Integers, Modular Groups, and Hyperbolic Space

NORMAN W. JOHNSON
Wheaton College (Mass.)

International Conference on
Geometry and Symmetry

Veszprém, Hungary
July 3, 2015

ABSTRACT. In each of the normed division algebras over the real field $\mathbb{R}$—namely, $\mathbb{R}$ itself, the complex numbers $\mathbb{C}$, the quaternions $\mathbb{H}$, and the octonions $\mathbb{O}$—certain elements can be characterized as *integers*. An integer of norm 1 is a *unit*. In a *basic system* of integers the units span a 1-, 2-, 4-, or 8-dimensional lattice, the points of which are the vertices of a regular or uniform Euclidean honeycomb. A *modular group* is a group of linear fractional transformations whose coefficients are integers in some basic system. In the case of the octonions, which have a nonassociative multiplication, such transformations form a *modular loop*. Each real, complex, or quaternionic modular group can be identified with a subgroup of a Coxeter group operating in hyperbolic space of 2, 3, or 5 dimensions.

Linear Fractional Transformations

When each point of a projective line FP^1 over a field F is identified uniquely either with an element x of F or with the extended value ∞, a projectivity (i.e., a permutation of the points of FP^1 that preserves cross ratios) can be expressed as a *linear fractional* transformation of the extended field $\mathrm{F} \cup \{\infty\}$, defined for four given field elements a, b, c, d ($ad - bc \neq 0$) by

$$x \longmapsto \frac{ax + c}{bx + d},$$

with $-d/b \longmapsto \infty$ and $\infty \longmapsto a/b$ if $b \neq 0$ and with $\infty \longmapsto \infty$ if $b = 0$. Such mappings can also be represented by 2×2 invertible matrices over F, constituting the *projective general linear* group $\mathrm{PGL}_2(\mathrm{F})$.

The Hyperbolic Plane

The complex projective line $\mathbb{CP}^1$ with one point fixed, represented in $\mathbb{R}^2$ by the familiar Argand diagram, provides a conformal model for the hyperbolic plane H^2. Points in the "upper half-plane" $\operatorname{Im} z > 0$ are the *ordinary* points of H^2, and the real axis represents the *absolute circle*. The isometry group of H^2 is the *projective pseudo-orthogonal* group $\mathrm{PO}_{2,1}$, isomorphic to the group of linear fractional transformations

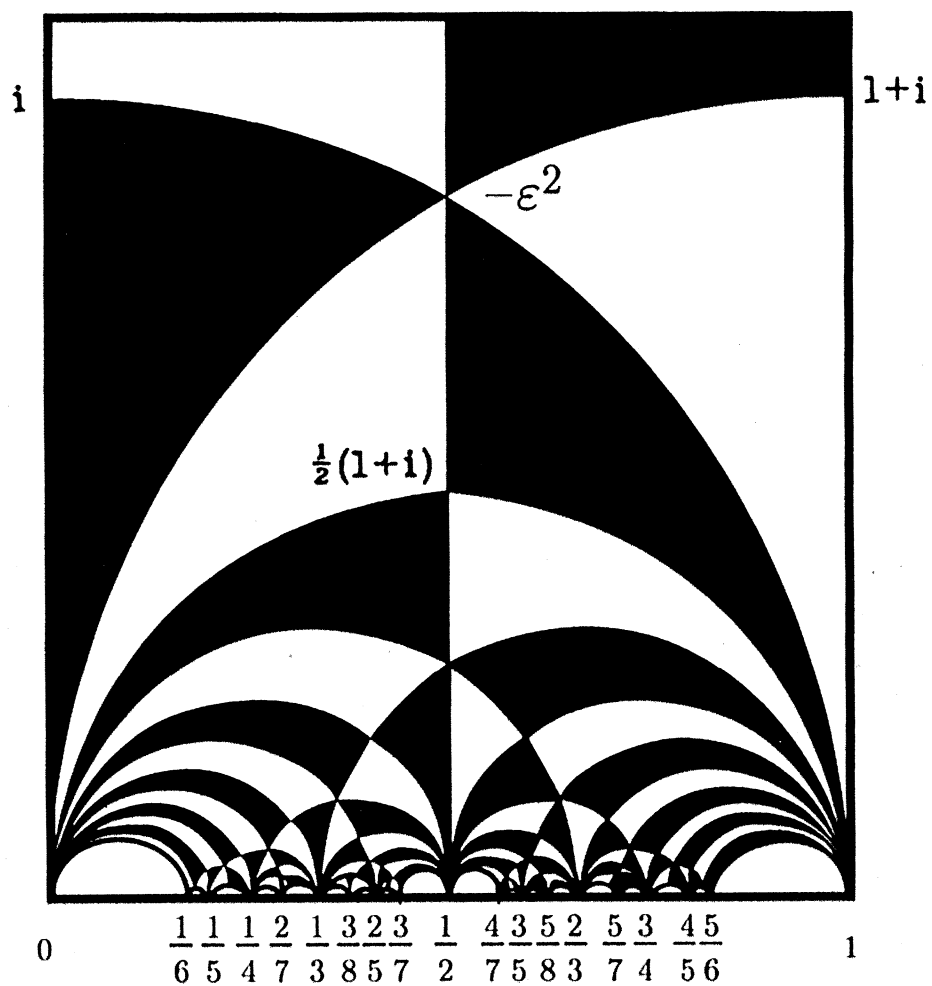$$\cdot \langle A \rangle : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$$

