$

therewith, defining composition.

Some Difficulties

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\left(\begin{smallmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{smallmatrix}\right)$.

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\left(\begin{smallmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{smallmatrix}\right)$.

Second, it seems one has to obtain

$$\begin{aligned}\Phi(x,y) = (B_yC_y - A_yD_y)x^2 \\ + \big((A_xD_y - B_xC_y) - (A_yD_x - B_yC_x)\big)xy \\ + (B_xC_x - A_xD_x)y^2\end{aligned}$$

by brute force calculation

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\begin{pmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{pmatrix}$.

Second, it seems one has to obtain

$$\begin{aligned}\Phi(x,y) = (B_yC_y - A_yD_y)x^2 \\ + \big((A_xD_y - B_xC_y) - (A_yD_x - B_yC_x)\big)xy \\ + (B_xC_x - A_xD_x)y^2\end{aligned}$$

by brute force calculation, or by looking it up.

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\left(\begin{smallmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{smallmatrix}\right)$.

Second, it seems one has to obtain

$$\begin{aligned}\Phi(x,y) = (B_yC_y - A_yD_y)x^2 \\ + \big((A_xD_y - B_xC_y) - (A_yD_x - B_yC_x)\big)xy \\ + (B_xC_x - A_xD_x)y^2\end{aligned}$$

by brute force calculation, or by looking it up.

Manjul Bhargava's work on higher composition laws amply deals with these first two issues.

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\begin{pmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{pmatrix}$.

Second, it seems one has to obtain

$$\Phi(x,y) = (B_yC_y - A_yD_y)x^2 + \big((A_xD_y - B_xC_y) - (A_yD_x - B_yC_x)\big)xy + (B_xC_x - A_xD_x)y^2$$

by brute force calculation, or by looking it up.

Manjul Bhargava's work on higher composition laws amply deals with these first two issues. I briefly illustrate my gross vulgarisation of that work for the present well known quadratic case

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\begin{pmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{pmatrix}$.

Second, it seems one has to obtain

$$\begin{aligned}\Phi(x,y) = (B_yC_y - A_yD_y)x^2 \\ + \big((A_xD_y - B_xC_y) - (A_yD_x - B_yC_x)\big)xy \\ + (B_xC_x - A_xD_x)y^2\end{aligned}$$

by brute force calculation, or by looking it up.

Manjul Bhargava's work on higher composition laws amply deals with these first two issues. I briefly illustrate my gross vulgarisation of that work for the present well known quadratic case, so as to instance its generalisations to cubic, and quartic fields.

Some Difficulties

First, given φ and φ', it may not be entirely obvious just how, or how best, to determine a 2 by 4 magic matrix $\left(\begin{smallmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{smallmatrix}\right)$.

Second, it seems one has to obtain

$$\begin{multline} \Phi(x,y) = (B_yC_y - A_yD_y)x^2 \\ + \big((A_xD_y - B_xC_y) - (A_yD_x - B_yC_x)\big)xy \\ + (B_xC_x - A_xD_x)y^2 \end{multline}$$

by brute force calculation, or by looking it up.

Manjul Bhargava's work on higher composition laws amply deals with these first two issues. I briefly illustrate my gross vulgarisation of that work for the present well known quadratic case, so as to instance its generalisations to cubic, and quartic fields. My remarks apply without meaningful change to function fields.

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$.

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega \rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$.

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P + \omega)/Q$, ideals $\langle Q, P + \omega\rangle_{\mathbb{Z}}$

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P + \omega)/Q$, ideals $\langle Q, P + \omega\rangle_{\mathbb{Z}}$, and forms $Q(x - \alpha y)(x - \overline{\alpha}y)$.

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P + \omega)/Q$, ideals $\langle Q, P + \omega\rangle_{\mathbb{Z}}$, and forms $Q(x - \alpha y)(x - \overline{\alpha} y)$. Of course that correspondence is no better than 'bi-unique'.

