(DA 342-343)

Gauss's notation

L5 #1 Disq. Arith. 1801. Gauss born in 1777

n prime. $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1$ the equation of interest.

Let r be a root (fixed).

$r, r^2, r^3, \ldots$

Ω - set of all roots

" " "

$[1]\ [2]\ [3]$ $\qquad [\lambda]$ for r^λ

(so $[\lambda]\cdot[\mu] = [\lambda+\mu]$

$[\lambda]^\nu = [\lambda\nu]$

Ex: $[0] + [\lambda] + \cdots + [(n-1)\lambda] = \begin{cases} 0 & n \nmid \lambda \\ n & n \mid \lambda. \end{cases}$

Let g be a primitive root mod n (generator of $(\mathbb{Z}/n)^\times$). $g^{\hat{}} = g$

$\{1, g, \ldots g^{n-2}\} = \{1, 2, \ldots, n-1\}$ mod n.

so for any $\lambda \in \mathbb{Z}\setminus n\mathbb{Z}$, $\{[\lambda], [\lambda g], [\lambda g^2], \ldots [\lambda g^{n-1}]\} = \Omega$.

Periods Fix a factorization $n-1 = e\cdot f$

Let $h = g^e$, and consider ~~[1], [h], [h]~~

$(f, \lambda) := [\lambda] + [\lambda h] + \cdots + [\lambda h^{f-1}]$ over the (sum) elements of the coset

$\left(= r^\lambda + r^{\lambda g^e} + r^{\lambda g^{2e}} + \cdots + r^{\lambda g^{(f-1)e}} \right)$

$= \sum_{k=0}^{f-1} r^{\lambda \cdot g^{ek}}$

Example: $n = 19$. $g = 2 \in (\mathbb{Z}/19)^\times$

$(6, 1) = [1] + [g^3] + [g^6] + [g^9] + [g^{12}] + [g^{15}]$

(f, λ)

so $19 - 1 = \underset{e}{3}\cdot\underset{f}{6}$ $\quad = [1] + [2^3] + [2^6] + \cdots + [2^{15}]$

$= [1] + [7] + [8] + [11] + [12] + [18]$

0		1
1	3	2
2	2	4
3	4	8
4	8	16
5	16	13
6		7
7		14
8		9
9		18
10		17
11		15
12		11
13		3
14		6
15		12
16		5
17		10
18		1

DA 344-345

Exercise • $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2) = \cdots$ $\quad (\lambda h^f = \lambda g^{ef} = \lambda g^{n-1} = \lambda)$

• $(n-1, 1)$ = sum of all elements of $\Omega = -1$

• periods decompose into sums of smaller length, e.g.

$(n-1, 1) = (f, \lambda) + (f, \lambda g) + \cdots + (f, \lambda g^{e-1})$ for any $ef = n-1$, $n \nmid \lambda$.

$(RHS \sum_{j=0}^{e-1} \sum_{k=0}^{f-1} r^{\lambda g^j \cdot g^{ek}} = \sum_{j,k} r^{\lambda g^{ek+j}}$ ← get $0, 1, \ldots, (f-1)+(e-1)$ $\because ef-1 = n-1-1$

eg. $n = 19$. $-1 = (18, 1) = (6,1) + (6,2) + (6,4)$ $\quad = \sum_{i=0}^{n-2} r^{\lambda \cdot g^i}$)

(*) Products of periods of same length. Take λ, μ not div. by n. $ef = n-1$.

$(f, \lambda)\cdot(f, \mu) = (f, \lambda+\mu) + (f, \lambda h + \mu) + (f, \lambda h^2 + \mu) + \cdots + (f, \lambda h^{f-1} + \mu)$

DA354.

Example: From now on take $\boxed{n=17}$. $17-1=2^4$.

Fix $g=3$ is a prim. root $\langle 3\rangle = (\mathbb{Z}/17)^\times$.

$n-1 = e\cdot f = 2\cdot 8$, $h = g^e = 9$

$$(8,1)\cdot(8,3) = (8,4)+(8,12)+(8,16)+(8,1)+(8,2)+(8,11)+(8,7)+(8,5)$$

(under: $\lambda+\mu$, $\lambda+\mu$, h^2+3 (= 84 = 13+3×16), h^3+3 (= 15+3), e^4+3 (= 19), h^5+3 (= 11), h^6+3 (= 7), h^7+3 (= 5); see table)

g	g^2	h
3	9	
4	10	
5	13	h^2
6	5	
7	15	h^3
8	11	
9	16	h^4
10	14	
11	8	h^5
12	7	
13	4	h^6
14	12	
15	2	h^7
16	6	
1	1	

Which of these give different $\langle h\rangle$-cosets? $(8,g^k)$ & $(8,g^\ell)$ agree when $k\equiv \ell \bmod 2$.

So $(8,1)\cdot(8,3) = \cancel{(8,1)}$

$$= (8,g^{12})+(8,g^{13})+(8,g^8)+(8,g^0)+(8,g^{14})+(8,g^7)+(8,g^{11})+(8,g^5)$$

$$= 4(8,1)+4\cdot(8,3=g^1) = -4.$$

Conclusion: $(8,1)$ and $(8,3)$ are the two roots of

$$X^2+X-4=0 \qquad \left(\frac{-1\pm\sqrt{17}}{2}\right)$$

(which is which root depends on the choice of r.

~~estimate~~ say you fix $r=\cos\left(\frac{2\pi}{17}\right)+i\sin\left(\frac{2\pi}{17}\right)$, $\mathbb{Q}\subset\mathbb{Q}(\sqrt{17})\subset\mathbb{Q}\left(e^{\frac{2\pi i}{17}}\right)$

$(8,1)=\sum_{k=0}^{7} e^{\frac{2\pi i}{17}(9^k)} > 0$ (ex), so $(8,1)=\frac{-1+\sqrt{17}}{2}$.

Next step: decompose $(8,1)$ into two shorter periods (lying in a larger subfield)

$$(8,1) = (4,1)+(4,9)$$

$$\sum_{k=0}^{7} r^{g^{2k}} = \sum_{k=0}^{3} r^{g^{4k}} + r^{g^{4k+2}}$$

Then compute

$$(4,1)\cdot(4,9) = (4,\underset{g^3}{10})+(4,\underset{g^5}{5})+(4,\underset{g^{10}}{8})+(4,\underset{g^4}{13})$$

(5: $h+\mu$, $22=5$; 8: h^2+9, $25=8$; 13: h^3+9, 13)

new $e=4$, new $h=g^4=13$

Recall $(4,g^a)=\sum_{k=0}^{3} r^{g^{a+4k}}$, so above sum covers $a\equiv 3,1,2,6 \bmod 4$ each exactly once

$$\Rightarrow (4,1)\cdot(4,9) = \sum_{i=0}^{15} r^{g^i} = -1$$

$\Rightarrow$ $(4,1)$ and $(4,9)$ are roots of

$$X^2-(8,1)X-1=0 \quad \text{ie}$$

$$\frac{-1+\sqrt{17}}{2}\pm\sqrt{(8,1)^2+4} = \frac{-1+\sqrt{17}}{2}\pm\sqrt{8-\frac{-1+\sqrt{17}}{2}} = \frac{1}{4}\left(-1+\sqrt{17}\pm\sqrt{34-2\sqrt{17}}\right)$$

and again can check which roots which

$$= \frac{1}{4}\left(-1+\sqrt{17}\pm 2\sqrt{\frac{17-\sqrt{17}}{2}}\right)$$

L5 #3

$= 4-(8,1)$ not needed

$$(8,1)^2 = (8,2)+(8,10)+(8,14)+(8,16)+(8,0)+(8,9)+(8,5)+(8,13)$$

$h=g^2=9$; $(8,10)$: $k=1$; $(8,14)$: $k^2=1$; $(8,16)$: $k^3=1$; $(8,0)$: $k^4=1$, $17=0$; $(8,9)$: $k^5=1$

Now our tower is $\mathbb{Q} \subset \mathbb{Q}((8,1)) \subset \mathbb{Q}((4,1))$

$\mathbb{Q}((8,1)) = \mathbb{Q}(\sqrt{17})$; $\mathbb{Q}((4,1)) = \mathbb{Q}((4,9))$; Exercise: $\mathbb{Q}((4,1)) = \mathbb{Q}(\sqrt{34-2\sqrt{17}})$

(note $\mathbb{Q}((4,1))=\mathbb{Q}((4,9)) \Rightarrow \mathbb{Q}((8,1)) \subset \mathbb{Q}((4,1))$)

} general result is DA 346. (each is a rational poly in the other, of degree $\le$ "e-1" $= 3$

And so on:

$$(4,1) = (2,1)+(2,13)$$

$$\sum_{k=0}^{3} r^{g^{4k}} = \sum_{k=0}^{1} r^{g^{8k}} + r^{g^{8k+4}} \qquad (g^4=13)$$

and $(2,1)\cdot(2,13) = (2,14)+(2,12)$ ($h+13$; $29=12$)

now $e=8, f=2$, $h=g^e=16 (=-1)$

$$= \sum_{k=0}^{1} \left(r^{14g^{8k}} + r^{12g^{8k}}\right)$$

$12\langle h\rangle$, $14\langle h\rangle$ get mod 17 the classes $5,12$; $3,14$

$$= \sum_{k=0}^{3} r^{g^{4k+1}} = (4,3) = g, g^5, g^{13}, g^9$$

So $(2,1)$ and $(2,13)$ are roots of

$r+r^{-1}$ $=$ $2\cos\left(\frac{2\pi}{17}\right)$; $r^{13}+r^{-13}$ $=$ $2\cos\left(\frac{8\pi}{17}\right)$

$$\boxed{X^2-(4,1)X+(4,3)=0}$$

Now we again observe that $(4,3)\in\mathbb{Q}((4,1))$ /exercise

and an explicit version gives a quadratic $\in \mathbb{Q}((4,1))[x]$

$\mathbb{Q}$ (2) $\subset \mathbb{Q}((8,1))$ (2) $\subset \mathbb{Q}((4,1))$ (2) $\subset \mathbb{Q}((2,1)) = 2\cos\left(\frac{2\pi}{17}\right)$ (2) $\subset \mathbb{Q}\left(e^{2\pi i/17}\right)$

again by checking $\mathbb{Q}((2,1)) = \mathbb{Q}((2,13))$

$(2,1)$ and $(2,13)$ are $\frac{(4,1) \pm \sqrt{(4,1)^2-4\cdot(4,3)}}{2} = \frac{(4,1)\pm 4}{2}$ ...

persevere to the precise expression: exercise)

Here the poly is clean: $X^2-(r+r^{-1})X+1$, $(2,1)$

Normal! $\mathbb{H} \triangleleft \mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/17})/\mathbb{Q}\right) \simeq (\mathbb{Z}/17)^\times$

$\mathbb{H}$: the order 4 subgroup; $\sigma \longmapsto \kappa(\sigma)$, $\sigma(r) = r^{\kappa(\sigma)}$

From modern point of view, $\mathbb{Q}((4,1))/\mathbb{Q}$ is Galois $= \mathbb{Q}(e^{2\pi i/17})^{\mathbb{H}}$

$r \xrightarrow{\sigma_{13}} r^{13}$ generates $\mathbb{H}$. $\quad \langle g^4\rangle = \langle 13\rangle$

$\sigma((4,1)) = \sigma\left(\sum_{k=0}^{3} r^{g^{4k}}\right) = \sigma\left(r+r^{13}+r^{16}+r^4\right)$

Now take σ_3 $\quad \kappa(\sigma_3) = g = \langle 3\rangle$

$\sigma_3((4,1)) = \sigma_3\left(r+r^{13}+r^{16}+r^4\right)$

$= (4,3)$

$(\sigma_3^2=\sigma_9)((4,1)) = (4,9)$

σ_9 fixes $(8,1)$.