with A real and $\det A \neq 0$, i.e., the (real) projective general linear group PGL_2. The subgroup $\mathrm{P}^+\mathrm{O}_{2,1}$ of direct isometries is isomorphic to the (real) *projective special linear* group PSL_2 (with $\det A > 0$).
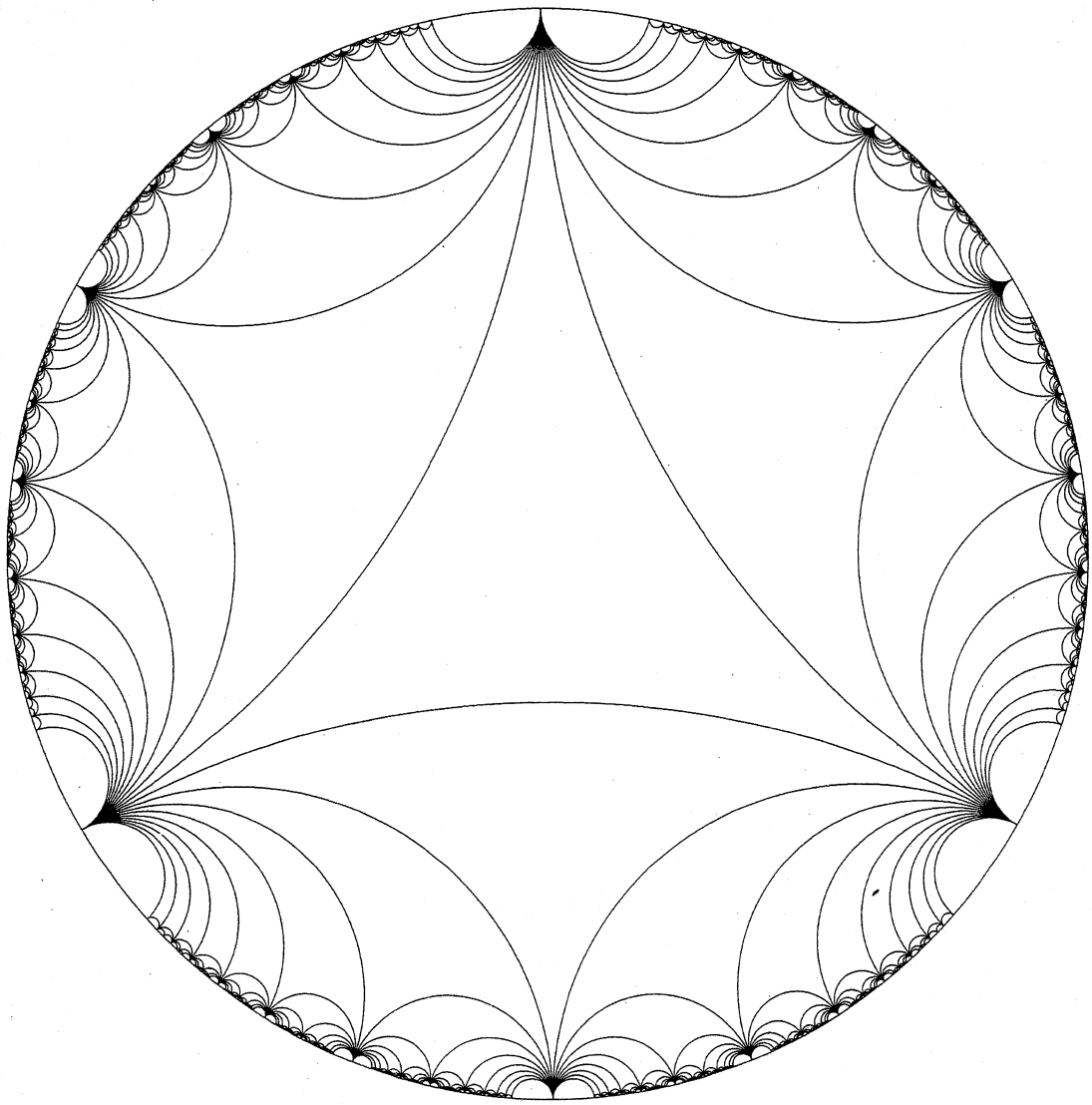
Modular Transformations