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P + \omega)/Q$, ideals $\langle Q, P + \omega\rangle_{\mathbb{Z}}$, and forms $Q(x - \alpha y)(x - \overline{\alpha} y)$. Of course that correspondence is no better than 'bi-unique'.

In brief, the ideal treats the sign of Q as irrelevant,

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega \rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P + \omega)/Q$, ideals $\langle Q, P + \omega \rangle_{\mathbb{Z}}$, and forms $Q(x - \alpha y)(x - \overline{\alpha} y)$. Of course that correspondence is no better than 'bi-unique'.

In brief, the ideal treats the sign of Q as irrelevant, the number $-(P + \omega)/Q$ has standard form $(-P - T + \omega)/Q$

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P + \omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P + \omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P + \omega)/Q$, ideals $\langle Q, P + \omega\rangle_{\mathbb{Z}}$, and forms $Q(x - \alpha y)(x - \overline{\alpha} y)$. Of course that correspondence is no better than 'bi-unique'.

In brief, the ideal treats the sign of Q as irrelevant, the number $-(P + \omega)/Q$ has standard form $(-P - T + \omega)/Q$ (note the implicit presumption that denominators always are positive), Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P+\omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P+\omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P+\omega)/Q$, ideals $\langle Q, P+\omega\rangle_{\mathbb{Z}}$, and forms $Q(x-\alpha y)(x-\overline{\alpha}y)$. Of course that correspondence is no better than 'bi-unique'.

In brief, the ideal treats the sign of Q as irrelevant, the number $-(P+\omega)/Q$ has standard form $(-P-T+\omega)/Q$ (note the implicit presumption that denominators always are positive), and the form thinks of itself as corresponding to α if its leading coefficient is positive, but to $\overline{\alpha}$ if Q is negative

Denote by ω a quadratic irrational integer of norm N and trace T, and satisfying $\omega > \overline{\omega}$. A typical quadratic element α of a quadratic field $\mathbb{Q}(\omega)$ is conventionally written as $\alpha = (P+\omega)/Q$, with Q dividing the norm $N + TP + P^2$ of its numerator.

The point is that the said convention is equivalent to guaranteeing that the $\mathbb{Z}$-module $\langle Q, P+\omega\rangle$ is an ideal of the domain $\mathbb{Z}[\omega]$. That provides a correspondence between numbers $\alpha = (P+\omega)/Q$, ideals $\langle Q, P+\omega\rangle_{\mathbb{Z}}$, and forms $Q(x-\alpha y)(x-\overline{\alpha}y)$. Of course that correspondence is no better than 'bi-unique'.

In brief, the ideal treats the sign of Q as irrelevant, the number $-(P+\omega)/Q$ has standard form $(-P-T+\omega)/Q$ (note the implicit presumption that denominators always are positive), and the form thinks of itself as corresponding to α if its leading coefficient is positive, but to $\overline{\alpha}$ if Q is negative (determining the sign of Q requires a convention as to the fixed sign of coefficients of xy).

Now set $\varphi(x,y) = Q(x-\alpha y)(x-\overline{\alpha}y)$, $\varphi'(x,y) = Q'(x-\alpha' y)(x-\overline{\alpha}' y)$.

Now set $\varphi(x,y) = Q(x-\alpha y)(x-\overline{\alpha}y)$, $\varphi'(x,y) = Q'(x-\alpha' y)(x-\overline{\alpha}' y)$. Then $\omega^2 - T\omega + N = 0$, and an intelligent look at the product

$$G(X-\alpha Y)(X'-\alpha' Y') = (x-\alpha'' y) =$$

$$(A_x XX' + B_x XY' + C_x X'Y + D_x YY') - \alpha''(A_y XX' + B_y XY' + C_y X'Y + D_y YY'),$$

readily reveals the magic matrix $M(\varphi, \varphi')$ to be

$$\begin{pmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{pmatrix} = \begin{pmatrix} G & B & C & D \\ 0 & Q/G & Q'/G & -(P+P'+T)/G \end{pmatrix},$$

