II. The Kronecker-Weber thm for quadratic fields and the QRL

Let $K|\mathbb{Q}$ be a quadratic extension. Can assume $K=\mathbb{Q}(\sqrt{D})$, D square free

Let's prove:

· Kronecker Weber's thm. for quadratic fields.

13 **Prop**: $S := \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\zeta^a$ the Gauss sum for $\left(\frac{*}{p}\right)$, ζ p-th primitive root of 1 $\Rightarrow$

$S^2 = \left(\frac{-1}{p}\right)p$. (last corollary).

Def: $p^* := \left(\frac{-1}{p}\right)p = \begin{cases} p & \text{if } p\equiv 1 \bmod 4 \\ -p & \text{if } p\equiv 3 \bmod 4 \end{cases}$. Notice $p^* \equiv 1 \bmod 4$.

odd

14 **Cor**: p odd prime $\Rightarrow$ $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. ← until here.

· Now, $i^4=1$ primitive 4-th root $\Rightarrow$ $\mathbb{Q}(i)$ is already cyclotomic.

Moreover: $\mathbb{Q}(\sqrt{-p^*}) \subseteq \mathbb{Q}(i).\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(i).\mathbb{Q}(\zeta_p)$ compositum of cyclotomic is cyclotomic $\Rightarrow$ $\mathbb{Q}(\sqrt{\pm p}) \subseteq \mathbb{Q}(\zeta_{4p})$.

· Now, $\zeta_8 = \frac{1+i}{\sqrt{2}}$. Since $i\in\mathbb{Q}(\zeta_8)$ $\Rightarrow$ $\sqrt{2},\sqrt{-2}\in\mathbb{Q}(\zeta_8)$ $\Rightarrow$ $\mathbb{Q}(\sqrt{\pm 2})\subseteq\mathbb{Q}(\zeta_8)$

Finally, if $D=\pm p_1\cdots p_r$ $\Rightarrow$ $\mathbb{Q}(\sqrt{D}) \subseteq \cancel{\mathbb{Q}(i)\mathbb{Q}(\zeta_8)\mathbb{Q}(\zeta_{p_1})\cdots\mathbb{Q}(\zeta_{p_r})} \subseteq$

$\subseteq \mathbb{Q}(i,\sqrt{2},\sqrt{p_1^*},\dots,\sqrt{p_r^*}) =$

$= \mathbb{Q}(i)\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{p_1^*})\cdots\mathbb{Q}(\sqrt{p_r^*}) \subseteq \mathbb{Q}(\zeta_{8p_1\cdots p_r})$.

Obs: Maybe, indeed, if sign $=+$ and D odd, $\mathbb{Q}(\sqrt{D})\subseteq\mathbb{Q}(\zeta_{\underbrace{4p_1\cdots p_r}_{4|D|}})$.

15 **Cor**: D square free $\Rightarrow$ $\mathbb{Q}(\sqrt{D})\subseteq\mathbb{Q}(\zeta_{4|D|})$. ← time permitting.

• <u>The</u> <u>quadratic reciprocity law</u> (Gauss: "Mathematics is the Queen of Science. Number Theory is the queen's crown. The QRL is the jewel of the crown!")

Consider Gauss sums in odd characteristic ℓ. All results apply as for complex ones (check it).

in particular $S := \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^a$, $\zeta \in \overline{\mathbb{F}}_\ell$, $\zeta^p = 1$ primitive $\Rightarrow$

$$S^2 = \left(\frac{-1}{p}\right) \cdot p$$

(16) <u>Lemma</u>: $S^{\ell-1} = \left(\frac{\ell}{p}\right)$.

<u>Proof</u>: $$\underset{\substack{\uparrow \\ \text{charact. } \ell}}{S^\ell} = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^{a\ell} = \sum_a \left(\frac{a\overset{\text{in } \mathbb{F}_p}{\overset{\swarrow}{\ell^{-1}}}}{p}\right) \zeta^a = \left(\frac{\ell^{-1}}{p}\right) \sum_a \left(\frac{a}{p}\right) \zeta^a = \underbrace{\left(\frac{\ell^{-1}}{p}\right)}_{= \left(\frac{\ell}{p}\right)} S \Rightarrow$$

$$S^{\ell-1} = \left(\frac{\ell}{p}\right) \#$$

(17) <u>Thm</u> (the QRL) p, ℓ prime, odd $\Rightarrow$ $\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right) (-1)^{\frac{p-1}{2} \frac{\ell-1}{2}}$.