The set of 2×2 matrices A over the rational integers $\mathbb{Z}$ with $\det A = \pm 1$ forms the *unit linear* group $\bar{\mathrm{S}}\mathrm{L}_2(\mathbb{Z})$. The subgroup of matrices A with $\det A = 1$ is the *special linear* group $\mathrm{SL}_2(\mathbb{Z})$. The corresponding group $\mathrm{PSL}_2(\mathbb{Z})$ of linear fractional transformations $\cdot\langle A \rangle$ is the (rational) *modular group*, with $\mathrm{P}\bar{\mathrm{S}}\mathrm{L}_2(\mathbb{Z})$ being the *extended modular group*.

Felix Klein showed in 1879 (cf. Poincaré 1882) that the modular group is isomorphic to the rotation group of the regular hyperbolic tessellation $\{3, \infty\}$. This is the direct subgroup of the paracompact Coxeter group $[3, \infty]$:

$$\mathrm{PSL}_2(\mathbb{Z}) \cong [3, \infty]^+.$$

i $1+i$

$-\varepsilon^2$

$\tfrac{1}{2}(1+i)$

0 $\dfrac{1}{6}\,\dfrac{1}{5}\,\dfrac{1}{4}\,\dfrac{2}{7}\,\dfrac{1}{3}\,\dfrac{3}{8}\,\dfrac{2}{5}\,\dfrac{3}{7}\quad\dfrac{1}{2}\quad\dfrac{4}{7}\,\dfrac{3}{5}\,\dfrac{5}{8}\,\dfrac{2}{3}\,\dfrac{5}{7}\,\dfrac{3}{4}\,\dfrac{4}{5}\,\dfrac{5}{6}$ 1

Hyperbolic 3-Space

The absolute $(n-1)$-sphere of hyperbolic n-space H^n has the geometry of *inversive* $(n-1)$-space I^{n-1}. For $n > 1$ the group $\mathrm{PO}_{n,1}$ of isometries of H^n is isomorphic to the group of circularities (homographies and antihomographies) of I^{n-1}. When $n = 2$, this is the group $\mathrm{PGL}_2 \cong \mathrm{PGL}_2(\mathbb{R})$ of linear fractional transformations $\cdot\langle A \rangle$ with A real. When $n = 3$, it is the group $\mathrm{PGL}_2(\mathbb{C})$ of linear fractional transformations

$$\cdot\langle A \rangle : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$$

with A complex, i.e., the group of projectivities of the complex projective line $\mathbb{C}\mathrm{P}^1$.

Quadratic Integers

For any square-free rational integer $d \neq 1$, the *quadratic field* $\mathbb{Q}(\sqrt{d})$ has elements $r + s\sqrt{d}$, where r and s are rational. The *conjugate* of $a = r + s\sqrt{d}$ is $\tilde{a} = r - s\sqrt{d}$, its *trace* $\operatorname{tr} a$ is $a + \tilde{a} = 2r$, and its *norm* $N(a)$ is $a\tilde{a} = r^2 - s^2 d$. The elements a with both $\operatorname{tr} a$ and $N(a)$ in $\mathbb{Z}$ are *quadratic integers* and constitute an integral domain, a two-dimensional algebra $\mathbb{Z}^2(d)$ over $\mathbb{Z}$, whose invertible elements, or *units*, have norm ± 1.

For $d > 0$ the elements of $\mathbb{Z}^2(d)$ are real and there are infinitely many units. When $d < 0$, $\mathbb{Z}^2(d)$ has both real and imaginary elements, the conjugate of z is its complex conjugate $\bar{z}$, $\operatorname{tr} z = 2\operatorname{Re} z$, $N(z) = |z|^2$, and (with two exceptions) the only units are ± 1.