$\sigma_3((4,1)) = (4,3)$

L5 #4 $\forall$ primes n, the equation for $(\frac{n-1}{2},1)$ & $(\frac{n-1}{2},g)$ can be analyzed

$e=2$, $f=\frac{n-1}{2}$

Again $(\frac{n-1}{2},1)+(\frac{n-1}{2},g)=-1$ $\quad\sum[g^{2k}]$ $\quad\sum[g^{2k+1}]$

DA356

and $\quad\sum$ squares $\quad\sum$ non-squares.

$$(\tfrac{n-1}{2},1)\cdot(\tfrac{n-1}{2},g)=\sum_{k=0}^{\frac{n-1}{2}}(\tfrac{n-1}{2},\ \text{non-squares}+g^{2k+1})$$

$$=\alpha(\tfrac{n-1}{2},0)+\beta(\tfrac{n-1}{2},1)+\gamma(\tfrac{n-1}{2},g)\qquad\text{(gather like terms)}$$

$\alpha=\begin{cases}0 & \text{if } -1 \text{ is a square}\\ 1 & \text{if } -1 \text{ is a non-square}\end{cases}$ some $\beta,\gamma\in\mathbb{Z}_{\geq 0}$ where moreover $\alpha+\beta+\gamma=\frac{n-1}{2}$

(A little) More interestingly, $\beta=\gamma$ (DA350) (general result) : replace r by r^g : this swaps $(\frac{n-1}{2},1)$ & $(\frac{n-1}{2},g)$

so $\beta(\frac{n-1}{2},1)+\gamma(\frac{n-1}{2},g)=\beta(\frac{n-1}{2},g)+\beta(\frac{n-1}{2},1)$

$(\beta-\gamma)((\frac{n-1}{2},1)-(\frac{n-1}{2},g))=0\Rightarrow\beta=\gamma$ (if the other $=$, we'd have $-\frac{1}{2}=(\frac{n-1}{2},1)=(\frac{n-1}{2},5)$, $\frac{1}{4}=\alpha(\frac{n-1}{2},0)+(\beta+\gamma)(-\frac{1}{2})\in\frac{1}{2}\mathbb{Z}$. $\Rightarrow\Leftarrow$)

$\sum r^{g^{2k}}$ sub r for r, get $r^g\cdot g^{2k}$

$(\frac{n-1}{2},0)=\sum g^{0\cdot g^{2k}}=\frac{n-1}{2}$

Case 1) -1 a square. Then $\alpha=0$, $\beta=\gamma=\frac{n-1}{4}$, and the equation is $X^2+X-\frac{n-1}{4}=0$, so $(\frac{n-1}{2},g)$ & $(\frac{n-1}{2},1)$ are

$$\frac{-1\pm\sqrt{1+4(\frac{n-1}{4})}}{2}=\boxed{-\frac{1}{2}\pm\frac{\sqrt{n}}{2}}$$

Cor: since $\beta,\gamma\in\mathbb{Z}$, $n\equiv 1 \bmod 4$ ($\Rightarrow n\equiv 3 \bmod 4$)

Case 2) -1 not a square. Then $\alpha=1$, $\frac{n-1}{2}=1+\beta+\gamma$, so $\beta=\gamma=\frac{n-3}{4}$, and the eqtn is

$$X^2+X+\underbrace{\left(\frac{n-1}{2}+\frac{n-3}{4}(-1)\right)}_{\frac{n+1}{4}}\quad\text{w/ roots}\quad\frac{-1\pm\sqrt{1-(n+1)}}{2}=\boxed{-\frac{1}{2}\pm\frac{\sqrt{-n}}{2}}$$

Cor: $(\frac{n-1}{2},1)-(\frac{n-1}{2},g)=\begin{cases}\pm\sqrt{n} & n\equiv 1 \bmod 4\\ \pm\sqrt{-n} & n\equiv 3 \bmod 4\end{cases}$ Also $\mathbb{Q}(\sqrt{(-1)^{\frac{n-1}{2}}\cdot n})\subset\mathbb{Q}(\zeta^{2\pi i/4})$

This difference is what we call the Gauss sum associated to the Legendre symbol

$$G=G((\tfrac{\cdot}{n}))=\sum_{x\in\mathbb{Z}/n}(\tfrac{x}{n})\cdot e^{\frac{2\pi i x}{n}}$$

Gauss later (1805) proved the sign is $+$ when we take $r=e^{2\pi i/n}$ (or $e^{2\pi i\cdot\text{squares}/n}$), $-$ otherwise

The fact that $G^2=(-1)^{\frac{n-1}{2}}\cdot n$ leads to a quick proof of QR.

Let $p\neq q$ be odd primes. $G=G((\frac{\cdot}{p}))$, so $G^2=(-1)^{\frac{p-1}{2}}\cdot p$

Then $G^{q-1}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot p^{\frac{q-1}{2}}$ Consider this equation in $\mathbb{Z}/q\subset\mathbb{Z}[S_p]/(q)$

Get $G^q\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot(\frac{p}{q})\cdot G \bmod q\mathbb{Z}[S_p]$

But $G^q=\left(\sum_{x\in\mathbb{Z}/p}(\frac{x}{p})S_p^x\right)^q\overset{\text{mod } q\mathbb{Z}[S_p]}{\equiv}\sum_x'(\frac{x}{p})S_p^{qx}=\sum_y(\frac{q^{-1}y}{p})\cdot S_p^y=(\frac{q^{-1}}{p})\cdot G$

$=(\frac{q}{p})\cdot G$

so mod $q\mathbb{Z}[S_p]$, $(\frac{q}{p})\cdot G\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot(\frac{p}{q})\cdot G \pmod q$, hence $(\frac{q}{p})\equiv(\frac{p}{q})\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \bmod q$

(e.s. multiply by G and use $p\neq q$)

L5 #5 Since both sides are integers, the congruence in $\mathbb{Z}[\zeta_p]$ forces same $\equiv$ in $\mathbb{Z}$, ($\mathbb{Z} \cap q\cdot\mathbb{Z}[\zeta_p] \overset{\text{Ex!}}{=} q\mathbb{Z}$), and then since $q>2$ & both sides are ± 1 we get equality in $\mathbb{Z}$: $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. ☐

Gauss gave 2 pfs of QR using his results on Gauss sums & saw them as a path toward cubic & quartic rec. (he formulated & laid groundwork – complete proofs by Eisenstein)

The other thread leading to Galois – Lagrange & his resolvents ... 1770.

Consider a cubic $f(x)=0$, $f\in\mathbb{Q}[x]$, with roots a,b,c, $\zeta = e^{2\pi i/3}$
Set $t_1 = a+\zeta b+\zeta^2 c$ & t_2 – t_6 the analogues with a,b,c permuted.

Let $R_f(x) = \prod_{i=1}^{6}(x-t_i)$, the resolvent (sextic)

The coeffs of R_f are symmetric in the t_i's, hence symmetric in a,b,c, and so (Newton) they can be expressed as $\mathbb{Q}$-polynomials in coeff. of f i.e. we know $R_f \in \mathbb{Q}[x]$ w/o knowing a,b,c.

(quadratic analog: quad=0=1, roots a,b; $t_1 = a-b$, $t_2 = b-a$; $R(x) = (x-(a-b))(x-(b-a)) = x^2 - (a-b)^2$; $a^2-2ab+b^2 = (a+b)^2-4ab$ (the discriminant of f))

Key observation: $R_f(x)$ is quadratic in x^3

Pf: Order the t_i's as follows: $t_1 = a+\zeta b+\zeta^2 c$ (a.k.a. t_1)

$t_2 = \zeta t_1 = c+a\zeta+b\zeta^2$

$t_3 = \zeta t_2 = b+c\zeta+a\zeta^2$

$t_4 = \dfrac{b+a\zeta+c\zeta^2}{a+c\zeta+b\zeta^2}$ $\quad t_5 = \zeta t_4 \quad t_6 = \zeta t_5$.

Then $(X-t_1)(X-t_2)(X-t_3) = (X-t_1)(X-\zeta t_1)(X-\zeta^2 t_1) = X^3 - t_1^3$

and $R_f(x) = (x^3-t_1^3)(x^3-t_4^3) = x^6 - (t_1^3+t_4^3)X + t_1^3 t_4^3$

↖ we know these values: $u+v$ = known, $u-v$ = known

so we can solve a quadratic to determine t_1^3, t_4^3 and then taking cube roots of each, we obtain the 6 solutions to $R_f(x)=0$.

Let t be any one of these 6 solutions, and reorder the roots a,b,c so that $t = a+b\zeta+c\zeta^2$.