<u>Proof</u>: $\ell = p \Rightarrow$ trivial, othw:

Given $a \in \mathbb{Z}$, $z \in \overline{\mathbb{F}}_\ell$ s.t. $z^2 = a \Rightarrow \left(\frac{a}{\ell}\right) = z^{\ell-1}$. Indeed: $z^{\ell-1} = z^{2\frac{\ell-1}{2}} = a^{\frac{\ell-1}{2}} = \left(\frac{a}{\ell}\right)$. $\Rightarrow$

$$\left(\frac{\left(\frac{-1}{p}\right) p}{\ell}\right) \underset{\substack{\uparrow \\ S^2 = \left(\frac{-1}{p}\right) \cdot p}}{=} S^{\ell-1} = \left(\frac{\ell}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}} \cdot p}{\ell}\right) = \underbrace{\left(\frac{(-1)^{\frac{p-1}{2}}}{\ell}\right)}_{(-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}}} \left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}} \left(\frac{p}{\ell}\right) \#.$$

<u>e.g.</u> $$\left(\frac{34569284994927}{1602961}\right) = \left(\frac{1188715}{1602961}\right) = \left(\frac{5 \cdot 11 \cdot 21613}{1602961}\right) = \left(\frac{5}{1602961}\right) \cdot \left(\frac{11}{1602961}\right) \cdot$$

$$\left(\frac{21613}{1602961}\right) \underset{\substack{\uparrow \\ 1602961 \equiv 1 \bmod 4 \Rightarrow (-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}} = 1}}{=} \left(\frac{1602961}{5}\right)\left(\frac{1602961}{11}\right)\left(\frac{1602961}{21613}\right) = \underbrace{\left(\frac{1}{5}\right)}_{1} \underbrace{\left(\frac{8}{11}\right)}_{-1} \left(\frac{3599}{21613}\right) = -\left(\frac{59}{21613}\right)\left(\frac{61}{21613}\right)$$

$$\underset{\substack{\uparrow \\ 21613 \equiv 1 \, (4)}}{=} \left(\frac{19}{59}\right)\left(\frac{19}{61}\right) = \left(\frac{59}{19}\right)\left(\frac{61}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{1}{19}\right) = \left(\frac{2}{19}\right) = -1.$$

Legendre symbols computation.

· **Def** (Jacobi symbol) → Helps simplify

P odd, $P \in \mathbb{Z}$. $P = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \Rightarrow \left(\frac{a}{P}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{n_i}$.

18 **Prop**: 1) $(a,P) > 1 \Rightarrow \left(\frac{a}{P}\right) = 0$.

2) $(a,P) = 1 \Rightarrow \left(\frac{a}{P}\right) = \pm 1$

3) P_1, P_2, P odd, $a_1, a_2, a \in \mathbb{Z} \Rightarrow \left(\frac{a}{P_1P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$, $\left(\frac{a_1a_2}{P}\right) = \left(\frac{a_1}{P}\right)\left(\frac{a_2}{P}\right)$

4) $a \equiv a' \pmod{P} \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{a'}{P}\right)$.

19 **Prop**: $\left(\frac{P_1}{P_2}\right) = (-1)^{\frac{P_1-1}{2}\frac{P_2-1}{2}} \left(\frac{P_2}{P_1}\right)$ (QRL).

⇑

Lemma: $P := p_1^{n_1} \cdots p_r^{n_r}$, $\varepsilon(P) := \frac{P-1}{2} \Rightarrow (-1)^{\varepsilon(P)} = \prod_{i=1}^{r} (-1)^{\varepsilon(p_i) \cdot n_i}$

20 **Cor**: $\omega(P) := \frac{P^2-1}{8} \Rightarrow \left(\frac{-1}{P}\right) = (-1)^{\varepsilon(P)}$, $\left(\frac{2}{P}\right) = (-1)^{\omega(P)}$.

· **The Kronecker symbol** (allows to describe the decomposition law of primes in quadratic fields).

Obs: $|\mathbb{Z}/4\mathbb{Z})^*| = 2 \Rightarrow$ there are only 2 Dirichlet chars mod 4, χ_1 and $(-1)^{\varepsilon(*)}$, primitive modulo 4. $(-1)^{\varepsilon(1)} = 1$, $(-1)^{\varepsilon(3)} = -1$.

$|(\mathbb{Z}/8\mathbb{Z})^*| = 4 \Rightarrow$ there are only 4 Dirichlet chars mod 8. Two of them are those induced from χ_1, $(-1)^{\varepsilon(*)}$ mod 4.