The Gaussian Integers

Complex numbers of the form $g_0 + g_1 i$, where g_0 and g_1 are rational integers and $i = \sqrt{-1}$, belong to the ring $\mathbb{G} = \mathbb{Z}[i]$ of *Gaussian integers*. There are four units in all: ± 1 and $\pm i$. When the complex field $\mathbb{C}$ is regarded as a two-dimensional vector space over $\mathbb{R}$, the Gaussian integers constitute a two-dimensional lattice C_2 spanned by the units 1 and i. The points of C_2 are the vertices of a regular tessellation $\{4, 4\}$ of the Euclidean plane.
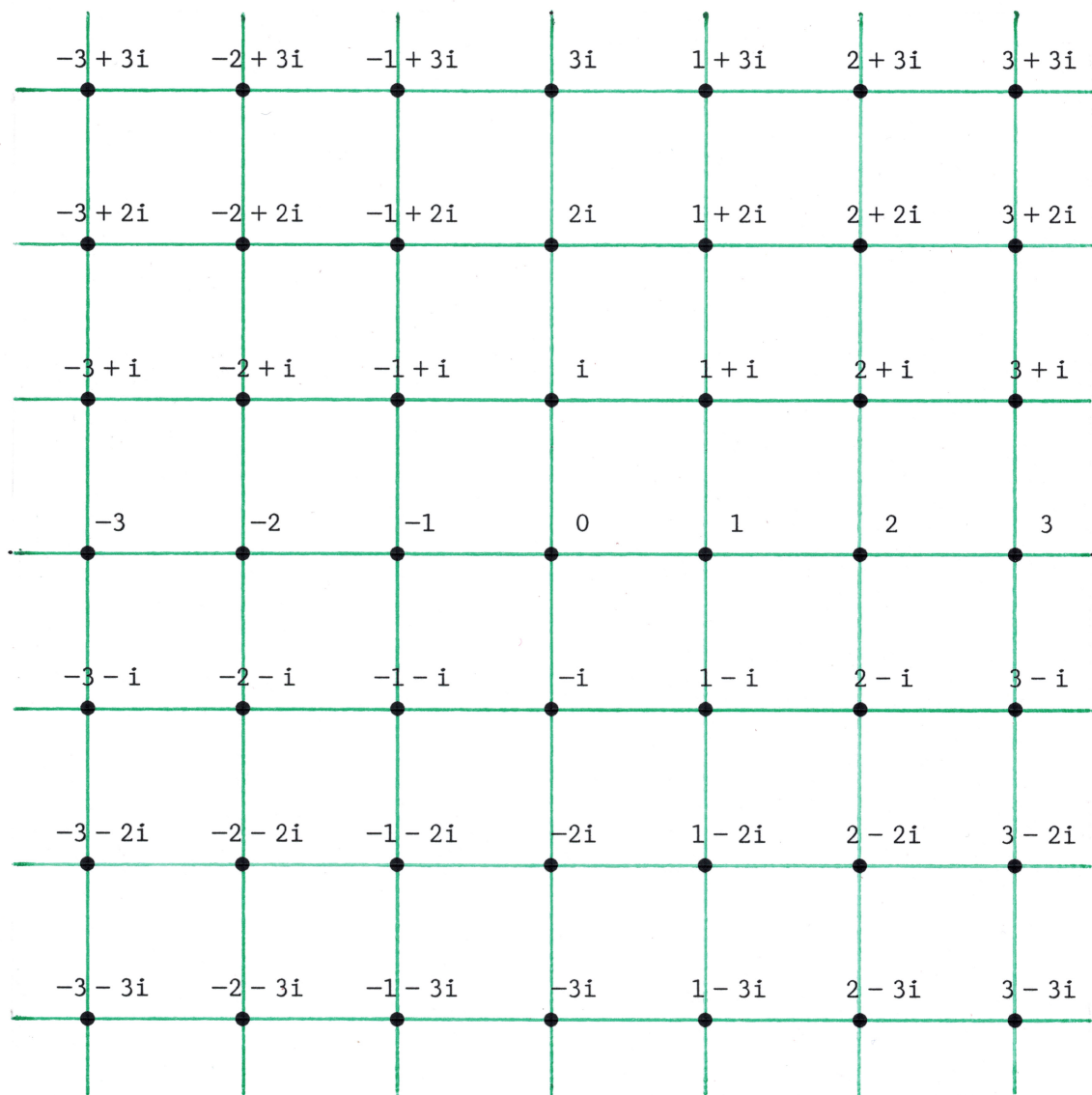
$-3+3i$	$-2+3i$	$-1+3i$	$3i$	$1+3i$	$2+3i$	$3+3i$
$-3+2i$	$-2+2i$	$-1+2i$	$2i$	$1+2i$	$2+2i$	$3+2i$
$-3+i$	$-2+i$	$-1+i$	i	$1+i$	$2+i$	$3+i$
-3	-2	-1	0	1	2	3
$-3-i$	$-2-i$	$-1-i$	$-i$	$1-i$	$2-i$	$3-i$
$-3-2i$	$-2-2i$	$-1-2i$	$-2i$	$1-2i$	$2-2i$	$3-2i$
$-3-3i$	$-2-3i$	$-1-3i$	$-3i$	$1-3i$	$2-3i$	$3-3i$

Fig. 1. The Gaussian integers

The Gaussian Modular Group

Just as restricting the coefficients of linear fractional transformations $\cdot\langle A \rangle$ to rational integers defines the rational modular group $\mathrm{PSL}_2(\mathbb{Z})$, so restricting them to Gaussian integers defines the *Gaussian modular group* $\mathrm{PSL}_2(\mathbb{G})$. This group was first described by Émile Picard in 1884 and is commonly known as the "Picard group."