Now, $a = \dfrac{(a+b+c)+(a+b\zeta+c\zeta^2)+(a+b\zeta^2+c\zeta)}{3} = \frac{1}{3}\left((a+b+c)+t_1+t_4\right)$

and likewise $b = \frac{1}{3}\left[a+b+c+\zeta^2 t_1+\zeta t_4\right]$ $\quad c = \frac{1}{3}\left[a+b+c+\zeta t_1+\zeta^2 t_4\right]$

so if we know t_1, t_4 we win. We know the unordered pair $\{t_1^3, t_4^3\}$, so there is an ambiguity to resolve to get a,b,c. However, for any solution t of $R_f(t)=0$ $\exists$ some reordering of a,b,c as above. The quantity $(a+b\zeta+c\zeta^2)(a+\zeta^2 b+\zeta c) = w$ is symmetric in a,b,c, hence known and ind. of the ordering. The roots of f are then

Ross 2024 L1 #1 — intro waffle.

QR: p odd prime. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, and for $q \neq p$ another odd prime, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

- Euler criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$ $\forall a \in \mathbb{Z}$, immediately deals w/ $\left(\frac{-1}{p}\right)$ (using p odd).

~~§ Proof via Gauss sums. Idea: given $p \neq q$,~~

Basic move: Leave $\mathbb{Q}$. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid f(\alpha) = 0 \text{ for some } f(x) \in \mathbb{Q}[x]\}$ (algebraic numbers) ← countably infinite (ex.)

Let $\overline{\mathbb{Z}} = \{\alpha \in \overline{\mathbb{Q}} \mid \exists \text{ monic } f(x) \in \mathbb{Z}[x] \text{ s.t. } f(\alpha) = 0\}$ (alg. integers).

Lemma ① $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Pf: $\supseteq$ clear. Let $\frac{a}{b} \in \mathbb{Q} \cap \overline{\mathbb{Z}}$ with $a, b \in \mathbb{Z}$, $(a,b) = 1$. Let $f \in \mathbb{Z}[x]$ be monic s.t. $f\left(\frac{a}{b}\right) = 0$. $\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_1 \cdot \frac{a}{b} + a_0 = 0$, $a_i \in \mathbb{Z}$. Multiply by b^n, get $b^n \mid a^n$, hence (since $(a,b)=1$) $b \mid a$, i.e. $\frac{a}{b} \in \mathbb{Z}$. ✓

~~Prop~~ Lemma ② $\overline{\mathbb{Z}}$ is a subring of $\mathbb{C}$. $\overline{\mathbb{Q}}$ is the field of fractions of $\overline{\mathbb{Z}}$.

Pf: Use following (easily generalizable) algebraic lemma. Notation: for any $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$, let $\mathbb{Z}[\alpha_1, \ldots, \alpha_r] = \{f(\alpha_1, \ldots, \alpha_r) \mid f(x) \in \mathbb{Z}[x_1, x_2, \ldots, x_r]\} \subset \mathbb{C}$. This is obviously a subring of $\mathbb{C}$.

Example: • $\alpha_1 = \pi$. $\mathbb{Z}[\pi]$ is, since π is transcendental, there all $\sum_{i=0}^{N} a_i \pi^i$ ($N \in \mathbb{Z}$, $a_i \in \mathbb{Z}$) and all $\sum a_i \pi^i$ are all distinct. The abelian group $\mathbb{Z}[\pi]$ is not generated as ab-gp. by finitely many elts (sens: $1, \pi, \pi^2, \ldots$)

• $\alpha_1 = e^{2\pi i/5}$ $\left(= \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}\right)$. $\mathbb{Z}[\alpha_1] = \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_1^2 + \mathbb{Z}\alpha_1^3 + \mathbb{Z}\alpha_1^4$ is finitely-generated as ab.

Sub-lemma ③: (i) If $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Z}}$, then $\mathbb{Z}[\alpha_1, \ldots, \alpha_r]$ is finitely gen'd. (the additive group)

(ii) Let $\alpha \in \mathbb{C}$. Then $\alpha \in \overline{\mathbb{Z}}$ iff $\exists$ additive subgp. $A \subset \mathbb{C}$ that is finitely-generated and such that $\alpha \cdot A \subset A$.

Pf: (i) Let $f_i(x) \in \mathbb{Z}[x]$ be monic s.t. $f_i(\alpha_i) = 0$. Set $d_i = \deg f_i$, so $\alpha_i^{d_i} =$ sum of integers $b_k \cdot \alpha_i^k$ for $0 \leq k < d_i$. Inductive arg easily shows $\forall n \geq d_i$, $\alpha_i^n \in \mathbb{Z} + \mathbb{Z}\alpha_i + \mathbb{Z}\alpha_i^2 + \cdots + \mathbb{Z}\alpha_i^{d_i - 1}$ →

[L11#2] Thus $\mathbb{Z}_1[\alpha_1,\dots,\alpha_r]$ is spanned (over $\mathbb{Z}_1$) by all $\left\{ \prod_{i=1}^{r} \alpha_i^{k_i} \;\middle|\; 0 \le k_i < d_i \ \forall i \right\}$. (a finite set).

(ii) trickier. Let $A = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n$ for some $e_i \in \mathbb{C}$ ($n \ge 1$) (no $\mathbb{Z}$-lin. ind. assumed)
$\alpha A \subset A$ translates to $\forall\, i$, $\alpha e_i = \sum_{j=1}^{n} a_{ij} e_j$ for some $a_{ij} \in \mathbb{Z}_1$
$\sum_{j=1}^{n} (\alpha \delta_{ij} - a_{ij}) e_j = 0 \ \forall i$. The $n \times n$ matrix $C_{\alpha - A} = \begin{bmatrix} \alpha - a_{11} & -a_{12} & \cdots & -a_{1n} \\ & \alpha - a_{22} & & \\ \vdots & & \ddots & \\ -a_{n1} & \cdots & \cdots & \alpha - a_{nn} \end{bmatrix}$ has a kernel $\neq 0$ ($\exists \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \in \mathbb{C}^n$)
so $0 = \det(C) =$ an expression $\alpha^n + (c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0)$ with $c_i \in \mathbb{Z}_1$.

Pf of Prop (2): Let $\alpha, \beta \in \overline{\mathbb{Z}}$. Since $-1 \in \mathbb{Z} \subset \overline{\mathbb{Z}}$, enough to show $\alpha+\beta, \alpha\beta \in \overline{\mathbb{Z}}$.
(i) shows $A = \mathbb{Z}_1[\alpha,\beta]$ is f.g. as ab. gp. $(\alpha+\beta)A \subset A$ and $\alpha\beta A \subset A$ clear.
(ii) then shows $\alpha+\beta, \alpha\beta \in \overline{\mathbb{Z}}$.

Eg: $\sqrt{7} + \cos\frac{2\pi}{5} \in \overline{\mathbb{Z}}$, and the proof shows it satisfies a deg 4 monic $\in \mathbb{Z}[x]$.
($\mathbb{Z}_1[\alpha,\beta] = \mathbb{Z}_1 + \mathbb{Z}_1\alpha + \mathbb{Z}_1\beta + \mathbb{Z}_1\alpha\beta$ since α, β deg 2) Ex: use the pf to calculate

Eg: Let $\zeta_m = e^{2\pi i/m}$ (a primitive m^{th} root of 1 in $\mathbb{C}$). Then $\sum_{i=0}^{m-1} \mathbb{Z}\zeta_m^i$ is a subring of $\mathbb{Z} \subset \mathbb{C}$, equal to $\mathbb{Z}[\zeta_m]$.
• For any $\alpha \in \overline{\mathbb{Z}}$, $\mathbb{Z}[\alpha] \subset \overline{\mathbb{Z}}$ and $\mathrm{Frac}\,\mathbb{Z}[\alpha] = \mathbb{Q}[\alpha]$ (exercise)
eg $\mathrm{Frac}\,\mathbb{Z}[\zeta_m] = \mathbb{Q}[\zeta_m]$ (generalizes, eg $\frac{2+i}{3+5i} \in \mathbb{Q}+\mathbb{Q}i$)
is a field called the m^{th} cyclotomic field. Q: what is $\overline{\mathbb{Z}} \cap \mathbb{Q}[\zeta_m]$? [Z] $\overline{\mathbb{Z}} \cap \mathbb{Q}[\sqrt{-3}] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$

Our proof of QR will take place in $\overline{\mathbb{Z}}$ (or $\mathbb{Z}[\zeta_p]$) and $\overline{\mathbb{Z}}/q\overline{\mathbb{Z}}$ (or $\mathbb{Z}[\zeta_p]/q\,\mathbb{Z}[\zeta_p]$). Here as usual for any $\gamma \in \overline{\mathbb{Z}}$ we say $\alpha \equiv \beta \bmod \gamma\overline{\mathbb{Z}}$ ($\alpha, \beta \in \overline{\mathbb{Z}}$) iff $\alpha - \beta \in \gamma\overline{\mathbb{Z}}$ ($\overline{\mathbb{Z}}$-multiples of γ). $\overline{\mathbb{Z}}/\gamma\overline{\mathbb{Z}}$ is the set of $\sim$ classes for this equivalence relation, and $+, \cdot$ on $\overline{\mathbb{Z}}$ induce, in the usual way, a ring structure on $\overline{\mathbb{Z}}/q\overline{\mathbb{Z}}$.
Note that $\mathbb{Z}/q\mathbb{Z} \subset^{\text{subring}} \overline{\mathbb{Z}}/q\overline{\mathbb{Z}}$, but $\overline{\mathbb{Z}}/q\overline{\mathbb{Z}}$ is not an int. domain (ex: for $q=3$, $\sqrt{3} \neq 0$ in $\overline{\mathbb{Z}}/3\overline{\mathbb{Z}}$ but $\sqrt{3}\cdot\sqrt{3} = 0$)

Reassuring lemma (4): If $N \in \mathbb{Z}_1$, $a, b \in \mathbb{Z}_1$, and $a \equiv b \bmod N\overline{\mathbb{Z}}$, then $a \equiv b \bmod N\mathbb{Z}$ (in $\mathbb{Z}_1$, ie mod $N\mathbb{Z}_1$)

Pf: $a - b \in N\overline{\mathbb{Z}}$ means $\exists\, \gamma \in \overline{\mathbb{Z}}$ s.t. $a = b + N\gamma$. $\gamma = \frac{a-b}{N} \in \mathbb{Q} \cap \overline{\mathbb{Z}} \overset{\text{Lemma 1}}{=} \mathbb{Z}_1$,
so $a \equiv b \bmod N\mathbb{Z}_1$. ∎

$t \in (\mathbb{Z}/p)^\times$

Ross 2024 L1 #3 (another example: as in $\mathbb{Z}$, if p prime $\in \mathbb{Z}$ and $\alpha, \beta \in \overline{\mathbb{Z}}$, then $(\alpha+\beta)^p \equiv \alpha^p + \beta^p \bmod p\,\overline{\mathbb{Z}}$.