Now set $\varphi(x,y) = Q(x-\alpha y)(x-\overline{\alpha}y)$, $\varphi'(x,y) = Q'(x-\alpha' y)(x-\overline{\alpha}' y)$. Then $\omega^2 - T\omega + N = 0$, and an intelligent look at the product

$$G(X-\alpha Y)(X'-\alpha' Y') = (x-\alpha'' y) =$$

$$(A_x XX' + B_x XY' + C_x X'Y + D_x YY') - \alpha''(A_y XX' + B_y XY' + C_y X'Y + D_y YY'),$$

readily reveals the magic matrix $M(\varphi, \varphi')$ to be

$$\begin{pmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{pmatrix} = \begin{pmatrix} G & B & C & D \\ 0 & Q/G & Q'/G & -(P+P'+T)/G \end{pmatrix},$$

with

$$G = \gcd(Q, Q', P+P+T).$$

Now set $\varphi(x,y) = Q(x-\alpha y)(x-\overline{\alpha}y)$, $\varphi'(x,y) = Q'(x-\alpha' y)(x-\overline{\alpha}' y)$. Then $\omega^2 - T\omega + N = 0$, and an intelligent look at the product

$$G(X-\alpha Y)(X'-\alpha' Y') = (x-\alpha'' y) =$$

$$(A_x XX' + B_x XY' + C_x X'Y + D_x YY') - \alpha''(A_y XX' + B_y XY' + C_y X'Y + D_y YY'),$$

readily reveals the magic matrix $M(\varphi, \varphi')$ to be

$$\begin{pmatrix} A_x & B_x & C_x & D_x \\ A_y & B_y & C_y & D_y \end{pmatrix} = \begin{pmatrix} G & B & C & D \\ 0 & Q/G & Q'/G & -(P+P'+T)/G \end{pmatrix},$$

with

$$G = \gcd(Q, Q', P+P+T).$$

Here B and C are obtained from $BQ' - CQ = G(P-P')$ and the Euclidean algorithm; that yields D, or one obtains it similarly.

A crude reformulation of Manjul Bhargava's wonderful observations begins with noticing that the two given forms

A crude reformulation of Manjul Bhargava's wonderful observations begins with noticing that the two given forms

$$\begin{vmatrix} A_x x + B_x y & C_x x + D_x y \\ A_y x + B_y y & C_y x + D_y y \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} A_x x + C_x y & A_y x + C_y y \\ B_x x + D_x y & B_y x + D_y y \end{vmatrix}$$

A crude reformulation of Manjul Bhargava's wonderful observations begins with noticing that the two given forms

$$\begin{vmatrix} A_x x + B_x y & C_x x + D_x y \\ A_y x + B_y y & C_y x + D_y y \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} A_x x + C_x y & A_y x + C_y y \\ B_x x + D_x y & B_y x + D_y y \end{vmatrix}$$

may be viewed simply as pairs of opposite faces

$$(A_x B_x A_y B_y, C_x D_x C_y D_y) \quad \text{and} \quad (A_x C_x B_x D_x, A_y C_y B_x D_x)$$

of a cube.

A crude reformulation of Manjul Bhargava's wonderful observations begins with noticing that the two given forms

$$\begin{vmatrix} A_x x + B_x y & C_x x + D_x y \\ A_y x + B_y y & C_y x + D_y y \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} A_x x + C_x y & A_y x + C_y y \\ B_x x + D_x y & B_y x + D_y y \end{vmatrix}$$

may be viewed simply as pairs of opposite faces

$$(A_x B_x A_y B_y, C_x D_x C_y D_y) \quad \text{and} \quad (A_x C_x B_x D_x, A_y C_y B_x D_x)$$

of a cube. Then the third pair $(A_x A_y B_x B_y, C_x C_y B_x D_x D_y)$ of opposite faces corresponds to the form

$$\begin{vmatrix} A_x x + A_y y & C_x x + C_y y \\ B_x x + B_y y & D_x x + D_y y \end{vmatrix}$$

and, this is the point

A crude reformulation of Manjul Bhargava's wonderful observations begins with noticing that the two given forms