The others are also quadratic as $(\mathbb{Z}/8\mathbb{Z})^*$ has exp 2: $3^2 = 1$, $5^2 = 1$, $7^2 = 1$.

$\chi_3 = (-1)^{\omega(*)}$, $\chi_4 = (-1)^{\omega(*) + \varepsilon(*)}$.

$\left(\frac{*}{p}\right)$ is the only quadratic character of conductor p.

Let $d := l_1 \dots l_r$, l_i odd prime, might also be $d:=1$.

$\Rightarrow \left(\frac{*}{d}\right) = \prod_i \left(\frac{*}{l_i}\right)$ is a Dirichlet character modulo d.

$(-1)^{\varepsilon(*)\cdot\varepsilon(d)}\left(\frac{*}{d}\right)$ is a Dir. character modulo $4d$.

Def: (Kronecker characters): $\chi_d := (-1)^{\varepsilon(d)\varepsilon(*)}\left(\frac{*}{d}\right)$ d-th Kronecker char. $\to$ mod $4d$

$\chi_{2d} := (-1)^{\omega(*)}\chi_d \to$ mod $8d$

$\chi_{-d} := (-1)^{\varepsilon(*)}\chi_d \to$ mod $4d$

$\chi_{-2d} := (-1)^{\varepsilon(*)}(-1)^{\omega(*)}\chi_d. \to$ mod $8d$.

21) Prop: D square-free $\Rightarrow$ χ_D is the unique quadratic Dirichlet character mod $4|D|$ s.t. $\forall$ p odd, $(p,D)=1$

$\chi_D(p) = \left(\frac{D}{p}\right)$. (exercise).
says how p factors in $\mathbb{Q}(\sqrt{D})$.

22) Prop: D square free, d its odd positive part $\Rightarrow f_{\chi_D} = 4|D|$ except if $D\equiv 1$ mod 4 in which case is d. (exercise)

23) Thm: Let χ be a quadratic Dirichlet character (primitive). Then, $\exists D$ square free s.t. $\chi = \chi_D$, defined modulo its conductor.

The proof uses:

24) Lem. 1: Let f be f_χ for some quadratic Dirichlet. Assume f odd $\Rightarrow$ f square-free.

25) Lem. 2: $f = f_\chi$, χ quadratic $\Rightarrow$ f is free of 2^4.

26) Lem 3: $f \neq 2f'$, f' odd. Indeed: f' odd $\Rightarrow$ $G(2f') \cong G(f)$.

IV. Ramification

IV.1. Trace and norm

In ANT, we define, for a number field K, the trace $Tr_{K|\mathbb{Q}}$ and $N_{K|\mathbb{Q}}$, norm. It's possible to generalise this definition to an extension $L|K$ of number fields. One has to use the set $\{\sigma : L \hookrightarrow L^{alg} \mid \sigma_{|K} = Id\}$ of K-embeddings of L. Task for the student:

27 Prop: $\forall \theta \in L$, $\varphi_\theta : L \to L$, $x \mapsto \theta x$, $\varphi_\theta \in End_K(L)$. Choose $\{b_1, \dots, b_n\} = B$ be a K-basis of L, $A_\theta = M(\varphi_\theta, B) \Rightarrow$ The $\det(A_\theta)$ and $Tr(A_\theta)$ do not depend on B. Moreover:

a) $N_{L|K}(\theta) := \det(A_\theta)$

b) $T_{L|K}(\theta) = Tr(A_\theta)$.

28 Prop: $\forall \theta, \theta_1, \theta_2 \in L$, $\alpha \in K$, it holds:

a) $T_{L|K}(\theta_1 + \theta_2) = T_{L|K}(\theta_1) + T_{L|K}(\theta_2)$

b) $T_{L|K}(\alpha\theta) = \alpha T_{L|K}(\theta)$

c) $T_{L|K}(\alpha) = n\alpha$, $n = [L:K]$.

d) $N_{L|K}(\theta_1\theta_2) = N_{L|K}(\theta_1) N_{L|K}(\theta_2)$

e) $N_{L|K}(\alpha\theta) = \alpha^n N_{L|K}(\theta)$.

29 Prop: $K \subseteq K' \subseteq L$ extension of number fields $\Rightarrow$ $T_{L|K}(\theta) = T_{K'|K}(T_{L|K'}(\theta))$ and $N_{L|K}(\theta) = N_{K'|K}(N_{L|K'}(\theta))$.