The star player of our proof:

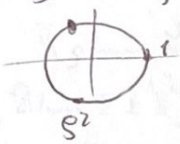
Defn (5) Fix p odd prime, $\zeta = \zeta_p = e^{2\pi i/p}$. Set

$$G = G_p = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right)\zeta^a \quad \in \mathbb{Z}[\zeta_p] \subset \overline{\mathbb{Z}} \subset \mathbb{C}$$

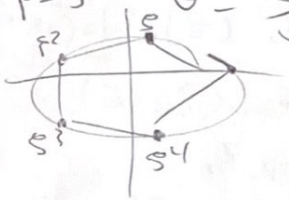
(can take $\sum_{a=1}^{p-1}$, equivalently). Huh? Why? (discussed later)

First eg: $p=3$ $\quad G = \zeta - \zeta^2 = \frac{-1+\sqrt{-3}}{2} - \frac{-1-\sqrt{-3}}{2} = \sqrt{-3}$ ($\sqrt{-3}$ is slightly sloppy for $i\sqrt{3}$ here),

$\zeta = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1+\sqrt{-3}}{2}$



$p=5$ $\quad G = \zeta - \zeta^2 - \zeta^3 + \zeta^4 = 2\cos\frac{2\pi}{5} - 2\cos\frac{4\pi}{5} = \frac{-1+\sqrt{05}}{2} - \frac{-1-\sqrt{05}}{2} = \sqrt{5}$



Idea of pf of QR - The above eg's generalize to $G^2 = (-1)^{\frac{p-1}{2}} \cdot p$ (step 1) (KEY)

$\sqrt{p}$ for $p \equiv 1 \pmod 4$
$i\sqrt{p}$ for $p \equiv 3 \pmod 4$
(exact value of G is known but tricky)

so $G \bmod_{\mathfrak{q}} \overline{\mathbb{Z}}$ is a candidate for a square root of $(-1)^{\frac{p-1}{2}} \cdot p$ in $\mathbb{Z}/\mathfrak{q}\mathbb{Z}$. But we need to determine whether $G \equiv$ integer $\bmod_{\mathfrak{q}} \overline{\mathbb{Z}}$.

For this, analyze $G^2 \bmod_{\mathfrak{q}} \overline{\mathbb{Z}}$. (Step 2). This will bring $\left(\frac{a}{p}\right)$ into the picture!

Prop (6) $G^2 = (-1)^{\frac{p-1}{2}} \cdot p$ (Step 1).

Pf: $G^2 = \sum_{a,b \in (\mathbb{Z}/p)^\times} \left(\frac{ab}{p}\right)\zeta^{a+b} = \sum_{t \in (\mathbb{Z}/p)^\times} \left(\frac{t}{p}\right) \boxed{\sum_{a \in (\mathbb{Z}/p)^\times} \zeta^{a(1+t)}}$

↗ set $b = at$ ($t \in (\mathbb{Z}/p)^\times$), so $\left(\frac{ab}{p}\right) = \left(\frac{t}{p}\right)$

if $t=-1$, this is $p-1$.

Otherwise, $1+t \in (\mathbb{Z}/p)^\times$, and $\{a(1+t) \mid a \in (\mathbb{Z}/p)^\times\} = (\mathbb{Z}/p)^\times$

so $\sum \zeta^{a(1+t)} = \sum \zeta^a = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1$.

$$= \left(\frac{-1}{p}\right)\cdot(p-1) - \sum_{t \in (\mathbb{Z}/p)^\times \setminus \{-1\}} \left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot p$$

Since $\sum_{t \in (\mathbb{Z}/p)^\times} \left(\frac{t}{p}\right) = 0$.

(L1 #4) To handle $(\frac{2}{p})$, we'll also want the Gauss sum when $p=2$.

Set $\zeta = \zeta_8 = e^{2\pi i/8}$ and $G = \underbrace{\zeta + \zeta^{-1}}_{=G_2''} \ (= \sqrt{2})$ in this case.

Prop (7) (Step 2). Let p be any prime and consider $G = G_p$. Let $q \neq p$ be prime.

Then $\begin{cases} G^q \equiv (\frac{q}{p}) \cdot G \bmod q\bar{\mathbb{Z}} & \text{if } p \text{ odd} \\ G^q \equiv (-1)^{\frac{q^2-1}{8}} \cdot G \bmod q\bar{\mathbb{Z}} & \text{if } p = 2. \end{cases}$ $\quad (\frac{a}{p})^2 = 1 \Rightarrow (\frac{a}{p}) = \frac{(a)}{(p)} \cdot \frac{(a^2)}{(p)}$

Pf: Let $p \neq 2$. $G^q = \left(\sum_{a \in (\mathbb{Z}/p)^\times} (\frac{a}{p}) \zeta^a\right)^q \equiv \sum_a (\frac{a}{p})^q \zeta^{aq} \bmod q\bar{\mathbb{Z}}$

$= (\frac{q}{p}) \sum_{a \in (\mathbb{Z}/p)^\times} (\frac{aq}{p}) \zeta^{aq} \bmod q\bar{\mathbb{Z}} = (\frac{q}{p}) \cdot G \bmod q\bar{\mathbb{Z}}$ $\quad (\{aq \mid a \in (\mathbb{Z}/p)^\times\} = \{a \in (\mathbb{Z}/p)^\times\})$

When $p=2$: $G^q = (\zeta + \zeta^{-1})^q \equiv \zeta^q + \zeta^{-q} \bmod q\bar{\mathbb{Z}}$. For $\zeta \ (= \zeta_8)$, if $q \equiv \pm 1 \bmod 8$, then $\zeta^q + \zeta^{-q} = \zeta + \zeta^{-1} = G$, and if $q \equiv \pm 3 \bmod 8$, $\zeta^q + \zeta^{-q} = \zeta^3 + \zeta^{-3} = -(\zeta + \zeta^{-1}) = -G$ $\quad (\zeta^3 = -\zeta^{-1})$

Thm (8) (Proof of QR). p odd prime, $q \neq p$ odd prime. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$, $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Pf: p odd. $G = G_p$. Then $G^q = (G^2)^{\frac{q-1}{2}} \cdot G = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} \cdot G$ (Prop 6), so by Euler's criterion $G^q \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (\frac{p}{q}) \cdot G \bmod q\bar{\mathbb{Z}}$. By Prop 7, $(\frac{q}{p}) \cdot G \equiv G^q \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (\frac{p}{q}) \cdot G \bmod q\bar{\mathbb{Z}}$. $G \in (\bar{\mathbb{Z}}/q\bar{\mathbb{Z}})^\times$ (since $G^2 = (-1)^{\frac{p-1}{2}} p$ is a unit as $p \neq q$), so $(\frac{q}{p}) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (\frac{p}{q}) \bmod q\bar{\mathbb{Z}}$. Lemma (4) $\Rightarrow$ $(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} (\frac{p}{q}) \bmod q\bar{\mathbb{Z}}$, and QR follows since $q > 2$ and both sides are ± 1.

- For $p=2$, $G = G_2 = \zeta_8 + \zeta_8^{-1}$, $G^q = 2^{\frac{q-1}{2}} \cdot G$, so (7) gives (as before) $(-1)^{\frac{q^2-1}{8}} \cdot G \equiv G^q \equiv (\frac{2}{q}) \cdot G \bmod q\bar{\mathbb{Z}}$, and we conclude as before. ∎

Rmk: Inspection of the proof shows that instead of working in $\bar{\mathbb{Z}}/q\bar{\mathbb{Z}}$ we could work in one of the following (equivalent...) settings:

- choose a finite field $\mathbb{F}_{q^f} \supset \mathbb{F}_q$ where a p^{th} root of 1 exists (i.e. take f s.t. $q^f \equiv 1 \bmod p$)
- Let $\mathfrak{q} \subset \mathbb{Z}[\zeta_p]$ be a prime ideal containing q. $\mathbb{Z}[\zeta_p]/\mathfrak{q}$ is a field $\supset \mathbb{F}_q$ where the above pf works, and indeed $|\mathbb{Z}[\zeta_p]/\mathfrak{q}| = q^f$, f min'l ≥ 1 s.t. $q^f \equiv 1 \bmod p$. (This takes proof)

Defn: An ideal I of a ring R (I is an additive gp under $+$, and $\forall r \in R, x \in I$, $r \cdot x$ is in I) is prime if $\forall a, b \in R$, if $ab \in I$ then $a \in I$ or $b \in I$.

Ross 2024 L2 #1

Why was Gauss looking at Gauss sums? This will lead us to basic notions of Galois theory used in our next pf of QR.

Let p be prime. $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$. Gauss showed that $\Phi_p(x)$ could be solved by inductively solving equations of prime degree, namely the prime factors of $p-1$.

Simple eg: $p=5$, $\zeta = \zeta_5$. ζ satisfies $p_1(x) = x^2 - (\zeta+\zeta^{-1})x + 1$; no longer in $\mathbb{Q}[x]$, but the coefficients lie in $\mathbb{Q}[\zeta+\zeta^{-1}] \subsetneq \mathbb{Q}(\zeta)$ (proper)

$3 \quad -1 \quad 1 \quad -3$

$\zeta+\zeta^{-1}$ satisfies $p_2(x) = x^2 - (\zeta+\zeta^{-1}+\zeta^2+\zeta^{-2})x + (\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2})$

$= x^2 + x - 1 \in \mathbb{Q}[x]$.

Where are the Gauss sums? For any p, ~~consider~~ let $g \in (\mathbb{Z}/p)^\times$ be a generator, and consider

$$S = \sum_{k=0}^{\frac{p-1}{2}-1} \zeta^{g^{2k}} = \zeta + \zeta^{g^2} + \zeta^{g^4} + \cdots + \zeta^{g^{p-3}} = \sum_{\substack{a \in (\mathbb{Z}/p)^\times \\ \text{s.t. } (\frac{a}{p})=1}} \zeta^a$$

and for any non-square $\lambda \in (\mathbb{Z}/p)^\times$ (e.g. $\lambda = g^1$)

$$N = \sum_{k=0}^{\frac{p-1}{2}-1} \zeta^{\lambda g^{2k}} = \sum_{\substack{a \in (\mathbb{Z}/p)^\times \\ \text{s.t. } (\frac{a}{p})=-1}} \zeta^a$$

In the $p=5$ eg, $S = \zeta+\zeta^{-1}$, $N = \zeta^2+\zeta^{-2}$.