In 1897 Fricke and Klein identified $\mathrm{PSL}_2(\mathbb{G})$ with a subgroup of the rotation group of the hyperbolic honeycomb $\{3, 4, 4\}$ (cf. Magnus 1974). Schulte and Weiss (1994) showed that it is a subgroup of index 2 in $[3, 4, 4]^+$, and Monson and Weiss (1995) exhibited it as a subgroup of index 2 in the hyper-compact Coxeter group $[\infty, 3, 3, \infty]$.

The Eisenstein Integers

Complex numbers of the form $e_0 + e_1\omega$, where e_0 and e_1 are rational integers and $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, belong to the ring $\mathbb{E} = \mathbb{Z}[\omega]$ of *Eisenstein integers*. There are six units: ± 1, $\pm\omega$, $\pm\omega^2$. When the complex field $\mathbb{C}$ is regarded as a two-dimensional vector space over $\mathbb{R}$, the Eisenstein integers constitute a two-dimensional lattice A_2 spanned by the units 1 and ω. The points of A_2 are the vertices of a regular tessellation $\{3, 6\}$ of the Euclidean plane.
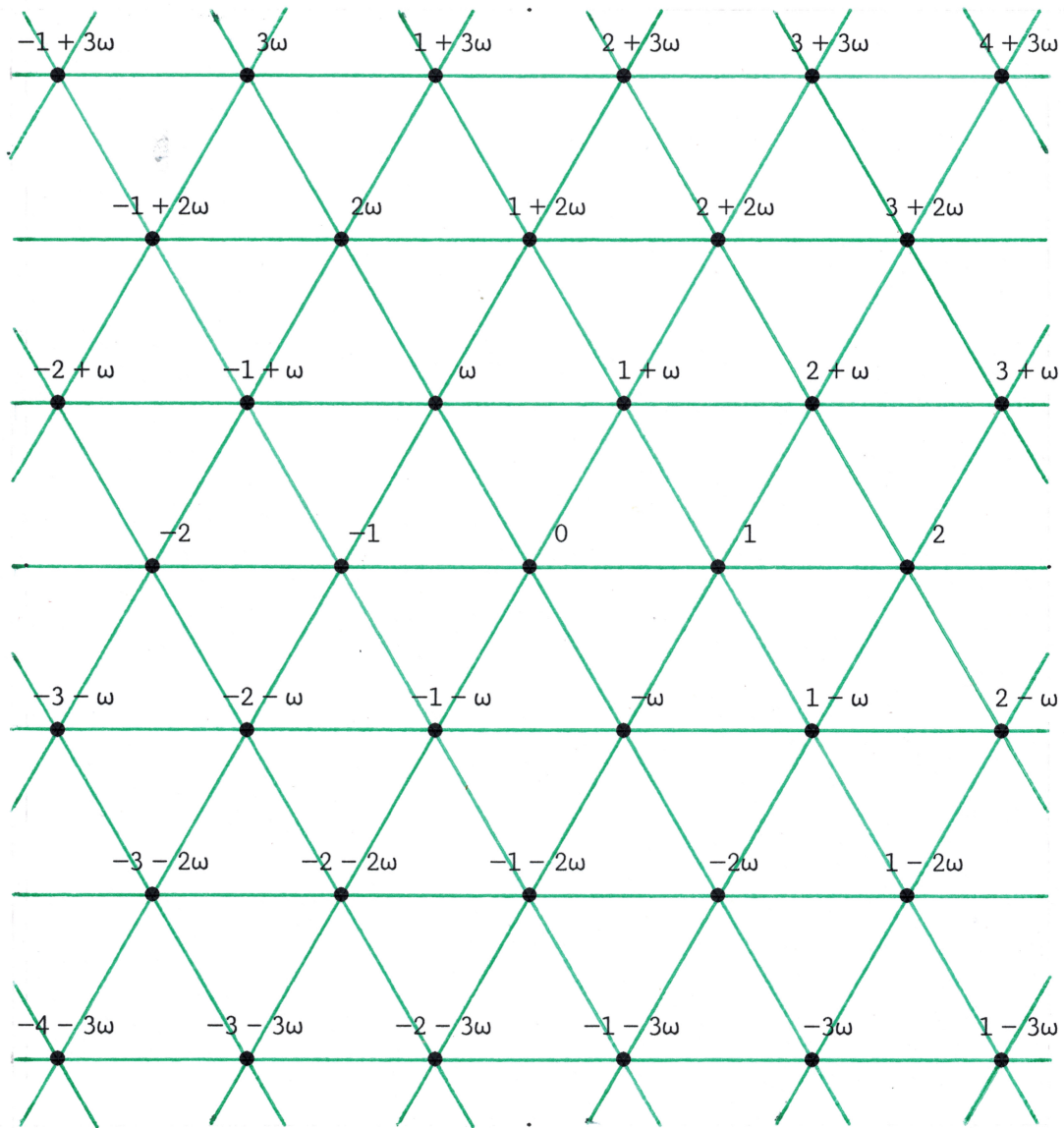
Fig. 2.   The Eisenstein integers