III.2 Ramification and inertia indices

Let $L|K$ be an extension of number fields. In an analogous manner as in ANT, $\forall \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, $\mathfrak{P}_i \in \mathrm{Spec}(\mathcal{O}_L)$, $1 \leq i \leq g$.

<u>Def</u> : Ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $e_i = e(\mathfrak{P}_i|\mathfrak{p}) = e_{\mathfrak{P}_i|\mathfrak{p}}$.

Notice that $\mathcal{O}_K/\mathfrak{p} \leq \mathcal{O}_L/\mathfrak{p}$ is a finite field extension of $\deg \leq n$. $=[L:K]$

<u>Def</u> : Inertia degree (or residual degree) is $f_i = f(\mathfrak{P}_i|\mathfrak{p}) = f_{\mathfrak{P}_i|\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.

30 <u>Prop</u> : In an analogous manner as in ANT: $\sum_{i=1}^{g} e_i f_i = n$.

• The Galois case :

Suppose L/K Galois of degree n. In particular, $G := \mathrm{Gal}(L/K)$ has order n.

31 <u>Prop</u> : G acts transitively on the set of primes of $\mathcal{O}_L$ over $\mathfrak{p}$.

<u>Proof</u> : exercise. Hint : check that $\forall i \in \{1, \dots, g\}$, $\forall \sigma \in G$, $\sigma(\mathfrak{P}_i)$ is a prime of $\mathcal{O}_L$ over $\mathfrak{p}$ and that $\{\sigma(\mathfrak{P}_1) \mid \sigma \in G\} = \{\mathfrak{P}_i \ 1 \leq i \leq g\}$.

$\Downarrow$

32 <u>Cor</u> : L/K Galois $\Rightarrow$ all the ramification indices are equal, say, to e. All the inertia degrees are equal, say, to f. Hence $\boxed{n = g \cdot e \cdot f}$.

<u>Proof</u>: exercise.

• Decomposition and inertia group

<u>Def</u> : Let $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ over $\mathfrak{p}$. The isotropy subgroup of G $D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ is called decomposition group of $\mathfrak{P}|\mathfrak{p}$.

We have a map
$$\begin{aligned} \varphi : D(\mathfrak{P}|\mathfrak{p}) &\to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \mid \mathcal{O}_K/\mathfrak{p}) \\ \sigma &\longmapsto \varphi(\sigma) = \bar{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P} \\ & \qquad x + \mathfrak{P} \longmapsto x^\sigma + \mathfrak{P}. \end{aligned}$$

<u>Def</u> : $\mathrm{Ker}(\varphi) = \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \text{ s.t. } \forall x \in \mathcal{O}_L,\ x^\sigma - x \in \mathfrak{P}\}$ is called inertia group of $\mathfrak{P}|\mathfrak{p}$, denoted $I(\mathfrak{P}|\mathfrak{p})$.

(33)

Thm: The extension $\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}$ is Galois and φ is surjective.

Proof: a) The extension is Galois. Enough to check normality:
$\forall \beta\in\mathcal{O}_L$, $f_\beta(x) := \prod_{\sigma\in G}(x-\sigma(\beta)) = \mathrm{Irr}(\beta,K)^{[L:K(\beta)]}$ (check!). Now, $\bar{f}_\beta(x)$ modulo $\mathfrak{P}$ decomposes in linear factors over $\mathcal{O}_L/\mathfrak{P}$ and $\mathrm{Irr}(\beta+\mathfrak{P},\mathcal{O}_K/\mathfrak{p})$ divides it $\Rightarrow$ $\mathrm{Irr}(\beta+\mathfrak{P},\mathcal{O}_K/\mathfrak{p})$ decomposes in linear factors over $\mathcal{O}_L/\mathfrak{P}$.
$\Rightarrow$ All the conjugates over $\mathcal{O}_K/\mathfrak{p}$ of all the ~~conjugates~~ elements of $\mathcal{O}_L/\mathfrak{P}$ are in $\mathcal{O}_L/\mathfrak{P}$ $\Rightarrow$ the extension is normal.

b) Take $\bar{\beta}\in\mathcal{O}_L/\mathfrak{P}$ primitive element. $\forall\sigma\in \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}\,|\,\mathcal{O}_K/\mathfrak{p})$, σ is determined by its image on $\bar{\beta}$. Take $\beta\in\mathcal{O}_L$ s.t. $\beta\equiv\bar{\beta}$ mod $\mathfrak{P}$ and $\beta\in\sigma^{-1}(\mathfrak{P})$ $\forall\sigma\in G\setminus D(\mathfrak{P}|\mathfrak{p})$ i.e. $\beta\equiv\bar{\beta} \bmod \mathfrak{P}$, $\beta\equiv 0 \bmod \sigma^{-1}(\mathfrak{P})$ $\forall\sigma\notin D(\mathfrak{P}|\mathfrak{p})$. ← CRT.

