Correction:

$[K/\mathbb{Q}] = n$

Proposition 3.2.1: (a) For any $\mathbb{Z}$-submodule $\Gamma \subset K$ of rank n with an ordered $\mathbb{Z}$-basis $(x_1, \ldots, x_n)$ the following value depends only on Γ:

$$\operatorname{disc}(\Gamma) := \operatorname{disc}(x_1, \ldots, x_n) \in \mathbb{Q}^\times.$$

(c) For any $\mathbb{Z}$-submodule $\Gamma \subset \mathcal{O}_K$ of rank n we have $\operatorname{disc}(\Gamma) \in \mathbb{Z} \smallsetminus \{0\}$.

$\Rightarrow \operatorname{disc}(\Gamma) = \det\big(\operatorname{tr}(x_i x_j)\big)_{i,j}$

Reminder:

Consider an integer $n \geqslant 1$, take a primitive n-th root of unity ζ and set $K := \mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$.

Proposition 3.6.3: If $n \geqslant 2$, then for any a coprime to n we have $\boxed{\frac{1-\zeta^a}{1-\zeta} \in \mathcal{O}_K^\times.}$ *(Cyclotomic units)*

Definition 3.6.4: The *n-th cyclotomic polynomial* Φ_n is the monic polynomial of degree $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ with the simple roots the primitive n^{th} root of unity.

$$\Phi_n(X) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^a)$$

Theorem 3.6.5: The polynomial Φ_n is an irreducible element of $\mathbb{Z}[X]$.

Jantzen-Schwermer: Algebra.

Theorem 3.6.6: The extension $K/\mathbb{Q}$ is finite galois of degree $\varphi(n)$ and there is a natural isomorphism $e\colon \operatorname{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ with the property

$$\forall \gamma \in \operatorname{Gal}(K/\mathbb{Q})\colon\ \gamma(\zeta) = \zeta^{e(\gamma)}.$$

cyclotomic character.

$\Phi_p(X) = 1 + X + \ldots + X^{p-1}$

$\Phi_p(Y+1)$ satisfies Eisenstein at p.

\ell

$d = [K/\mathbb{Q}] = \varphi(n)$
$= (\ell-1)\,\ell^{\nu-1}$

Theorem 3.6.7: If $n = \ell^\nu$ for a prime ℓ and an integer $\nu \geqslant 1$, then:

(a) We have $\Phi_{\ell^\nu}(X) = \sum_{i=0}^{\ell-1} X^{i\ell^{\nu-1}}$.

(b) The ideal $(1-\zeta)$ of $\mathcal{O}_K$ satisfies $(1-\zeta)^{\ell^{\nu-1}(\ell-1)} = (\ell)$.

(c) The ideal $(1-\zeta)$ is the unique prime ideal of $\mathcal{O}_K$ above $(\ell) \subset \mathbb{Z}$ and has residue field $\mathcal{O}_K/(1-\zeta) \cong \mathbb{F}_\ell$.

(d) $\mathcal{O}_K = \mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(\Phi_{\ell^\nu})$.

(e) $\mathrm{disc}(\mathcal{O}_K) = \pm \ell^{\ell^{\nu-1}(\nu\ell-\nu-1)}$.

Proof: (a) $\Phi_{\ell^\nu}(X) = \dfrac{X^{\ell^\nu}-1}{X^{\ell^{\nu-1}}-1} = \sum_{i=0}^{\ell-1} X^{i\cdot\ell^{\nu-1}}$.

(b) $\Phi_{\ell^\nu}(1) \overset{(a)}{=} \sum_{i=0}^{\ell-1} 1 = \ell$

$$\overset{\|}{\prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}} (1-\zeta^a) \in \mathcal{O}_K^\times \cdot \prod_a (1-\zeta) = \mathcal{O}_K^\times \cdot (1-\zeta)^d$$

(c) $\mathrm{Nm}((\ell)) \overset{\text{def}}{=} [\mathcal{O}_K : \mathcal{O}_K \ell] = \ell^d$ because $\mathcal{O}_K \cong \mathbb{Z}^d$ as $\mathbb{Z}$-module.