- $G = S - N$,
- $S + N = -1$, and Gauss calculates $S \cdot N = \alpha \cdot \underbrace{(\frac{p-1}{2})}_{\sum_{k=0}^{\frac{p-1}{2}-1} \zeta^0} + \beta \cdot S + \gamma \cdot N$ by expanding & grouping, showing

$\alpha = 1 + \frac{(\frac{-1}{p})}{2}$, $\beta = \gamma$, and $\alpha + \beta + \gamma = \frac{p-1}{2}$, hence

$$\alpha = \beta = \frac{1}{2}\left[\frac{p-1}{2} - \left(\frac{1-(\frac{-1}{p})}{2}\right)\right] = \begin{cases} \frac{p-1}{4} & \text{if } (\frac{-1}{p}) = 1 \\ \frac{p-3}{4} & \text{if } (\frac{-1}{p}) = -1 \end{cases}$$

This is equivalent to computing $G^2 = (S-N)^2 = (S+N)^2 - 4SN =$

$$= 1 - 4\left[\frac{p-1}{2} \cdot \frac{1-(\frac{-1}{p})}{2} - \left(\frac{p-1}{4} - \frac{(1-(\frac{-1}{p}))}{4}\right)\right]$$

$$= 1 - (p-1) + (p-1)(\tfrac{-1}{p}) + (p-1) - (p-1)(\tfrac{-1}{p}) = p(\tfrac{-1}{p})$$

S and N satisfy the quadratic eqtn $x^2 - (S+N)x + S \cdot N = x^2 + x + \begin{cases} -(\frac{p-1}{4}) & p \equiv 1 \ (4) \\ \frac{p+1}{4} & p \equiv -1 \ (4) \end{cases}$

an example of Gauss's intermediate prime degree equations $(\mathbb{Q}(S) = \mathbb{Q}(N) = \mathbb{Q}(\sqrt{p^*}))$ $\mathbb{Q}[x]$

(This $p=5$ example is slightly misleading---)

The more general principle in building S (and N) is one of symmetrization: for any subgroup $H < (\mathbb{Z}/p)^\times$ (above, $H = \{\text{squares}\}$), ~~consider~~ and

L2#2

any $\lambda \in (\mathbb{Z}/p)^\times$, consider ~~$S(\zeta, \lambda)$~~

$$S(H,\lambda) = \sum_{h \in H} \zeta^{\lambda \cdot h}$$

. This only depends on the coset λH (so e.g. $\forall \lambda \in H$, $S(H,\lambda) = S(H,1)$)

For $H \neq (\mathbb{Z}/p)^\times$, $S(H,\lambda)$ satisfies a lower-degree equation over $\mathbb{Q}$ than ζ, so gives a proper intermediate field $\mathbb{Q}[\zeta] \supset \mathbb{Q}[S(H,\lambda)] \supset \mathbb{Q}$

Gauss's theory, and Galois theory in general, allows us to understand all intermediate fields $\mathbb{Q}[\zeta] \supset F \supset \mathbb{Q}$.

→ Indeed, let $\lambda_1, \dots, \lambda_r$ be representatives in $(\mathbb{Z}/p)^\times$ of the distinct elts of $(\mathbb{Z}/p)^\times / H$. Then $S(H,\lambda_1), \dots, S(H,\lambda_r)$ are algebraic conjugates over $\mathbb{Q}$: they are the roots of an irreducible $f(x) \in \mathbb{Q}[x]$, namely

$f(x) = \prod_{i=1}^{r} (X - S(H,\lambda_i))$. We've made two claims, neither of which is obvious: ① $f(x) \in \mathbb{Q}[x]$

② $f(x)$ irreducible in $\mathbb{Q}[x]$. Some idea from Galois theory will help prove ②

Defn: Let $F \subset K$ be a containment of fields. Let

$$\mathrm{Aut}(K/F) = \{ \text{ring isomorphisms } \sigma : K \xrightarrow{\sim} K \mid \sigma|_F = \mathrm{id}_F \}.$$

Easy ex: $\mathrm{Aut}(K/F)$ is a group (under composition) (non-abelian in general).

Our key eg: $m \in \mathbb{Z}_{\geq 1}$, $\zeta = \zeta_m$, $K = \mathbb{Q}[\zeta_m]$, $F = \mathbb{Q}$

We know the min'l poly over $\mathbb{Q}$ of ζ_m is ~~$\Phi_m(x)$~~ $\Phi_m(x)$, irred. of degree $\varphi(m)$, so ~~$\mathbb{Q}[x]/\Phi_m(x)$~~ $\mathbb{Q}[x]/\Phi_m(x) \xrightarrow{\sim} \mathbb{Q}[\zeta_m]$ is a field iso, and $\dim_{\mathbb{Q}} \mathbb{Q}[\zeta_m] = \varphi(m)$

$x \longmapsto \zeta_m$

$\mathrm{Aut}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$ contains some "obvious" elements:

$\forall\, a \in (\mathbb{Z}/m)^\times$, $\zeta \mapsto \zeta^a$ induces an element $\sigma_a \in \mathrm{Aut}\left(\frac{\mathbb{Q}[\zeta_m]}{\mathbb{Q}}\right)$ (extend in the unique way to a ring hom)

(Pf: Since ζ^a is a root of $\Phi_m(x)$ for $(a,m)=1$, we also have a field iso

$\mathbb{Q}[\zeta_m] \xleftarrow{\sim} \mathbb{Q}[x]/\Phi_m(x) \xrightarrow{\sim} \mathbb{Q}[\zeta_m]$. Composing gives σ_a.)

$\zeta^a \longleftarrow x \longmapsto \zeta$

Prop ~~There~~ There is a group iso $\kappa : \mathrm{Aut}\left(\frac{\mathbb{Q}[\zeta_m]}{\mathbb{Q}}\right) \xrightarrow{\sim} (\mathbb{Z}/m)^\times$

$\sigma \longmapsto$ ~~κ~~ $\kappa(\sigma) :=$ the unique $a \in (\mathbb{Z}/m)^\times$ s.t. $\sigma(\zeta_m) = \zeta_m^a$

with inverse

$\sigma_a \longleftarrow a$

Ross 2024 L2 #3 | **Pf:** We've shown $a \longmapsto \sigma_a$ is well-defined. It is a hom:

$\sigma_{ab}(\zeta_m) = \zeta_m^{ab} = (\zeta_m^b)^a = \sigma_a(\zeta_m^b) = \sigma_a(\sigma_b(\zeta_m))$.

κ is also a well-defined hom: $\forall\ \sigma \in \mathrm{Aut}$, ~~$\sigma(\Phi_m)$~~ $\Phi(\sigma(\zeta_m)) = \sigma\Phi(\zeta_m) = \sigma(0) = 0$

so $\sigma(\zeta_m) \in$ roots of $\Phi_m = \{\zeta^a \mid a \in (\mathbb{Z}/m)^\times\}$ so κ makes sense. It is a hom because $(\sigma\tau)(\zeta) = \sigma(\zeta^{\kappa(\tau)}) = \sigma(\zeta)^{\kappa(\tau)} = \zeta^{\kappa(\sigma)\kappa(\tau)}$

$= \zeta^{\kappa(\sigma\tau)}$ so $\kappa(\sigma\tau) = \kappa(\sigma)\kappa(\tau)$ in $(\mathbb{Z}/m)^\times$.

The two maps are clearly inverses, so they are isos.

Rmk: Can also view this as: easy to see κ injective, and since $\{\sigma_a \mid a \in (\mathbb{Z}/m)^\times\} \subset \mathrm{Aut}$, we must have surj. too by size comparison.

Rmk: When $m = p$, what we called $S(H, \lambda)$ is then equivalently: consider ~~$\mathbb{Z}_H$~~ $\kappa^{-1}(H) \subset \mathrm{Aut}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$; then

$$S(H,\lambda) = \sum_{\sigma \in \kappa^{-1}(H)} \sigma(\sigma_\lambda(\zeta)) = \sum_{\sigma \in \sigma_\lambda \cdot \kappa^{-1}(H)} \sigma(\zeta)$$

($\sigma_\lambda(\zeta) = \zeta^{\kappa(\sigma_\lambda)}$; $\sigma_\lambda \cdot \kappa^{-1}(H)$ is a coset in Aut)

: we are using subgroups of Aut to "symmetrize" the root ζ.

L2 #3 improvement! $g_1, \dots, g_r$ reps in G of G/H.

$$S(H, g_i) = \sum_{h \in H} g_i h(\zeta). \quad f(x) = \prod_{i=1}^{r} (X - S(H, g_i)) = \text{poly} \in \mathbb{Q}[\zeta_q][X]$$

whose coeffs are symm. polys in $\{S(H, g_i)\}_{i=1}^r$

Claim: $f(x) \in \mathbb{Q}[x]$ and is irreducible.

Input: If $\alpha \in \mathbb{Q}[\zeta_m]$ and $g(\alpha) = \alpha\ \forall\ g \in \mathrm{Aut}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$, then $\alpha \in \mathbb{Q}$. (We'll do this if we have time).

Assume input.

Pf that $f(x) \in \mathbb{Q}[x]$: By the input, STP $\forall\ g \in \mathrm{Aut}(\mathbb{Q}[\zeta_q]/\mathbb{Q})$, g fixes each coeff. of f, i.e. $gf = f$ (where $g(\sum a_n x^n) = \sum g(a_n) x^n$).

But $g(f(x)) = \prod_{i=1}^{r} (X - g(S(H, g_i))) = \prod_{i=1}^{r} (X - S(H, gg_i))$

$= \prod_{i=1}^{r} (X - S(H, g_i))$ since g permutes the cosets G/H (and $S(H,\lambda)$ only depends on λH).

$= f(x)$. Thus $f(x) \in \mathbb{Q}[x]$.