$$\begin{vmatrix} A_x x + B_x y & C_x x + D_x y \\ A_y x + B_y y & C_y x + D_y y \end{vmatrix} \quad \text{and} \quad \begin{vmatrix} A_x x + C_x y & A_y x + C_y y \\ B_x x + D_x y & B_y x + D_y y \end{vmatrix}$$

may be viewed simply as pairs of opposite faces

$$(A_x B_x A_y B_y, C_x D_x C_y D_y) \quad \text{and} \quad (A_x C_x B_x D_x, A_y C_y B_x D_x)$$

of a cube. Then the third pair $(A_x A_y B_x B_y, C_x C_y B_x D_x D_y)$ of opposite faces corresponds to the form

$$\begin{vmatrix} A_x x + A_y y & C_x x + C_y y \\ B_x x + B_y y & D_x x + D_y y \end{vmatrix}$$

and, this is the point, the "cube law", which sets the compound of these three forms to be the trivial form $(x - \omega y)(x - \overline{\omega} y)$ of their common discriminant, naturally defines a compounding of forms.

Ideals

One readily de-forms the remarks above by noting that composition immediately provides a rule for multiplying ideals presented as $\mathbb{Z}$-modules.

Ideals

One readily de-forms the remarks above by noting that composition immediately provides a rule for multiplying ideals presented as $\mathbb{Z}$-modules. Set $\alpha'' = (p + \omega)/q$.

Ideals

One readily de-forms the remarks above by noting that composition immediately provides a rule for multiplying ideals presented as $\mathbb{Z}$-modules. Set $\alpha'' = (p+\omega)/q$. Then

$$qG\big(Qx-(\omega+P)y\big)\big(Q'x'-(\omega+P')y'\big)=QQ'\big(qX-(\omega+p)Y\big)\,,$$

Ideals

One readily de-forms the remarks above by noting that composition immediately provides a rule for multiplying ideals presented as $\mathbb{Z}$-modules. Set $\alpha'' = (p+\omega)/q$. Then

$$qG\big(Qx-(\omega+P)y\big)\big(Q'x'-(\omega+P')y'\big) = QQ'\big(qX-(\omega+p)Y\big)\,,$$

plainly asserting that

$$\langle Q,\omega+P\rangle\langle Q',\omega+P'\rangle = G\langle q,\omega+p\rangle$$

Ideals

One readily de-forms the remarks above by noting that composition immediately provides a rule for multiplying ideals presented as $\mathbb{Z}$-modules. Set $\alpha'' = (p+\omega)/q$. Then

$$qG\bigl(Qx-(\omega+P)y\bigr)\bigl(Q'x'-(\omega+P')y'\bigr) = QQ'\bigl(qX-(\omega+p)Y\bigr),$$

plainly asserting that

$$\langle Q, \omega+P\rangle\langle Q', \omega+P'\rangle = G\langle q, \omega+p\rangle$$

if $q(x-\alpha''y)(x-\overline{\alpha}''y)$ is the composite of the two given forms $Q(x-\alpha y)(x-\overline{\alpha}y)$ and $Q'(x-\alpha' y)(x-\overline{\alpha}' y)$.

Ideals

One readily de-forms the remarks above by noting that composition immediately provides a rule for multiplying ideals presented as $\mathbb{Z}$-modules. Set $\alpha'' = (p+\omega)/q$. Then

$$qG\big(Qx-(\omega+P)y\big)\big(Q'x'-(\omega+P')y'\big) = QQ'\big(qX-(\omega+p)Y\big)\,,$$

plainly asserting that

$$\langle Q,\omega+P\rangle\langle Q',\omega+P'\rangle = G\langle q,\omega+p\rangle$$

if $q(x-\alpha''y)(x-\overline{\alpha}''y)$ is the composite of the two given forms $Q(x-\alpha y)(x-\overline{\alpha}y)$ and $Q'(x-\alpha' y)(x-\overline{\alpha}' y)$.