$\| (b)$

$\mathrm{Nm}((1-\zeta)^d) = \mathrm{Nm}((1-\zeta))^d \underset{\text{def}}{=} [\mathcal{O}_K : (1-\zeta)]^d$

$\Rightarrow |\mathcal{O}_K/(1-\zeta)| = [\mathcal{O}_K : (1-\zeta)] = \ell$

$\Rightarrow \mathcal{O}_K/(1-\zeta)$ is a ring of order ℓ $\Rightarrow \cong \mathbb{F}_\ell$

$\Rightarrow (1-\zeta)$ is maximal $\Rightarrow$ prime

By (a) $\ell \in (1-\zeta) \Rightarrow (1-\zeta)$ above $\ell\mathbb{Z}$.

For any prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathfrak{p} \cap \mathbb{Z} = \ell\mathbb{Z}$ we have $(1-\zeta)^d \cdot \mathcal{O}_K = \ell \cdot \mathcal{O}_K \subset \mathfrak{p} \Rightarrow (1-\zeta)\mathcal{O}_K \subset \mathfrak{p}$. $\Rightarrow$ "="

Claim 1: $\forall k \geq 1: \quad \mathcal{O}_K = \mathbb{Z}[\zeta] + (1-\zeta)^k \cdot \mathcal{O}_K$.

Proof: $k=1$: $\mathcal{O}_K = \mathbb{Z} + (1-\zeta)\cdot \mathcal{O}_K = \mathbb{Z}[\zeta] + (1-\zeta)\,\mathcal{O}_K$ ✓

$k \rightsquigarrow k+1$: $\mathcal{O}_K = \mathbb{Z} + (1-\zeta)\,\mathcal{O}_K = \mathbb{Z} + (1-\zeta)\cdot\left[\mathbb{Z}[\zeta] + (1-\zeta)^k \cdot \mathcal{O}_K\right] = \mathbb{Z}[\zeta] + (1-\zeta)^{k+1}\,\mathcal{O}_K$. qed

Hence: $\forall k \geq 1: \quad \mathcal{O}_K = \mathbb{Z}[\zeta] + \ell^k \cdot \mathcal{O}_K$.

because $\ell^k \cdot \mathcal{O}_K = (1-\zeta)^{dk} \cdot \mathcal{O}_K$.

Hence $[\mathcal{O}_K : \mathbb{Z}[\zeta]]$ is prime to ℓ.

Claim 2: $\mathrm{disc}(1, \zeta, \ldots, \zeta^{d-1}) = \pm \ell^N$ for an integer $N \geq 1$.

Proof: $\Sigma := \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$$\Rightarrow \mathrm{disc}(\Phi_n) = \prod_{\substack{\sigma,\tau \in \Sigma \\ \sigma \neq \tau \\ \text{up to permutation}}} (\sigma(\zeta) - \tau(\zeta))^2 = \pm \prod_{\substack{\sigma \neq \tau \\ \sigma,\tau \in \Sigma}} (\sigma(\zeta) - \tau(\zeta)) \overset{\tau = \sigma\rho}{=} \pm \prod_{\substack{\sigma,\rho \in \Sigma \\ \rho \neq id}} (\sigma(\zeta) - \sigma(\rho(\zeta)))$$

$$= \pm \prod_{\substack{a,b \in (\mathbb{Z}/n\mathbb{Z})^\times \\ b \neq 1}} (\zeta^a - \zeta^{ab}) = \pm \prod_{\substack{a,b \\ b \neq 1}} \zeta^a \cdot (1 - \zeta^{a(1-b)}) \in \mathcal{O}_K^\times \cdot \prod_{\substack{a,b \\ b\neq 1}} (1-\zeta^{a(1-b)})$$

$$\in \mathcal{O}_K^\times \cdot \prod_{b \neq 1} (1 - \zeta^{1-b})^d$$

$\zeta^{(1-b)}$ is a primitive root of unity of order ℓ^r for some $1 \leq r \leq \nu$.

$\Rightarrow \dfrac{1-\zeta^{a(1-b)}}{1-\zeta^{1-b}}$ is a unit in $\mathcal{O}_{\mathbb{Q}(\zeta^{1-b})} \subset \mathcal{O}_K$.

(b) for ℓ^μ instead ℓ^ν. $\Downarrow$ $(1-\zeta^{1-b})^{(\ell-1)\cdot\ell^{\nu-1}} \in \mathcal{O}_K^\times \cdot \ell$.

$\quad \in \mathcal{O}_K^\times \cdot \prod_{b\neq 1}$ (primitive powers of ℓ)

$d = (\ell-1)\ell^{\nu-1}$

$\Rightarrow \underbrace{\operatorname{disc}(\Phi_n)}_{\in \mathbb{Z}\setminus\{0\}} = u\cdot \underbrace{\ell^N}_{\in \mathbb{Z}\setminus\{0\}}$ for some $N \geq 1$ and $u \in \mathcal{O}_K^\times$. $\Rightarrow u \in \mathbb{Z}^\times = \{\pm 1\}$.