L2 #4

~~then $\alpha \in \mathbb{Q}$. This shows $f(x) \in \mathbb{Q}[x]^{\vee}$~~ RESUME

Pf: Assume the claim (input). Then we check $f(x)$ is irr. in $\mathbb{Q}[x]$

Well, if $f(x) = f_1(x) f_2(x)$ is a non-triv. factorization, then roots of f_1 (and f_2) form a ~~set~~ G-stable subset of {roots of f} (since $\forall \sigma \in G$, $\sigma f_1 = f_1$). Roots of $f = \{S(H, \tau)\}_{\tau \in G/H}$ is permuted transitively by G: given $\tau_1, \tau_2 \in G$, $(\tau_1 \tau_2^{-1}) \cdot S(H, \tau_2)$

$= \tau_1 \tau_2^{-1} \sum_{h \in H} \tau_2 h(\zeta) = \sum \tau_1 h(\zeta) = S(H, \tau_1)$. So $f_1 = f$.

To For the claim, we'll prove a more general result that is a big step in the pf of the main thm. of Galois theory [ex: give an elementary pf in our special case]

Thm Let K be any field. Let $H < \mathrm{Aut}(K)$ be any finite subgroup of $\mathrm{Aut}(K)$.
Set $F = K^H = \{\alpha \in K \mid h(\alpha) = \alpha \ \forall h \in H\}$
Then F is a field (clear) and $[K : F] = \#H$ (we only use $\geq$ for the claim)

In our case $H = \mathrm{Aut}(\mathbb{Q}[\zeta_m]/\mathbb{Q})$, $K = \mathbb{Q}[\zeta_m]$, we get $[K : K^H] = \varphi(m)$. ($\geq$) But $K \supset K^H \supset \mathbb{Q}$, $\varphi(m)$, so $K^H = \mathbb{Q}$. ∎

Ross 2024 | L2 ⇒ 5

Pf of Thm: (i) If H is merely a subset of $\mathrm{Aut}(K)$, then we check $[K:K^H] \geq |H|$.

Lemma: The elements of H are K-linearly ind., so $|H| \leq \dim_K \mathrm{Hom}_{F\text{-vect}}(K,K) = [K:F]$

Exercise: For any field K & distinct gp homs $\chi_1, \dots, \chi_n : G \to K^\times$, $\nexists$ K-linear relat. $\sum a_i \chi_i = 0$ (as functions $G \to K$) (induction on n)

Note that in our $\mathbb{Q}(\zeta_m)$ example $\mathrm{Aut}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, knowing $[\mathbb{Q}(\zeta_m):\mathbb{Q}] \geq \varphi(m)$ is already enough to see $\mathbb{Q}(\zeta_m)^{\mathrm{Aut}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} = \mathbb{Q}$.

(ii) For H a subgroup, the reverse inclusion holds. We'll just do it for $K = \mathbb{Q}(\zeta_m)$, $F = \mathbb{Q}$. We have inclusions

$$\mathbb{Q} \subset \mathbb{Q}[S(H,1)] \subset K^H \subset K = \mathbb{Q}[\zeta_m]$$

($\mathbb{Q} \subset \mathbb{Q}[S(H,1)]$: $|G/H|$; $K^H \subset K$: $\geq |H|$ (i))

$$\varphi(m) = \#G.$$

because $S(H,1)$ satisfies an irred $\in \mathbb{Q}[x]$ of this degree

so we know from (i) that $[K:K^H] \geq |H|$

But $[K:\mathbb{Q}[S(H,1)]] = [K:K^H] \cdot [K^H:\mathbb{Q}[S(H,1)]]$

$$\frac{|G|}{|G/H|} = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}[S(H,1)]:\mathbb{Q}]}$$

$$|H| \cdot [K^H:\mathbb{Q}[S(H,1)]]$$

$$|H|$$

Thus $K^H = \mathbb{Q}[S(H,1)]$ and $[K:K^H] = |H|$!

(Alternative for (ii): $\mathbb{Q} \subset K^H \subset K = \mathbb{Q}(\zeta_m)$ ($K^H \subset K$: $\geq H$) Each $g \in \mathrm{Gal}(K/\mathbb{Q})$ restricts to an element of $\mathrm{Aut}(K^H/\mathbb{Q})$ (since $\forall x \in K^H$, $h \in H$, $hgx = g(g^{-1}hg)x = ghx = gx$ since G is abelian). $g_1|_{K^H} = g_2|_{K^H} \Leftrightarrow g_2^{-1}g_1|_{K^H} = \mathrm{id} \Leftrightarrow g_2^{-1}g_1 \in \mathrm{Aut}(K/K^H) \supseteq H$ don't return $\varphi(m)$ $=$.)

Exp pf: Induct. Clear $n=1$. Let $\sum_{i=1}^n a_i \chi_i = 0$ $a_i \in K$. If some $a_i = 0$, reduced to the $n-1$ case, so wma all $a_i \neq 0$. $\chi_1 \neq \chi_2 \Rightarrow \exists s \in G$ s.t. $\chi_1(s) \neq \chi_2(s)$. $\sum a_i \chi_i(x) = 0 \ \forall x$, $\Rightarrow \sum a_i \chi_1(g) \chi_i(x) = 0$

$\sum_i a_i \chi_i(g) \chi_i(x) = 0$ / subtract

$\sum_{i=2}^n a_i (\chi_i(s) - \chi_1(s)) \chi_i(x) = 0$ $\overset{\text{ind. hyp.}}{\Rightarrow}$ $a_2, \dots, a_n = 0$ $\Rightarrow$ all $a_i = 0$

($\chi_i(s) - \chi_1(s) \neq 0$ for $i = 2$)

Galois theory

[L2=6] (or L3≠1)

Defn: Let K/F be a field ext. of finite degree. We say K/F is Galois if $|\mathrm{Aut}(K/F)| = [K:F]$. We tend to write $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$, the Galois group of K/F.

Thm (Galois correspondence) Let K/F be a Galois ext. There are inclusion-reversing bijections, inverse to one another

$$\left\{\begin{array}{l}\text{subgroups} \\ H < \mathrm{Gal}(K/F)\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\text{subfields} \\ F \subset L \subset K\end{array}\right\} \quad \text{given by}$$

$$\longleftarrow$$

$$H \longmapsto K^H$$

$$\mathrm{Aut}(K/L) \longleftarrow L$$

(and K/L is Galois)

complete if $\mathbb{Q}(\zeta_m)/\mathbb{Q}$

Pf: (i) Claim: For any H, $\mathrm{Aut}(K/K^H) = H$. Indeed, $H < \mathrm{Aut}(K/K^H)$ is clear. Suppose $\exists\ \sigma \in \mathrm{Aut}(K/K^H) \setminus H$. Then $H \cup \{\sigma\}$ is a set of $|H|+1$ auts $K \to K$ that are id on K^H, so by last thm, $|H| \geq [K:K^H] \geq |H|+1$ (see part (i) of Thm.)

$\Rightarrow \Leftarrow$

(ii) Claim: For any L, K/L is Galois & $K^{\mathrm{Gal}(K/L)} = L$. If we know K/L Galois, then $|\mathrm{Gal}(K/L)| = [K:L]$ and $[K:K^{\mathrm{Gal}(K/L)}] = |\mathrm{Gal}(K/L)| = [K:L]$. But $L \subset K^{\mathrm{Gal}(K/L)} \subset K$, so $L = K^{\mathrm{Gal}(K/L)}$.

$[K:L]$ $\quad$ $[K:L]$

$L[x]/f(x) \twoheadrightarrow K$, $x \mapsto \alpha$

We'll complete the proof just for $K/F = \mathbb{Q}(\zeta_m)/\mathbb{Q}$ again. For any $L \subset \mathbb{Q}(\zeta_m) = K$, $K = L[\alpha]$ for any root α of ~~a splitting field over L of~~ $\Phi_m(x)$ (b/c same true w/ $L = \mathbb{Q}$) or of any of its irred factors $f(x) \in L[x]$ (deg $f = [K:L]$ then). Let α, β be two roots (in K) of $f(x)$. Claim: $\exists\ \sigma: K \xrightarrow{\sim} K$ in $\mathrm{Aut}(K/L)$ s.t. $\sigma(\alpha) = \beta$.

Pf: $K \cong L[x]/f(x) \xrightarrow{\sim} K$. We obtain at least $\deg(f) = [K:L]$ elements of $\mathrm{Aut}(K/L)$, and we win:

$\alpha \longleftarrow x \longmapsto \beta$

set $H = \mathrm{Aut}(K/L)$, so $K \supseteq K^H \supseteq L$, so $[K:L] = H$ and $L = K^H$. ∎

$[K:L] \leq |H|$ $\quad$ $[K:L]$

by what we've just said

L3 #0 Defn K/F = Galois (of finite degree) if $|\underbrace{Aut(K/F)}_{\text{write Gal.}}| = [K:F]$

Thm: K/F Galois. There are inclusion-reversing bij, inverse to one another,

$$\left\{\begin{array}{l}\text{subgps.}\\ H < Gal(K/F)\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\text{subfields}\\ F \subset L \subset K\end{array}\right\} \quad \text{given by}$$

$$H \longmapsto K^H$$

$$Aut(K/L) \longleftarrow L$$

and K/L is Galois

Pf Example: $K/F = \mathbb{Q}[\zeta_m]/\mathbb{Q}$ is Galois. Prove the thm. just for this example:

Let $G = Gal(\mathbb{Q}[\zeta_m]/\mathbb{Q})$. For any $H<G$, last time we saw

$$\mathbb{Q} \subset \mathbb{Q}(S(H,1)) = K^H \subset K \quad \text{where } S(H,1) = \sum_{\sigma \in H} \sigma(\zeta), \quad \zeta = e^{2\pi i/m}$$

($\mathbb{Q} \subset \mathbb{Q}(S(H,1))$: degree $|G/H|$; $K^H \subset K$: degree $|H|$)

$H < Aut(K/K^H)$ is clear. You can finish the proof that $H = Aut(K/K^H)$ either by (i) using the general arg from last time (K-linear ind. of distinct homs $K^\times \to K^\times$ shows if $\sigma \in Aut(K/K^H) \setminus H$, then $|H \cup \{\sigma\}| \le [K:K^H] = |H|$, but $|H|+1$ and $H \cup \{\sigma\}$ is K-lin. ind. $\Rightarrow\Leftarrow$.

This works $\forall$ K/F.)

