

Bonus Lecture

Gauss composition: Relates BQFs $\longleftrightarrow$ ideals in $\mathcal{O}_K$,
 $K/\mathbb{Q}$ quadratic

Quadratic Ring: commutative ring that $\simeq \mathbb{Z}^2$ as a $\mathbb{Z}$ -module

E.g. $R \subseteq \mathcal{O}_K$, $K/\mathbb{Q}$ is quadratic

$D \in \mathbb{Z}$, $D \equiv 0, 1 \pmod{4}$, not a $\square$.

$$R_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$$

$$= \mathbb{Z}[t] / (t^2 - Dt + \frac{D^2-D}{4})$$

$\in \mathbb{Z} \text{ b/c } D \equiv 0, 1 \pmod{4}$.

Propⁿ: Suppose $K/\mathbb{Q}$ quad field ext, $R \subseteq K$ subring, w/ $R \simeq \mathbb{Z}^2$ as a $\mathbb{Z}$ -module. Then $R \simeq R_D$ for some D .

Rmk: This D is unique.

Pf: $R = \mathbb{Z} + \mathbb{Z}\tau$ b/c $(1, \tau)$ is a basis of $R \simeq \mathbb{Z}^2$ for some τ .

$$\tau^2 = -b\tau - c \quad \text{some integers } b, c$$

$$c = -b(-c \text{ some integer}) > c$$

$$\tau = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{for some choice of } \sqrt{}$$

$$D := \underline{b^2 - 4c}$$

$$\tau = \underbrace{\frac{-b + 4c - b^2}{2}} + \underbrace{\frac{b^2 - 4c + \sqrt{b^2 - 4c}}{2}}$$

$$= \in \mathbb{Z} \quad \left(\frac{D + \sqrt{D}}{2} \right) \Rightarrow \mathbb{Z} + \mathbb{Z}\tau$$

$$= \mathbb{Z} + \mathbb{Z}\tau_D,$$

$$\text{where } \tau_D = \frac{D + \sqrt{D}}{2}.$$

⑩

Suppose $I \subseteq R_D$ is an ideal, nonzero.

Set $N(I) = [R_D : I]$ (as abelian gps)

$I \subseteq R_D \cong \mathbb{Z}^2 \Rightarrow I$ is free so $I \cong \mathbb{Z}^2$

so I has a basis u, v .

Lemma: Suppose $I = \mathbb{Z}u \oplus \mathbb{Z}v$, $u = a + b\tau_D$,
 $v = c + d\tau_D$

then $N(I) = |ad - bc|$.

Pf: $\mathbb{Z}^2 = R_D \rightarrow R_D = \mathbb{Z}^2$

$I \mapsto u$

$\tau_D \mapsto v$

$n, \dots, 1, a, c, \dots, a, 1, \dots$

$$\tau_D \mapsto \vee$$

• M has matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \Rightarrow \det(M) = ad - bc$

• OTOH, $I = M \cdot \mathbb{Z}^2$ so $[\mathbb{Z}^2 : M\mathbb{Z}^2] = [R_D : I] = |\det(M)|$.

$$\Rightarrow N(I) = |ad - bc|$$

Define $N_{u,v}(I) = ad - bc$ (w/o absolute values)

$$\Rightarrow N(I) = [R_D : I] = \pm N_{u,v}(I)$$

Another piece of notation:

• $\sigma: K \rightarrow K$ unique nontrivial automorphism

• $N: K \rightarrow \mathbb{Q}$ norm, $N(\alpha) = \alpha \sigma(\alpha)$

If $\alpha = \beta + \gamma \tau_D$, $\beta, \gamma \in \mathbb{Q}$ then

$$\begin{aligned} N(\alpha) &= \left(\beta + \gamma \left(\frac{D + \sqrt{D}}{2} \right) \right) \left(\beta + \gamma \left(\frac{D - \sqrt{D}}{2} \right) \right) \\ &= \beta^2 + D\beta\gamma + \left(\frac{D^2 - D}{4} \right) \gamma^2 \end{aligned}$$

In particular, if $\beta, \gamma \in \mathbb{Z}$ then $N(\alpha) \in \mathbb{Z}$.
(so that $\alpha \in R_D$)

Lemma: If $I \subseteq R_D$ an ideal, $\alpha \in I$, then $N(I) \mid N(\alpha)$.