The Eisenstein Modular Group

Luigi Bianchi (1891, 1892) showed that if $\mathbb{D}$ is an imaginary quadratic integral domain, the group $\mathrm{PSL}_2(\mathbb{D})$ acts discontinuously on hyperbolic 3-space. Though Fricke and Klein applied this to the Gaussian integers $\mathbb{G} = \mathbb{Z}[i]$, the Eisenstein integers $\mathbb{E} = \mathbb{Z}[\omega]$ were generally ignored.

It was not until 1994 that Schulte and Weiss (cf. Monson & Weiss 1995, 1997) related the *Eisenstein modular group* $\mathrm{PSL}_2(\mathbb{E})$ to the honeycomb $\{3, 3, 6\}$, showing that $\mathrm{PSL}_2(\mathbb{E})$ is isomorphic to a subgroup of the rotation group $[3, 3, 6]^+$.

Coxeter Groups and Subgroups

The ring $\mathbb{Z}$ of rational integers can be identified with the points of a lattice C_1 spanned by the units ± 1, the vertices of a regular partition $\{\infty\}$. The modular group $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the rotation group $[3, \infty]^+$ of the regular hyperbolic tessellation $\{3, \infty\}$.

Similarly, the rings $\mathbb{G}$ and $\mathbb{E}$ of Gaussian and Eisenstein integers correspond to lattices C_2 and A_2, whose points are the vertices of the regular tessellations $\{4, 4\}$ and $\{3, 6\}$. As shown by Johnson and Weiss (1999), the respective modular groups are isomorphic to "ionic" subgroups of hyperbolic Coxeter groups:

$$\mathrm{PSL}_2(\mathbb{G}) \cong [3, 4, 1^+, 4]^+,$$
$$\mathrm{PSL}_2(\mathbb{E}) \cong [(3, 3)^+, 6, 1^+].$$

Quaternions and Hyperbolic 5-Space

Theodor Vahlen (1902) showed that homographies of inversive $(n-1)$-space I^{n-1} can be represented by linear fractional transformations over a Clifford algebra of dimension 2^{n-2} (cf. Ahlfors 1985). The cases $n = 2$, 3, and 4 correspond to the real field $\mathbb{R}$, the complex field $\mathbb{C}$, and the division ring $\mathbb{H}$ of *quaternions*.

John Wilker (1993) showed how a homography of I^4, or a direct isometry of H^5, is represented by a linear fractional transformation $\cdot\langle A \rangle$ determined by a 2×2 invertible matrix over $\mathbb{H}$. Thus the special projective pseudo-orthogonal group $P^+O_{5,1}$ is isomorphic to the projective special linear group $PSL_2(\mathbb{H})$.

The Hamilton Integers

William Rowan Hamilton, who discovered the quaternions in 1843, later investigated the ring $\mathbb{Z}[i, j]$ of quaternionic integers

$$g = g_0 + g_1 i + g_2 j + g_3 k,$$

where the g's are rational integers. Lipschitz (1886) devoted a whole book to this system, which I denote by ℍam and call the *Hamilton integers*. The ring ℍam has eight invertible elements, or units:

$$\pm 1, \pm i, \pm j, \pm k.$$

The Hurwitz Integers

In 1896 Adolf Hurwitz described the ring $\mathbb{Z}[u, v]$ of quaternionic integers

$$h = h_0 + h_1 u + h_2 v + h_3 w,$$

where the h's are rational integers and where

$$u = \tfrac{1}{2} - \tfrac{1}{2}i - \tfrac{1}{2}j + \tfrac{1}{2}k \quad \text{and} \quad v = \tfrac{1}{2} + \tfrac{1}{2}i - \tfrac{1}{2}j - \tfrac{1}{2}k,$$

with $w = (uv)^{-1}$. This system will be denoted by ℍur and called the *Hurwitz integers*. The ring ℍur has 24 units, consisting of the eight Hamilton units and 16 others of the type

$$\pm \tfrac{1}{2} \pm \tfrac{1}{2}i \pm \tfrac{1}{2}j \pm \tfrac{1}{2}k.$$

The Hybrid Integers

Still another system of quaternionic integers is the ring $\mathbb{Z}[\omega, j]$ of quaternions

$$e = e_0 + e_1\omega + e_2 j + e_3\omega j,$$

where the e's are rational integers and where

$$\omega = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{3}i \quad \text{and} \quad \omega j = -\tfrac{1}{2}j + \tfrac{1}{2}\sqrt{3}k.$$