OR

(ii) Check directly that any $\sigma \in G \setminus H$ can't fix $S(H,1)$: via $\kappa: G \xrightarrow{\sim} (\mathbb{Z}/m)^\times$, this translates to $x \notin U$ (a unit mod m) implies $\sum_{y \in U} \zeta^{xy} \neq \sum_{y \in U} \zeta^y$ $\quad xU \cap U = \emptyset$ $(x \notin U)$,

and then we are done if we know $\{\zeta^a\}_{a \in (\mathbb{Z}/m)^\times}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[\zeta_m]$

For $m=p$ this is easy (this is essentially an earlier exercise): $1, \zeta_p, \dots, \zeta_p^{p-2}$ is clearly a $\mathbb{Q}$-basis, and $\zeta_p, \dots, \zeta_p^{p-2}, \zeta_p^{p-1} = -\zeta_p^{p-2} - \dots - \zeta_p - 1$ is then clearly one too.

Now for any $\mathbb{Q} \subset L \subset \mathbb{Q}[\zeta_m] = K$, we show K/L is Galois and $K^{Gal(K/L)} = L$.

Suppose we know K/L Galois. Then

$$[K:K^{Gal(K/L)}] \underset{\text{generality from last time}}{=} |Gal(K/L)| = [K:L]. \quad \text{But } L \subseteq K^{Gal(K/L)} \subset K$$

so for degree reasons $=$ holds. [This part is general.] To show K/L Galois, note $K = L[\alpha]$ for any root α of $\Phi_m(x)$ or of its irreducible factors f over L (so $\deg(f) = [K:L]$).

Let α, β be two roots in K of such an f. Then $\exists\ \sigma: K \xrightarrow{\sim} K$ in $Aut(K/L)$ s.t. $\sigma(\alpha) = \beta$, namely $K \xleftarrow{\sim} L[x]/f(x) \xrightarrow{\sim} K$, $\alpha \longleftarrow x \longmapsto \beta$. We get $\deg(f) = [K:L]$ elts in $Aut(K/L)$, so

Ross 2024 L3 #1 ($K \supset K^{\mathrm{Aut}(K/L)} \supset L$, and by degrees and such $[K:L] = |\mathrm{Aut}(K/L)|$. so K/L Galois. #

Example: $K = \mathbb{Q}[\zeta_p]$ is Galois, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times$, and the

$\mathbb{Q}$ $\qquad \sigma_a \longleftarrow a$ s.t. $\sigma_a(\zeta) = \zeta^a$

subfields of $\mathbb{Q}(\zeta_p)$ are in bijection w/ s/groups of $(\mathbb{Z}/p)^\times$, i.e. $\forall$ divisor $d/(p-1)$, $\exists!_{H = C_d} C_d < (\mathbb{Z}/p)^\times$, and the subfields are the K^{C_d} (recall $x^{-1}(C_d)$) ($= \mathbb{Q}[S(C_d, 1)]$, explicitly).

Take the subgroup $H = \left[(\mathbb{Z}/p)^\times\right]^2 < (\mathbb{Z}/p)^\times$ of squares, so

$\mathbb{Q}[\zeta_p]$

| deg $\frac{p-1}{2}$

$\mathbb{Q}[\zeta_p]^H = \mathbb{Q}[S(H,1)] = \mathbb{Q}\left[\sum_{k=0}^{\frac{p-1}{2}-1} \zeta^{g^{2k}}\right]$ the Gauss sum variant we encountered earlier, showing $(-1-(\frac{-1}{p})p)$

$\|$ $\longleftarrow$

$\mathbb{Q}\left[\frac{-1 + \sqrt{1 - (\cdots)}}{2}\right] = \mathbb{Q}\left[\sqrt{(\frac{-1}{p})\cdot p}\right]$

(recall $x^2 + x + \frac{1-1}{4}$ was min poly $\frac{1-1}{4}$ is $\frac{1-(\frac{-1}{p})p}{4}$)

deg = 2

$\mathbb{Q}$.

This picture will be the basis for our Galois theory pf/re-interpretation of the previous proof. We won't need the Gauss sums at all, though: Gal. thm. tells us $\exists!$ L s.t. $\mathbb{Q} \subset L \subset \mathbb{Q}[\zeta_p]$ w/ $L/\mathbb{Q}$ quadratic, and $S(H,1)$ only used above to identify $L = \mathbb{Q}[\sqrt{(\frac{-1}{p})p}]$. Suffices instead to check $\mathbb{Q}[\sqrt{(\frac{-1}{p})p}] \subset \mathbb{Q}[\zeta_p]$, which is a simple exercise using that

$p = \Phi_p(1) = \prod_{i=1}^{p-1}(1-\zeta^i)$ (pair the $i, p-i$ terms to show $(\frac{-1}{p})\cdot p$ is a square in $\mathbb{Q}[\zeta_p]$). Notation convention: $p^* = (\frac{-1}{p})\cdot p$.

Let ℓ be an odd prime $\neq p$, and consider $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$.

QR follows from giving two answers to the question:

(*) Is $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}[\sqrt{p^*}])$?

Answer 1: $\mathbb{Q}[\sqrt{p^*}] = \mathbb{Q}[\zeta_p]^H$, $H = (x^{-1})(\text{squares})$, so $\sigma_\ell|_{\mathbb{Q}[\sqrt{p^*}]} =: d$

iff $\sigma_\ell \in H$ iff $(\frac{\ell}{p}) = 1$

"cyclotomic perspective"

L3 #2 **Answer 2:** ("quadratic perspective"). We show $\sigma_q|_{\mathbb{Q}[\sqrt{p^*}]} = \mathrm{id}$ iff $f(x) = x^2 + x + \begin{cases} \frac{1-p}{4} & p \equiv 1 \bmod 4 \\ \frac{1+p}{4} & p = 3 \end{cases}$ factors mod q

(iff $\sqrt{p^*} \in \mathbb{Z}/q$, ie $\left(\frac{p^*}{q}\right) = 1$). Why:

PIZZA

Pizza

ⓐ $\mathcal{O} := \overline{\mathbb{Z}} \cap \mathbb{Q}[\sqrt{p^*}] = \mathbb{Z}[\text{root } \alpha \text{ of } f] \cong \mathbb{Z}[x]/f(x)$, so

(exercise) (call the other root β)

$\mathcal{O}/q\mathcal{O} \cong \mathbb{Z}/q[x]/f(x)$. $\sigma_q|_{\mathbb{Q}[\sqrt{p^*}]}$ preserves $\mathcal{O}$ and $q\mathcal{O}$, so gives

a ring isomorphism $\overline{\sigma}_q : \mathcal{O}/q\mathcal{O} \xrightarrow{\sim} \mathcal{O}/q\mathcal{O}$

(made ⓐ $\mathbb{Z}[\zeta_p]/q$, and we know mod q $\overline{\sigma}_q$ is $\overline{\sigma}_q(a) = a^q$ where $\forall\, a \in \mathbb{Z}[\zeta_p]/q$: L1).

- Suppose $f(x)$ mod q irreducible. Then $\mathcal{O}/q\mathcal{O}$ is a finite field with q^2 elements. Thus $\overline{\sigma}_q$ is non-trivial on $\mathcal{O}/q\mathcal{O}$, hence σ_q is non-triv. on $\mathcal{O}$ and on $\mathbb{Q}[\sqrt{p^*}]$
- Now suppose $f(x) \bmod q = (x-\bar{\alpha})(x-\bar{\beta})$. Then ($\bar{\alpha} \neq \bar{\beta}$) $\mathcal{O}/q\mathcal{O} \xrightarrow{\sim} \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ is a ring iso (CRT), and $a \mapsto a^q$ is trivial (id) on RHS, hence on LHS $x \mapsto (\alpha, \beta)$

Claim: $\sigma_q|_{\mathcal{O}}$ is id (hence $\sigma_q|_{\mathbb{Q}[\sqrt{p^*}]} = \mathrm{id}$).

$\{\alpha, \beta\} \ni \overline{\sigma}_q(\alpha) = \alpha + qy$ for some $y \in \mathcal{O}$ since $\overline{\sigma}_q$ trivial. If $\sigma_q(\alpha) = \beta$, then $q \mid (\beta - \alpha)$ in $\mathcal{O}$, ie $q \mid \sqrt{p^*}$ in $\mathcal{O}$. $\Rightarrow\Leftarrow$ (using norm)

Answer 1 = Answer 2, so $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$, which is Q12. □

Rmk: This Gal thry proof has a broader context. ↙ Frobenius el'ts – prime splitting ↘ two answers to "does q split in $\mathcal{O}$"?

- This pf needed very little general Gal thry, but it provides the right framework. Needed

$\chi : \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p)^\times$, $\mathbb{Q}[\sqrt{p^*}] \subset \mathbb{Q}[\zeta_p]$ is the field fixed by π^{-1} (squares) (pointwise)

and $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}[\sqrt{p^*}]) \xrightarrow{\sim} \{\text{squares}\}$ (no other auts fix it pointwise)

rec x/a: $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \mathrm{Nm}\, \mathbb{A}_L^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$, $\sigma_q \mapsto \sigma_q$

$\downarrow$ $\qquad\qquad$ $\downarrow$

$\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \mathrm{Nm}\, \mathbb{A}_L^\times \qquad \mathrm{Gal}(L/\mathbb{Q})$

σ_q trivial iff $q \in \mathrm{Nm}\, \mathbb{A}_L^\times$ (since val 1) $\Leftrightarrow$ q splits $\Leftrightarrow$ σ_q trivial

L3 #2 Answer 2: ("quadratic perspective"). We show $\sigma_\mathfrak{q}|_{\mathbb{Q}[\sqrt{p^*}]} = \mathrm{id}$ iff $f(x) = x^2 + x + \begin{cases} \frac{1-p}{4} & p \equiv 1 \bmod 4 \\ \frac{1+p}{4} & p = 3 \end{cases}$ factors mod $\mathfrak{q}$

(iff $\sqrt{p^*} \in \mathbb{Z}/\mathfrak{q}$, ie $\left(\frac{p^*}{\mathfrak{q}}\right) = 1$). Why:

PIZZA

$\mathcal{O} := \overline{\mathbb{Z}} \cap \mathbb{Q}[\sqrt{p^*}] = \mathbb{Z}[\underbrace{\text{root of } f}_{\alpha}] \cong \mathbb{Z}[x]/f(x)$, so

(exercise) (call the other root β)

$\mathcal{O}/\mathfrak{q}\mathcal{O} \cong \mathbb{Z}/\mathfrak{q}[x]/f(x)$. $\sigma_\mathfrak{q}|_{\mathbb{Q}[\sqrt{p^*}]}$ preserves $\mathcal{O}$ and $\mathfrak{q}\mathcal{O}$, so gives

a ring isomorphism $\overline{\sigma}_\mathfrak{q} : \mathcal{O}/\mathfrak{q}\mathcal{O} \xrightarrow{\sim} \mathcal{O}/\mathfrak{q}\mathcal{O}$

(since $\mathcal{O} \subseteq \mathbb{Z}[\zeta_p]/\mathfrak{q}$, and we know mod $\mathfrak{q}$ $\overline{\sigma}_\mathfrak{q}$ is $\overline{\sigma}_\mathfrak{q}(a) = a^\mathfrak{q}$ where $\forall\, a \in \mathbb{Z}[\zeta_p]/\mathfrak{q}$: L1).