(d) Prop. 1.7.5 $\Rightarrow$ $\mathcal{O}_K \subset \dfrac{1}{\operatorname{disc}(\mathbb{Z}[\zeta])}\cdot \mathbb{Z}[\zeta] = \dfrac{1}{\ell^N}\cdot\mathbb{Z}[\zeta]$

Combine with Claim 1 $\Rightarrow$ $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

$$\underbrace{\mathbb{Z}[X]/(\Phi_n)}_{\text{free } \mathbb{Z}\text{-module of rank } d = \deg(\Phi_n)} \xrightarrow{\sim} \underbrace{\mathbb{Z}[\zeta]}_{\text{also}} = \mathcal{O}_K.$$

(e) $\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(\mathbb{Z}[\zeta]) = \pm \ell^N$.

qed.

Theorem 3.6.8: For arbitrary n we have:

(a) $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

(b) The discriminant $\operatorname{disc}(\mathcal{O}_K) \in \mathbb{Z}$ is divisible precisely by the primes dividing n.

Proof: $n=1$: $\zeta = 1$, $\mathcal{O}_K = \mathbb{Z}$, $\operatorname{disc}(\mathbb{Z}) = 1$.

$n = \ell^\nu$ for ℓ prime, $\nu > 0$: Thm. 3.6.7.

$n = m \cdot m'$ for $m, m' > 1$ coprime. $\Rightarrow$ Chinese remainder thm:

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}.$$

$$\Rightarrow \mu_n \cong \mu_m \times \mu_{m'}$$

and $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times$.

$$\begin{tikzcd}
& \mathbb{Q}(\mu_n) \arrow[dl, dash, "(\mathbb{Z}/m'\mathbb{Z})^\times"'] \arrow[dd, dash, "(\mathbb{Z}/n\mathbb{Z})^\times"] \arrow[dr, dash, "(\mathbb{Z}/m\mathbb{Z})^\times"] & \\
\mathbb{Q}(\mu_m) \arrow[dr, dash, "(\mathbb{Z}/m\mathbb{Z})^\times"'] & & \mathbb{Q}(\mu_{m'}) \arrow[dl, dash, "(\mathbb{Z}/m'\mathbb{Z})^\times"] \\
& \mathbb{Q} &
\end{tikzcd}$$

So $\mathbb{Q}(\mu_m)$ and $\mathbb{Q}(\mu_{m'})$ are linearly disjoint over $\mathbb{Q}$ and $\mathbb{Q}(\mu_m, \mu_{m'}) = \mathbb{Q}(\mu_n)$.

1.8.3 $\Rightarrow$ $\mathcal{O}_{\mathbb{Q}(\mu_n)} \xleftarrow{\sim} \mathcal{O}_{\mathbb{Q}(\mu_m)} \otimes_{\mathbb{Z}} \mathcal{O}_{\mathbb{Q}(\mu_{m'})}$

$\Rightarrow$ (a) & (b).

qed.

3.7 Quadratic Reciprocity

Fix an odd prime ℓ and set $K := \mathbb{Q}(\mu_\ell)$ and $\zeta := e^{\frac{2\pi i}{\ell}}$.

Definition 3.7.1: The *Legendre symbol* of an integer a with respect to ℓ is

$$\boxed{\left(\frac{a}{\ell}\right)} := \begin{cases} 0 & \text{if } a \equiv 0 \bmod (\ell), \\ +1 & \text{if } a \equiv b^2 \bmod (\ell) \text{ for some } b \in \mathbb{Z} \smallsetminus \ell\mathbb{Z}, \\ -1 & \text{otherwise.} \end{cases}$$

In the first two cases a is called a *quadratic residue*, otherwise a *quadratic non-residue modulo* (ℓ).

Proposition 3.7.2: For any integers a, b we have:

(a) $\left(\frac{a}{\ell}\right) = \left(\frac{b}{\ell}\right)$ whenever $a \equiv b \bmod (\ell)$.

(b) $\left(\frac{a}{\ell}\right) \equiv a^{\frac{\ell-1}{2}} \bmod (\ell)$.

(c) $\left(\frac{ab}{\ell}\right) = \left(\frac{a}{\ell}\right)\left(\frac{b}{\ell}\right)$.