This system will be denoted by $\mathbb{H}yb$ and called the *hybrid integers*. The ring $\mathbb{H}yb$ has 12 units:

$$\pm 1, \ \pm\omega, \ \pm\omega^2, \ \pm j, \ \pm\omega j, \ \pm\omega^2 j.$$

Lattices and Honeycombs

When $\mathbb{H}$ is taken as a four-dimensional vector space over $\mathbb{R}$, each of the rings of integral quaternions constitutes a four-dimensional lattice spanned by the units.

For the Hamilton integers points of the lattice C_4 are vertices of a regular honeycomb $\{4, 3, 3, 4\}$ of E^4.

For the Hurwitz integers points of the lattice D_4, which contains C_4 as a sublattice, are vertices of a regular honeycomb $\{3, 3, 4, 3\}$ of E^4.

For the hybrid integers points of the lattice $A_2 \oplus A_2$ are vertices of a uniform honeycomb $\{3, 6\} \times \{3, 6\}$ of E^4, the product of two regular tessellations of E^2.

Quaternionic Modular Groups

When the coefficients of a linear fractional transformation $\cdot\langle A\rangle$ are restricted to elements of a ring of integral quaternions, we have one of the *quaternionic modular groups* $\mathrm{PSL}_2(\mathbb{H}am)$, $\mathrm{PSL}_2(\mathbb{H}ur)$, or $\mathrm{PSL}_2(\mathbb{H}yb)$. These groups were investigated by Johnson and Weiss (1999). Each of them is a subgroup (or an extension of a subgroup) of a paracompact or hypercompact Coxeter group operating in H^5:

$$\mathrm{PSL}_2(\mathbb{H}am) \cong [3,\ 4,\ (3,\ 3)^\triangle,\ 4]^+,$$
$$\mathrm{PSL}_2(\mathbb{H}ur) \cong [(3,\ 3,\ 3)^+,\ 4,\ 3^+],$$
$$\mathrm{PSL}_2(\mathbb{H}yb) \cong 4[1^+,\ 6,\ (3,\ 3,\ 3,\ 3)^+,\ 6,\ 1^+].$$

The Octonions

The division algebra $\mathbb{O}$ of *octonions* was discovered by John Graves in 1843 and rediscovered by Arthur Cayley in 1845. It constitutes an eight-dimensional vector space over $\mathbb{R}$, and (like $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$) has a multiplicative norm. Whereas both $\mathbb{R}$ and $\mathbb{C}$ are fields and $\mathbb{H}$ is a skew-field, multiplication in $\mathbb{O}$ is neither commutative nor associative. The nonzero octonions form a multiplicative *Moufang loop* $\mathrm{GM}(\mathbb{O})$.

Basic Systems of Integers

The notion of *integer* can be applied to any normed division algebra. Leonard Dickson (1923) proposed criteria for a set of complex, quaternionic, or octonionic integers. Our theory requires a *basic system* of integers to have the following properties:

(1) the trace and the norm of each element are rational integers;

(2) the elements form a subring of $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$, with a set of units closed under multiplication;

(3) when $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$ is taken as a vector space over $\mathbb{R}$, the elements are the points of a two-, four-, or eight-dimensional lattice spanned by the units.

What Are the Basic Systems?

The only basic system of real integers is the ring $\mathbb{Z}$ of rational integers, with two units. The rings $\mathbb{G}$ and $\mathbb{E}$ of Gaussian and Eisenstein integers, the only domains of quadratic integers with both real and imaginary units (four for $\mathbb{G}$, six for $\mathbb{E}$), are the two basic systems of complex integers.

Using results of Du Val (1964), Johnson and Weiss (1999) showed that the units of a basic system of integral quaternions must form a binary dihedral group $2D_2$ or $2D_3$ or the binary tetrahedral group $2A_4$ and hence that the only basic systems are the rings $\mathbb{H}am$ (8 units), $\mathbb{H}yb$ (12 units), and $\mathbb{H}ur$ (24 units).

Integral Octonions (A)

Conway and Smith (2003) investigated rings of real, complex, quaternionic, and octonionic integers, which fall into four distinct families. There are just four basic systems of integral octonions (Johnson 2013; cf. Boddington & Rumynin 2007; Curtis 2007).