$f(x):=\prod_{\sigma\in G}(x-\sigma(\beta))$. The non-zero roots modulo $\mathfrak{P}$ are $\sigma(\beta)+\mathfrak{P}$, $\sigma\in D(\mathfrak{P}|\mathfrak{p})$
$\Rightarrow$ all the conjugates of $\bar{\beta}+\mathfrak{P}$ are reduction mod $\mathfrak{P}$ of conjugates ~~of~~ $\sigma(\beta)$ ~~for~~ of β $\Rightarrow$ given $\tau\in\mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}\,|\,\mathcal{O}_K/\mathfrak{p})$ $\exists\sigma\in D(\mathfrak{P}|\mathfrak{p})$ s.t. $\tau=\bar{\sigma}$.

Denote $p:=\mathrm{char}(\mathcal{O}_K/\mathfrak{p})$ s.t. $q=p^r=|\mathcal{O}_K/\mathfrak{p}|$, $\overline{\mathcal{O}_K/\mathfrak{p}}=\mathbb{F}_q$.

We have:
$$\boxed{1\to I(\mathfrak{P}|\mathfrak{p})\to D(\mathfrak{P}|\mathfrak{p})\to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}\,|\,\mathcal{O}_K/\mathfrak{p}) \overset{\text{Galois}}{=} \mathrm{Gal}(\mathbb{F}_{q^f}\,|\,\mathbb{F}_q)\to 1}$$

Obs: Let $\mathfrak{P}'$ be another prime over $\mathfrak{p}$ $\Rightarrow$ $\exists\sigma\in G \mid \mathfrak{P}'=\sigma(\mathfrak{P})$ $\Rightarrow$ $D(\mathfrak{P}'|\mathfrak{p})=\sigma^{-1}D(\mathfrak{P}|\mathfrak{p})\sigma$.

$\sigma_1,\sigma_2\in G$, $\sigma_1\sim\sigma_2$ iff $\sigma_1\sigma_2^{-1}\in D(\mathfrak{P}|\mathfrak{p})$ $\Leftrightarrow$ $\sigma_1\sigma_2^{-1}(\mathfrak{P})=\mathfrak{P}$ $\Leftrightarrow$ $\sigma_1(\mathfrak{P})=\sigma_2(\mathfrak{P})$.

$\Rightarrow |G/D(\mathfrak{P}|\mathfrak{p})| = g = \dfrac{n}{D(\mathfrak{P}|\mathfrak{p})} = \dfrac{g.e.f}{D(\mathfrak{P}|\mathfrak{p})}$ $\Rightarrow$ $|D(\mathfrak{P}|\mathfrak{p})|=ef$ $\Rightarrow$ $|I(\mathfrak{P}|\mathfrak{p})|=e$. #

III.3 the discriminant

<u>Def</u>: Let $B = \{b_1, \dots, b_n\}$ be a K-basis of L. $\Delta[B] = \det(T_{L|K}(b_i b_j)) \in K$.

<u>obs</u>: $\cdot\ \Delta[B'] = C^2 \Delta[B]$, $C = M(B, B')$.

$\cdot$ If $B \subseteq \mathcal{O}_L \Rightarrow \Delta[B] \subseteq \mathcal{O}_K$.

<u>Def</u>: $\Delta := \Delta[\mathcal{O}_L | \mathcal{O}_K] = \langle \Delta[B] \mid B \subseteq \mathcal{O}_L$ K-basis of $L \rangle_{\mathcal{O}_K}$.

$\Rightarrow \Delta = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, $\mathfrak{p}_i \in \mathrm{Spec}(\mathcal{O}_K)$.

<u>Thm</u>: Let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$. $\mathfrak{p}$ ramifies in $\mathcal{O}_L \Leftrightarrow \mathfrak{p} \mid \Delta$.

for $K = \mathbb{Q}$, see "Discriminants and ramified primes" (Keith Conrad):

https://kconrad.math.uconn.edu/blurbs/gradnumthy/disc.pdf.