(d) $\boxed{\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}}$.

Proof: (a) ✓

(b) true if $\ell \mid a$; otherwise: $\mathbb{F}_\ell^\times \cong \mathbb{Z}/(\ell-1)\mathbb{Z}$, $[a] \longleftrightarrow [\alpha]$

squares $\cong 2\mathbb{Z}/(\ell-1)\mathbb{Z}$

so $[a]$ is a square iff $2 \mid \alpha$ iff $[\frac{\ell-1}{2}\cdot\alpha] = [0]$

iff $[a^{\frac{\ell-1}{2}}] = [1]$.

otherwise $[\frac{\ell-1}{2}\cdot\alpha] = [\frac{\ell-1}{2}] \Rightarrow [a^{\frac{\ell-1}{2}}] = [-1]$.

(c) $\underbrace{\left(\frac{ab}{\ell}\right)}_{\in\{\pm1,0\}} \overset{(b)}{\equiv} (ab)^{\frac{\ell-1}{2}} = a^{\frac{\ell-1}{2}}\cdot b^{\frac{\ell-1}{2}} \overset{(b)}{\equiv} \underbrace{\left(\frac{a}{\ell}\right)\cdot\left(\frac{b}{\ell}\right)}_{\in\{\pm1,0\}} \bmod (\ell)$.

$\ell \geq 3$. $\Big\} \Rightarrow$ equality.

(d) $\left(\frac{-1}{\ell}\right) \overset{(b)}{\equiv} (-1)^{\frac{\ell-1}{2}} \Rightarrow$ equality.

qed

$ab^{-1} = c$

$\iff a = bc$

Definition 3.7.3: The *Gauss sum* associated to the prime ℓ is $\boxed{g_\ell := \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) \cdot \zeta^a.}$

Proposition 3.7.4: The Gauss sum satisfies $\boxed{g_\ell^2 = \ell^* := (-1)^{\frac{\ell-1}{2}} \ell.}$

Proof: $\boxed{g_\ell^2} = \sum_{a,b\in\mathbb{F}_\ell^\times} \left(\frac{a}{\ell}\right)\cdot\zeta^a \cdot \underbrace{\left(\frac{b}{\ell}\right)}_{\left(\frac{b^{-1}}{\ell}\right)}\cdot\zeta^b = \sum_{a,b\in\mathbb{F}_\ell^\times} \left(\frac{ab^{-1}}{\ell}\right)\cdot\zeta^{a+b} = \sum_{b,c\in\mathbb{F}_\ell} \left(\frac{c}{\ell}\right)\cdot\zeta^{bc+b}$

$= \sum_{c\in\mathbb{F}_\ell^\times} \left(\frac{c}{\ell}\right)\cdot \underbrace{\left[\sum_{b\in\mathbb{F}_\ell^\times} (\zeta^{c+1})^b\right]}$

$\zeta^{c+1} = \begin{cases} 1 & \text{if } c=-1 \text{ in } \mathbb{F}_\ell^\times \\ \text{primitive } \ell^{\text{th}} \text{ root of unity otherwise} \end{cases}.$

$= \sum_{c\in\mathbb{F}_\ell^\times} \left(\frac{c}{\ell}\right)\cdot \begin{cases} \ell-1 & \text{if } c=-1 \\ -1 & \text{else} \end{cases}$

$= \begin{cases} \sum 1^b = \ell-1 & \text{if } c=-1 \\ \sum_{a\in\mathbb{F}_\ell^\times} \zeta^a = -1 & \text{if } c\neq -1. \end{cases}$

because $\sum_{i=0}^{\ell-1} \zeta^i = 0.$

$= \ell\cdot\left(\frac{-1}{\ell}\right) - \underbrace{\sum_{c\in\mathbb{F}_\ell^\times}\left(\frac{c}{\ell}\right)}_{=0} = \boxed{\ell\cdot\left(\frac{-1}{\ell}\right)}.$

Proposition 3.7.5: The unique subfield of K of degree 2 over $\mathbb{Q}$ is $K' := \mathbb{Q}(\sqrt{\ell^*}\,)$.

Proof: $\mathbb{Q}(g_\ell) \subset K$

$\mathbb{Q}(\sqrt{\ell^*}) \neq \mathbb{Q}$

$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_\ell^\times \cong \mathbb{Z}/(\ell-1)\mathbb{Z}.$

$\cup$

$2\mathbb{Z}/(\ell-1)\mathbb{Z}$ = unique subgroup of index 2.