Note that the 'infrastructural composition' I detail is well defined on forms or ideals whereas compounding is well defined only on equivalence classes of forms, or ideals.

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite.

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi, \varphi')$, whose entries are single precision (the precision of the data)

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi, \varphi')$, whose entries are single precision (the precision of the data), rather than the double precision coefficients of the raw composite.

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi, \varphi')$, whose entries are single precision (the precision of the data), rather than the double precision coefficients of the raw composite. In practice, it essentially suffices to apply the Euclidean algorithm to the pair $(B_x, B_y) = (B, Q/G)$ until one has two remainders of half-precision.

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi, \varphi')$, whose entries are single precision (the precision of the data), rather than the double precision coefficients of the raw composite. In practice, it essentially suffices to apply the Euclidean algorithm to the pair $(B_x, B_y) = (B, Q/G)$ until one has two remainders of half-precision. That also supplies the data necessary to obtain enough of the reduced magic matrix $\mathcal{M}(\varphi, \varphi')$ to write a reduced composite

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi, \varphi')$, whose entries are single precision (the precision of the data), rather than the double precision coefficients of the raw composite. In practice, it essentially suffices to apply the Euclidean algorithm to the pair $(B_x, B_y) = (B, Q/G)$ until one has two remainders of half-precision. That also supplies the data necessary to obtain enough of the reduced magic matrix $\mathcal{M}(\varphi, \varphi')$ to write a reduced composite and to compute its position (distance) in the cycle of forms.

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi, \varphi')$, whose entries are single precision (the precision of the data), rather than the double precision coefficients of the raw composite. In practice, it essentially suffices to apply the Euclidean algorithm to the pair $(B_x, B_y) = (B, Q/G)$ until one has two remainders of half-precision. That also supplies the data necessary to obtain enough of the reduced magic matrix $\mathcal{M}(\varphi, \varphi')$ to write a reduced composite and to compute its position (distance) in the cycle of forms.

By happy chance, that reduction process also appears in general to find the 'nearest' reduced form (a matter of issue in the real = indefinite case)

Reduction

I add as an aside that the algorithmic issue in composing pairs of quadratic forms of course is not cute formulæ but the time taken to reduce a composite. Dan Shanks's NUCOMP deals with that by reducing the magic matrix $M(\varphi,\varphi')$, whose entries are single precision (the precision of the data), rather than the double precision coefficients of the raw composite. In practice, it essentially suffices to apply the Euclidean algorithm to the pair $(B_x,B_y)=(B,Q/G)$ until one has two remainders of half-precision. That also supplies the data necessary to obtain enough of the reduced magic matrix $\mathcal{M}(\varphi,\varphi')$ to write a reduced composite and to compute its position (distance) in the cycle of forms.

By happy chance, that reduction process also appears in general to find the 'nearest' reduced form (a matter of issue in the real = indefinite case) apparently because that process reduces to the 'previous' reduced form.

The Cubic Case

One might think that in the cubic case one should look at ternary cubic forms and therefore at $3 \times 3 \times 3$ cubes of integers.

The Cubic Case

One might think that in the cubic case one should look at ternary cubic forms and therefore at $3 \times 3 \times 3$ cubes of integers. A "cube rule" then does give a composition law, but for more than one wants

The Cubic Case

One might think that in the cubic case one should look at ternary cubic forms and therefore at $3 \times 3 \times 3$ cubes of integers. A "cube rule" then does give a composition law, but for more than one wants, because ideal classes correspond just to the decomposable forms.

The Cubic Case

One might think that in the cubic case one should look at ternary cubic forms and therefore at $3 \times 3 \times 3$ cubes of integers. A "cube rule" then does give a composition law, but for more than one wants, because ideal classes correspond just to the decomposable forms.

Bhargava explains that the correct box is $2 \times 3 \times 3$, thus a pair (A, B) of 3×3 matrices, and that the unique $\mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ invariant is a cubic form

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dx^3 = \det(Ax - By)\,.$$

The Cubic Case

One might think that in the cubic case one should look at ternary cubic forms and therefore at $3 \times 3 \times 3$ cubes of integers. A "cube rule" then does give a composition law, but for more than one wants, because ideal classes correspond just to the decomposable forms.