To the systems $\mathcal{G}^1 = \mathbb{Z}$ (2 units), $\mathcal{G}^2 = \mathbb{G}$ (4 units), and $\mathcal{G}^4 = \mathbb{H}am$ (8 units) we can add the system $\mathcal{G}^8 = \mathbb{O}cg$ of *Cayley–Graves integers* (or "Gravesian octaves") with 16 units spanning a lattice C_8, points of which are the vertices of a regular honeycomb $\{4, 3^6, 4\}$ of $\mathbb{E}^8$.

Integral Octonions (B)

Along with systems $\mathcal{E}^2 = \mathbb{E}$ (6 units) and $\mathcal{E}^4 = \mathbb{H}\text{yb}$ (12 units) we have the system $\mathcal{E}^8 = \mathbb{O}\text{ce}$ of *compound Eisenstein integers* (or "Eisensteinian octaves") with 24 units spanning a lattice $4A_2 = A_2 \oplus A_2 \oplus A_2 \oplus A_2$, points of which are the vertices of a uniform honeycomb $\{3, 6\}^4$, the rectangular product of four regular tessellations of E^2.

Two systems $\mathcal{H}^4 = \mathbb{H}\text{ur}$ (24 units) can be combined to produce the system $\mathcal{H}^8 = \mathbb{O}\text{ch}$ of *coupled Hurwitz integers* (or "Hurwitzian octaves") with 48 units that span a lattice $2D_4 = D_4 \oplus D_4$, points of which are the vertices of a uniform honeycomb $\{3, 3, 4, 3\}^2$, the rectangular product of two regular honeycombs of E^4.

Integral Octonions (C)

Dickson (1923) showed that certain sets of octonions having coordinates in $\mathbb{Z}$ or $\mathbb{Z} + \frac{1}{2}$ form a system of octonionic integers. In fact, he obtained three such systems. Coxeter (1946) found that there are in all *seven* of these systems, one corresponding to each of the seven unit octonions $e_1, \ldots, e_7$.

Each system $\mathcal{D}^8 = \mathbb{O}\text{cd}$ of *Coxeter–Dickson integers* (or "Dicksonian octaves") has 240 units spanning a lattice E_8, points of which are the vertices of Thorold Gosset's uniform honeycomb 5_{21}. The lattice E_8 contains C_8, $4A_2$, and $2D_4$ as sublattices, and the ring $\mathbb{O}\text{cd}$ contains $\mathbb{O}\text{cg}$, $\mathbb{O}\text{ce}$, and $\mathbb{O}\text{ch}$ as subrings.

Octonionic Modular Loops

Rings of octonionic integers cannot be used to define modular groups. First, the division algebra $\mathbb{O}$ is non-associative, satisfying only the weaker alternative laws $(aa)b = a(ab)$ and $(ab)b = a(bb)$. Second, the connection between linear fractional transformations and hyperbolic geometry runs through the family of Clifford algebras, including $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$ but not $\mathbb{O}$.

Though not associative, invertible 2×2 matrices over one of the basic systems of octonionic integers form a *special Moufang loop* $\mathrm{SM}_2(\mathbb{O}cg)$, $\mathrm{SM}_2(\mathbb{O}ce)$, $\mathrm{SM}_2(\mathbb{O}ch)$, or $\mathrm{SM}_2(\mathbb{O}cd)$. Identifying the matrices $\pm A$, we obtain an *octonionic modular loop* $\mathrm{PSM}_2(\mathbb{O}cg)$, $\mathrm{PSM}_2(\mathbb{O}ce)$, $\mathrm{PSM}_2(\mathbb{O}ch)$, or $\mathrm{PSM}_2(\mathbb{O}cd)$.

Summary

The ten basic systems of real, complex, quaternionic, or octonionic integers fall into four families:

$$\mathcal{G}^1 = \mathbb{Z}, \quad \mathcal{G}^2 = \mathbb{G}, \quad \mathcal{G}^4 = \mathbb{H}\text{am}, \quad \mathcal{G}^8 = \mathbb{O}\text{cg},$$
$$\mathcal{E}^2 = \mathbb{E}, \quad \mathcal{E}^4 = \mathbb{H}\text{yb}, \quad \mathcal{E}^8 = \mathbb{O}\text{ce},$$
$$\mathcal{H}^4 = \mathbb{H}\text{ur}, \quad \mathcal{H}^8 = \mathbb{O}\text{ch},$$
$$\mathcal{D}^8 = \mathbb{O}\text{cd}.$$

The elements of each basic system are the points of a lattice in E^1, E^2, E^4, or E^8. The real, complex, and quaternionic systems define modular groups related to Coxeter groups operating in H^2, H^3, or H^5. The four octonionic systems define modular loops.