Pf: $\alpha R_D \subseteq I \subseteq R_D$

$$\Rightarrow \underbrace{[R_D : \sigma R_D]}_{=1} = [R_D : I][I : \sigma R_D]$$

$$\underline{|N(\sigma)|} = \underline{N(I) \cdot [I : \sigma R_D]} \quad (2)$$

Suppose now $I = \mathbb{Z}u + \mathbb{Z}v$ is an ideal of R_D .

$$\text{Set } f_{I,u,v}(x,y) = \frac{N(xu+yv)}{N_{u,v}(I)} \\ = Ax^2 + Bxy + Cy^2 \text{ where}$$

$$A = \frac{N(u)}{N_{u,v}(I)}, \quad B = \frac{N(u+v) - N(u) - N(v)}{N_{u,v}(I)}, \quad C = \frac{N(v)}{N_{u,v}(I)}$$

$$\text{If } x, y \in \mathbb{Q}, \quad \frac{N(xu+yv)}{N_{u,v}(I)} = Ax^2 + Bxy + Cy^2$$

$$f_{I,u,v}(x,y) = \frac{1}{N_{u,v}(I)} (xu+yv)(x\sigma(u)+y\sigma(v))$$

Claim: $f_{I,u,v}(x,y)$ is an integral BQF, i.e. $A, B, C \in \mathbb{Z}$.

Claim follows from the lemma.

How does $f_{I, u, v}(x, y)$ depend upon scaling I and how does it depend upon choice of basis u, v ?

Scaling: $I = \mathbb{Z}u + \mathbb{Z}v$, $\alpha \in \mathbb{R}_D$

$$\alpha I = \mathbb{Z}\alpha u + \mathbb{Z}\alpha v$$

$$f_{\alpha I, \alpha u, \alpha v}(x, y) = \frac{N(\alpha u x + \alpha v y)}{N_{\alpha u, \alpha v}(\alpha I)} = \frac{N(\alpha) N(ux + vy)}{N(\alpha) N_{u, v}(I)} = f_{I, u, v}(x, y).$$

Denominator: $u = a + b\tau_D$, $T_\alpha: \mathbb{R}_D \rightarrow \mathbb{R}_D$
 $v = c + d\tau_D$, $\beta \mapsto \alpha\beta$.

$$\text{In basis } 1, \tau_D, \quad \alpha u = T_\alpha \begin{pmatrix} a \\ b \end{pmatrix}, \quad \alpha v = T_\alpha \begin{pmatrix} c \\ d \end{pmatrix}$$

$$\Rightarrow N_{\alpha u, \alpha v}(\alpha I) = \det \left(T_\alpha \begin{pmatrix} a \\ b \end{pmatrix} \mid T_\alpha \begin{pmatrix} c \\ d \end{pmatrix} \right)$$

$$= \det \left(T_\alpha \begin{pmatrix} a & c \\ b & d \end{pmatrix} \right) = N(\alpha) N_{u, v}(I).$$

Change of Basis: $I = \mathbb{Z}u + \mathbb{Z}v = \mathbb{Z}u' + \mathbb{Z}v'$

$$f_1(x, y) = f_{I, u, v}(x, y), \quad f_2(x, y) = f_{I, u', v'}(x, y)$$

$I_{u,v}$ $-1, \tau, v$

• $\exists m \in GL_2(\mathbb{Z})$ s.t.

$$\begin{pmatrix} u \\ v \end{pmatrix} = m \begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} pu' + qv' \\ ru' + sv' \end{pmatrix}$$

$$m = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

• $r_u = (a, b)$ if $u = a + b\tau_D$ similarly for $r_{u'}, r_{v'}$

• $r_v = (c, d)$ if $v = c + d\tau_D$

Then $r_u = pr_{u'} + qr_{v'}$ $\Rightarrow \begin{pmatrix} r_u \\ r_v \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} r_{u'} \\ r_{v'} \end{pmatrix}$

$r_v = rr_{u'} + sr_{v'}$

$$\Rightarrow N_{u,v}(I) = \det(m) N_{u',v'}(I)$$

$$\begin{aligned} f_1(x, y) &= \frac{1}{N_{u,v}(I)} N((x, y) \begin{pmatrix} u \\ v \end{pmatrix}) \\ &= \frac{1}{\det(m) N_{u',v'}(I)} N((x, y) m \begin{pmatrix} u' \\ v' \end{pmatrix}) \\ &= \frac{1}{\det(m)} f_2((x, y) m) \end{aligned}$$

Define: $(m \circ f)(x, y) = \frac{1}{\det(m)} f((x, y) m)$

$$\frac{1}{\det(m)} \gamma((x, y)m)$$

Then $f_1 = m \circ f_2$.

Recall: $Cl(R_D) = \{ I \subseteq R_D \text{ nonzero ideals} \} / \sim$

where $I \sim J$ if $\alpha I = \beta J$ for some nonzero $\alpha, \beta \in R_D$.

Cor: $Cl(R_D) \longrightarrow (\text{Integral BQFs})$

$Cl_2(\mathbb{Z})$

$I \longmapsto Cl_2(\mathbb{Z}) \ni f_{I, u, v}(x, y)$

is well-defined.

THM (Gauss composition) This association lands in BQFs of discriminant D and is a bijection onto the $Cl_2(\mathbb{Z})$ orbits of BQFs of disc D .