Bhargava explains that the correct box is $2 \times 3 \times 3$, thus a pair (A, B) of 3×3 matrices, and that the unique $\mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ invariant is a cubic form

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dx^3 = \det(Ax - By)\,.$$

Hence the unique $\Gamma = \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ invariant is the discriminant $\mathrm{Disc}(f)$ of f.

Bhargava notes that there is a canonical correspondence between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral cubic forms and isomorphism classes of cubic rings.

Bhargava notes that there is a canonical correspondence between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral cubic forms and isomorphism classes of cubic rings.

Specifically, given a cubic ring R (a ring free of rank 3 as a $\mathbb{Z}$-module), take $(1, \omega, \theta)$ as a Z-basis for R. A 'normal' such basis has $\omega \cdot \theta \in \mathbb{Z}$ and one may define seven integers a, ... ,n by setting

$$\omega\theta = n\,, \qquad \omega^2 = m + b\omega - a\theta\,, \qquad \theta^2 = l + d\omega - c\theta\,.$$

Bhargava notes that there is a canonical correspondence between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral cubic forms and isomorphism classes of cubic rings.

Specifically, given a cubic ring R (a ring free of rank 3 as a $\mathbb{Z}$-module), take $(1, \omega, \theta)$ as a Z-basis for R. A 'normal' such basis has $\omega \cdot \theta \in \mathbb{Z}$ and one may define seven integers a, $\ldots$, n by setting

$$\omega\theta = n\,, \qquad \omega^2 = m + b\omega - a\theta\,, \qquad \theta^2 = l + d\omega - c\theta\,.$$

Then the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega\theta \cdot \theta$ yield as unique solution

$$\omega\theta = -ad\,, \qquad \omega^2 = -ac + b\omega - a\theta\,, \qquad \theta^2 = -bd + d\omega - c\theta$$

Bhargava notes that there is a canonical correspondence between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral cubic forms and isomorphism classes of cubic rings.

Specifically, given a cubic ring R (a ring free of rank 3 as a $\mathbb{Z}$-module), take $(1, \omega, \theta)$ as a Z-basis for R. A 'normal' such basis has $\omega \cdot \theta \in \mathbb{Z}$ and one may define seven integers a, ... ,n by setting

$$\omega\theta = n\,, \qquad \omega^2 = m + b\omega - a\theta\,, \qquad \theta^2 = l + d\omega - c\theta\,.$$

Then the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega\theta \cdot \theta$ yield as unique solution

$$\omega\theta = -ad\,, \qquad \omega^2 = -ac + b\omega - a\theta\,, \qquad \theta^2 = -bd + d\omega - c\theta$$

and it follows that a binary cubic form $\det(Ax - By)$ leads to a unique cubic ring.

Bhargava notes that there is a canonical correspondence between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral cubic forms and isomorphism classes of cubic rings.

Specifically, given a cubic ring R (a ring free of rank 3 as a $\mathbb{Z}$-module), take $(1, \omega, \theta)$ as a Z-basis for R. A 'normal' such basis has $\omega \cdot \theta \in \mathbb{Z}$ and one may define seven integers a, … ,n by setting

$$\omega\theta = n\,, \qquad \omega^2 = m + b\omega - a\theta\,, \qquad \theta^2 = l + d\omega - c\theta\,.$$

Then the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega\theta \cdot \theta$ yield as unique solution

$$\omega\theta = -ad\,, \qquad \omega^2 = -ac + b\omega - a\theta\,, \qquad \theta^2 = -bd + d\omega - c\theta$$

and it follows that a binary cubic form $\det(Ax - By)$ leads to a unique cubic ring. Moreover, a $\mathrm{GL}_2(\mathbb{Z})$ transformation of the basis (ω, θ) of R/Z (and a subsequent renormalisation) transforms $f(x, y)$ by the same transformation.

