Counting cubic fields

Differences between $n=2$ and $n=3$:

- For $n=2$, every quadratic field could be written as $\mathbb{Q}(\sqrt{D})$ for some D
- For $n=3$, there are cubic fields that cannot be expressed as $\mathbb{Q}(\sqrt[3]{a})$ for some a.

Example: $f(x) = x^3 + x^2 - 1$ if α is a root, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\sqrt[3]{a})$ for any a

$g(x) = x^3 + x^2 - 3x - 1$ if β a root of $g(x)$, then $\mathbb{Q}(\beta) \neq \mathbb{Q}(\sqrt[3]{b})$ for some b

(lmfdb.org)

If $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ $a_i \in \mathbb{Z}$ irreducible, and α satisfies $f(\alpha)=0$

$$\mathbb{Q}(\alpha) = \{ c_0 + c_1\alpha + c_2\alpha^2 \mid c_0, c_1, c_2 \in \mathbb{Q} \}$$
$$= \langle 1, \alpha, \alpha^2 \rangle_{\mathbb{Q}}$$

Algebraic Goal: come up w/ a replacement for the enumeration of quadratic fields by squarefree integers for cubic fields

(1) Side goals/hope/dreams: come up w/ a replacement for the parameter D that we bounded by X and let $X \to \infty$

Fact: Every number field has a unique ring of integers inside of it

If $K = \mathbb{Q}(\alpha)$ is a number field, then inside of K is set of all algebraic integers in K.

Def'n: An algebraic integer is a root of a monic integer coefficient polynomial.

Example: $x^2 - 5$ so $\sqrt{5}$ is algebraic integer

$\frac{\sqrt{5}}{7}$ is not an algebraic integer because $x^2 - \frac{5}{49}$ is not integer coefficient

and $49x^2 - 5$ is not monic

weird but true: $\frac{1+\sqrt{5}}{2}$ is the root of $x^2 - x - 1$

Ring of Integers

- they are rings (commutative, w/ identity)
- no zero divisors
- they are ~~free~~ $\mathbb{Z}$-modules (vector space structure but over $\mathbb{Z}$ instead of a field)
- Krull dimension 1

Strategy: Enumerate cubic rings of integers in order to enumerate cubic fields.

- employ that fact that such rings have a rank 3 (dim 3) $\mathbb{Z}$-module
- create a moduli space for all "nice" bases of cubic rings

nice basis $\longleftrightarrow v \in V$

What makes a basis nice?

① $\mathbb{Z}$ is a subset (submodule) of any rank 3 $\mathbb{Z}$-module so the first basis element can be taken to be 1

$$R = \langle 1, \omega, \theta \rangle_{\mathbb{Z}} = \{ z_1 + z_2\omega + z_3\theta \mid z_1, z_2, z_3 \in \mathbb{Z} \}$$

Since $\langle 1, \omega, \theta \rangle$ is a ring, we should be multiply elements
This means that $\omega^2 \in R$ and therefore should be expressible in terms of the basis. Same for θ^2 and $\omega\theta$

(2) In stead of assuming that

$$\omega\theta = d + e\omega + f\theta \qquad d, e, f \in \mathbb{Z}$$

we can translate ω and θ so that $e=0$ and $f=0$.

$$\omega^2 = a + b\omega + c\theta \qquad a, b, c \in \mathbb{Z}$$
$$\omega\theta = d \qquad d \in \mathbb{Z}$$
$$\theta^2 = g + h\omega + i\theta \qquad g, h, i \in \mathbb{Z}$$

$$\omega\theta \cdot \theta = \omega \cdot \theta^2$$
$$d \cdot \theta = \omega(g + h\omega + i\theta)$$
$$d \cdot \theta = g\omega + h\omega^2 + i\omega\theta$$
$$= g\omega + h(a + b\omega + c\theta) + id$$
$$d \cdot \theta = (ha + id) + (g + bh)\omega + ch\,\theta$$

$$\Rightarrow \; ha + id = 0$$
$$g + bh = 0$$
and $\underline{\underline{d = ch}}$

You can get formulas for a and g in terms of b, c, h, i

so we can talk about the multiplication structure on rank 3 $\mathbb{Z}$-modules in a nice basis using <u>4 integers</u>

$$\langle 1, \omega, \theta \rangle \xrightarrow{\gamma} \langle 1, \omega', \theta' \rangle \qquad Gl_2(\mathbb{Z}) = \gamma$$

How does $Gl_2(\mathbb{Z})$ act on b, c, h, i?

As if b, c, h, i were the coefficients of 2-variable degree 3 polynomial

$$f(x,y) = -cx^3 + bx^2y - ixy^2 + hy^3$$

$$\gamma f = f((x,y)\gamma)$$