Ideals in Cubic Rings

Bhargava calls a pair (I, I') of (fractional) ideals of R ‘balanced’ if $II' \subseteq R$ and $\mathrm{Norm}(I)\,\mathrm{Norm}(I') = 1$;

Ideals in Cubic Rings

Bhargava calls a pair (I, I') of (fractional) ideals of R ‘balanced’ if $II' \subseteq R$ and $\mathrm{Norm}(I)\,\mathrm{Norm}(I') = 1$; loosely, an equivalence class of balanced pairs is a pair of equivalence classes of ideals inverse to one another in the ideal class group.

Ideals in Cubic Rings

Bhargava calls a pair (I, I') of (fractional) ideals of R 'balanced' if $II' \subseteq R$ and $\mathrm{Norm}(I)\,\mathrm{Norm}(I') = 1$; loosely, an equivalence class of balanced pairs is a pair of equivalence classes of ideals inverse to one another in the ideal class group. Then the nondegenerate orbits of Γ acting on the boxes of integers correspond to the isomorphism classes of pairs $\big(R, (I, I')\big)$.

Ideals in Cubic Rings

Bhargava calls a pair (I, I') of (fractional) ideals of R 'balanced' if $II' \subseteq R$ and $\mathrm{Norm}(I)\,\mathrm{Norm}(I') = 1$; loosely, an equivalence class of balanced pairs is a pair of equivalence classes of ideals inverse to one another in the ideal class group. Then the nondegenerate orbits of Γ acting on the boxes of integers correspond to the isomorphism classes of pairs $\big(R, (I, I')\big)$.

The explicit correspondence asks one to write $I = \langle \alpha_1, \alpha_2, \alpha_3 \rangle_{\mathbb{Z}}$, $I' = \langle \alpha'_1, \alpha'_2, \alpha'_3 \rangle_{\mathbb{Z}}$ and, recalling $II' \subseteq R = \langle 1, \omega, \theta \rangle$, to compute all the $\alpha_i \alpha'_j = c_{ij} + a_{ij}\omega + b_{ij}\theta$. Then $A = (a_{ij})$, $B = (b_{ij})$ will do.

Ideals in Cubic Rings

Bhargava calls a pair (I, I') of (fractional) ideals of R 'balanced' if $II' \subseteq R$ and $\mathrm{Norm}(I)\,\mathrm{Norm}(I') = 1$; loosely, an equivalence class of balanced pairs is a pair of equivalence classes of ideals inverse to one another in the ideal class group. Then the nondegenerate orbits of Γ acting on the boxes of integers correspond to the isomorphism classes of pairs $\big(R, (I, I')\big)$.

The explicit correspondence asks one to write $I = \langle \alpha_1, \alpha_2, \alpha_3 \rangle_{\mathbb{Z}}$, $I' = \langle \alpha'_1, \alpha'_2, \alpha'_3 \rangle_{\mathbb{Z}}$ and, recalling $II' \subseteq R = \langle 1, \omega, \theta \rangle$, to compute all the $\alpha_i \alpha'_j = c_{ij} + a_{ij}\omega + b_{ij}\theta$. Then $A = (a_{ij})$, $B = (b_{ij})$ will do. This all follows from the trivial case $I = I' = R$, when

$$(A, B) = \left(\begin{bmatrix} & & 1 \\ & -a & \\ 1 & & -c \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & b & \\ & & d \end{bmatrix} \right).$$

The pair (A, B) just now given display the principal class of forms defined by f.

The pair (A, B) just now given display the principal class of forms defined by f.

Manjul delightedly shows that, eventually, the R-module structure of the I, respectively I', given by the correspondence is explicitly given in terms of determinants made from the columns, respectively rows of A and B

The pair (A, B) just now given display the principal class of forms defined by f.

Manjul delightedly shows that, eventually, the R-module structure of the I, respectively I', given by the correspondence is explicitly given in terms of determinants made from the columns, respectively rows of A and B, instanced by

$$-\omega \cdot \alpha_1 = |B_1 A_2 A_3| \cdot \alpha_1 + |A_1 B_1 A_3| \cdot \alpha_2 + |A_1 A_2 B_1| \cdot \alpha_3$$

$$-\omega \cdot \alpha_2 = |B_2 A_2 A_3| \cdot \alpha_1 + |A_1 B_2 A_3| \cdot \alpha_2 + |A_1 A_2 B_2| \cdot \alpha_3$$

$$-\omega \cdot \alpha_3 = |B_3 A_2 A_3| \cdot \alpha_1 + |A_1 B_3 A_3| \cdot \alpha_2 + |A_1 A_2 B_3| \cdot \alpha_3$$

$$-\theta \cdot \alpha_1 = |A_1 B_2 B_3| \cdot \alpha_1 + |B_1 A_1 B_3| \cdot \alpha_2 + |B_1 B_2 A_1| \cdot \alpha_3$$

$$-\theta \cdot \alpha_2 = |A_2 B_2 B_3| \cdot \alpha_1 + |B_1 A_2 B_3| \cdot \alpha_2 + |B_1 B_2 A_2| \cdot \alpha_3$$

$$-\theta \cdot \alpha_3 = |A_3 B_2 B_3| \cdot \alpha_1 + |B_1 A_3 B_3| \cdot \alpha_2 + |B_1 B_2 A_3| \cdot \alpha_3$$

Composition

Ultimately, composition is defined in terms of multiplication of ideal pairs (I, I'). Bhargava presses the analogy:

Composition

Ultimately, composition is defined in terms of multiplication of ideal pairs (I, I'). Bhargava presses the analogy:

In the case of binary quadratic forms, the unique $\mathrm{SL}_2(\mathbb{Z})$-invariant is the discriminant D, which classifies orders in quadratic fields. The primitive classes having a fixed value of D form a group under a certain natural composition law. This group is naturally isomorphic to the narrow class group of the corresponding quadratic order.

Composition

Ultimately, composition is defined in terms of multiplication of ideal pairs (I, I'). Bhargava presses the analogy:

In the case of binary quadratic forms, the unique $\mathrm{SL}_2(\mathbb{Z})$-invariant is the discriminant D, which classifies orders in quadratic fields. The primitive classes having a fixed value of D form a group under a certain natural composition law. This group is naturally isomorphic to the narrow class group of the corresponding quadratic order.

In the case of $2 \times 3 \times 3$ integer boxes, the unique $\mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-invariant is the cubic form f, which classifies orders in cubic fields. The projective classes having a fixed value of f form a group under a certain natural composition law. This group is naturally isomorphic to the ideal class group of the corresponding cubic order.

References

Manjul Bhargava:

References

Manjul Bhargava:

'Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations', *Ann. of Math.* (2) **159** (2004), no. 1, 217–250;

References

Manjul Bhargava:

'Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations', *Ann. of Math.* (2) **159** (2004), no. 1, 217–250;

'Higher composition laws. II. On cubic analogues of Gauss composition', *Ann. of Math.* (2) **159** (2004), no. 2, 865–886;

References

Manjul Bhargava:

'Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations', *Ann. of Math.* (2) **159** (2004), no. 1, 217–250;

'Higher composition laws. II. On cubic analogues of Gauss composition', *Ann. of Math.* (2) **159** (2004), no. 2, 865–886;

'Higher composition laws. III. The parametrization of quartic rings', *Ann. of Math.* (2) **159** (2004), no. 3, 1329–1360;

References

Manjul Bhargava:

'Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations', *Ann. of Math.* (2) **159** (2004), no. 1, 217–250;

'Higher composition laws. II. On cubic analogues of Gauss composition', *Ann. of Math.* (2) **159** (2004), no. 2, 865–886;

'Higher composition laws. III. The parametrization of quartic rings', *Ann. of Math.* (2) **159** (2004), no. 3, 1329–1360;

'The density of discriminants of quartic rings and fields', *Ann. of Math.* (2) **162** (2005), no. 2, 1031–1063.