- Suppose $f(x)$ mod $\mathfrak{q}$ irreducible. Then $\mathcal{O}/\mathfrak{q}\mathcal{O}$ is a finite field with $\mathfrak{q}^2$ elements. Thus $\overline{\sigma}_\mathfrak{q}$ is non-trivial on $\mathcal{O}/\mathfrak{q}\mathcal{O}$, hence $\sigma_\mathfrak{q}$ is non-triv. on $\mathcal{O}$ and on $\mathbb{Q}[\sqrt{p^*}]$
- Now suppose $f(x) \bmod \mathfrak{q} = (x-\bar{\alpha})(x-\bar{\beta})$. Then ($\bar{\alpha} \neq \bar{\beta}$) $\mathcal{O}/\mathfrak{q}\mathcal{O} \cong \mathbb{Z}/\mathfrak{q}\mathbb{Z} \times \mathbb{Z}/\mathfrak{q}\mathbb{Z}$ is a ring iso (CRT), and $a \mapsto a^\mathfrak{q}$ is trivial (id) on RHS, hence on LHS $x \longmapsto (\alpha, \beta)$

Claim: $\sigma_\mathfrak{q}|_\mathcal{O}$ is id (hence $\sigma_\mathfrak{q}|_{\mathbb{Q}[\sqrt{p^*}]} = \mathrm{id}$).

$\{\alpha, \beta\} \ni \overline{\sigma}_\mathfrak{q}(\alpha) = \alpha + \mathfrak{q}y$ for some $y \in \mathcal{O}$ since $\overline{\sigma}_\mathfrak{q}$ trivial. If $\sigma_\mathfrak{q}(\alpha) = \beta$, then

$\mathfrak{q} \mid (\beta - \alpha)$ in $\mathcal{O}$, ie $\mathfrak{q} \mid \sqrt{p^*}$ in $\mathcal{O}$. $\Rightarrow\!\Leftarrow$ (using norm)

Answer 1 = Answer 2, so $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$, which is QR. □

Rmk: This Gal thry proof has a broader context. ← Frobenius elts – prime splitting – two answers to "does $\mathfrak{q}$ split in $\mathcal{O}$"?

- This pf needed very little general Gal thry, but it provides the right framework. Needed

$\chi : \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p)^\times$, $\mathbb{Q}[\sqrt{p^*}] \subset \mathbb{Q}[\zeta_p]$ is the field fixed by $\ker\chi$ (squares)

and $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}[\sqrt{p^*}]) \xrightarrow{\sim} \{\text{squares}\}$ (pointwise) (no other subs fix it pointwise)

recall: $\mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times \mathrm{Ker}\,\mathrm{Nm}_{\mathbb{A}_L} \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q})$, $\sigma_\mathfrak{q} \longmapsto \sigma_\mathfrak{q}$

$\mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times \mathrm{Nm}\,\mathbb{A}_L^\times \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$

$\sigma_\mathfrak{q}$ trivial iff $\mathfrak{q} \in \mathrm{Nm}\,\mathbb{A}_L^\times$ (since unit) $\Leftrightarrow$ $\mathfrak{q}$ splits $\Leftrightarrow$ $\sigma_\mathfrak{q}$ trivial

Lec #1 Start Qp.

Motivation: Solving polynomial equations mod higher and higher powers of a prime p. For $a \in \mathbb{Z}_{(p)}$ (or $\mathbb{Q}$), write $v_p(a)$ for the power of p dividing a ($a = p^{v_p(a)} \cdot$ (coprime to p))

Lemma: Let $f(x) \in \mathbb{Z}_{(p)}[x]$, $n, k \in \mathbb{Z}_{\geq 0}$: ~~$0 < 2k < n$~~ $n \geq 2k+1$, $\alpha \in \mathbb{Z}/p^n$ s.t. $f(\alpha) \equiv 0 \bmod p^n$ and ~~$\bmod p$~~ $v_p(f'(\alpha)) = k$ [this makes sense, ie any $\tilde{\alpha} \in \mathbb{Z}_{(p)}$ cong. to $\alpha \bmod p^n$ will have the same $v_p(f'(\tilde{\alpha}))$ since $k < n$:

Then $\exists\ \alpha_{n+1} \in \mathbb{Z}/p^{n+1}$: $\alpha_{n+1} \equiv \alpha \bmod p^{n-k}$, $v_p(f'(\alpha_{n+1})) = k$, $f(\alpha_{n+1}) \equiv 0 \bmod p^{n+1}$

(Think $n=1$, $k=0$.)

Pf: Let $\beta = \alpha + p^{n-k} \cdot z \bmod p^{n+1}$ (fixing a lift of α to $\mathbb{Z}/p^{n+1}$)

$f(\beta) = f(\alpha) + p^{n-k} z f'(\alpha) + p^{2n-2k} \cdot w$ some $w \in \mathbb{Z}_{(p)}$. $2n-2k \geq n+1$, so

$f(\beta) \equiv \underbrace{f(\alpha)}_{\equiv 0 \bmod p^n} + \underbrace{p^{n-k} z f'(\alpha)}_{v_p(p^{n-k} f'(\alpha)) = n} \bmod p^{n+1}$ $\Longrightarrow$ can choose z (unique mod p) s.t. $f(\beta) \equiv 0 \bmod p^{n+1}$.

Set ~~$\alpha_{n+1} = \beta$~~ for this choice. $\alpha_{n+1} \equiv \alpha \bmod p^{n-k}$ clear,

$f'(\alpha_{n+1}) = f'(\alpha) + p^{n-k} z f''(\alpha) \equiv f'(\alpha) \bmod p^{n-k}$ and $n-k > k$

then forces $v_p(f'(\alpha_{n+1})) = v_p(f'(\alpha)) = k$. ∎

e.g. squares, ~~$a \bmod p$~~ [Suppose p odd], $\left(\frac{a}{p}\right) = 1$. Then take $f(x) = x^2 - a$

$f'(x) = 2x$. Let $\alpha_1^2 \equiv a \bmod p$, so $f(\alpha_1) \equiv 0 \bmod p$, $f'(\alpha_1) \not\equiv 0 \bmod p$. We get $\alpha_2 \equiv \alpha_1 \bmod p$ s.t. $f(\alpha_2) \equiv 0 \bmod p^2$ $f'(\alpha_2) \not\equiv 0 \bmod p$,

$\alpha_3 \equiv \alpha_2 \bmod p^2$

$\alpha_4 \equiv \alpha_3 \bmod p^3$

$\alpha_{n+1} \equiv \alpha_n \bmod p^n$, $f(\alpha_{n+1}) \equiv 0 \bmod p^{n+1}$, $f'(\alpha_{n+1}) \not\equiv 0 \bmod p$

$\cdots \to \mathbb{Z}/p^{n+1} \to \mathbb{Z}/p^n \to \cdots \to \mathbb{Z}/p$

$\alpha_{n+1} \longmapsto \alpha_n \longmapsto \alpha_{n-1} \cdots \mapsto \alpha_1$. The system $(\alpha_1, \alpha_2, \cdots) \in \prod_{n \geq 1} \mathbb{Z}/p^n$

leads us to define ring of p-adic numbers $\varprojlim \mathbb{Z}/p^n$.

[2]! For $p=2$ above fails since $f'(\alpha_1) \equiv 0 \bmod p$. The lemma shows that if ~~$\alpha_3 \in \mathbb{Z}/8$~~ given s.t. $f(\alpha_3) \equiv 0 \bmod 8$, then since $v_2(f'(\alpha_3)) = v_2(2\alpha_3) = 1$ ($\alpha^2 \equiv 1 \bmod 8$) we get $\alpha_4 \equiv \alpha_3 \bmod p^2$, $\alpha_5 \equiv \alpha_4 \bmod p^3$ ($\alpha_3 \bmod p$, $\alpha_3 \bmod p^2$, $\alpha_4 \bmod p^3$, $\alpha_5 \bmod p^4$, $\cdots$) gives the compatible system

Dfn: Let $\mathbb{Z}_p = \{(a_1, a_2, \cdots) \in \prod_{n \geq 1} \mathbb{Z}/p^n \mid a_{i+1} \equiv a_i \bmod p^i\ \forall i\}$. $\mathbb{Z}_p$ is a ring, $+$ and $\cdot$ component-wise. $\forall n$, $\exists$ surj. ring homs $\mathbb{Z}_p \xrightarrow{\pi_n} \mathbb{Z}/p^n$ and $\pi_n = (\text{reduced mod } p^n) \circ \pi_{n+1}$ $((a_n) \longmapsto a_n)$

Note
- $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ (subring)
- v_p extends to a map $v_p : \mathbb{Z}_p \to \mathbb{Z} \cup \{\infty\}$, $v_p(\alpha) = \max n$ s.t. $\alpha \bmod p^n \equiv 0$ ($\alpha = 0 \leftrightarrow n = \infty$)
- $\mathbb{Q}_p := \operatorname{Frac} \mathbb{Z}_p$. Exercise: $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$ and $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid v_p(a) = 0\}$

The argument of the lemma shows: For $f \in \mathbb{Z}_p[x]$, $n, k \in \mathbb{Z}_{\geq 0}$ with $n \geq 2k+1$, $\alpha \in \mathbb{Z}_p$ s.t. $f(\alpha) \equiv 0 \bmod p^n$ and $v_p(f'(\alpha)) = k$, $\exists\ \beta \in \mathbb{Z}_p$: $\beta \equiv \alpha \bmod p^{n-k}$, $v_p(f'(\beta)) = k$, $f(\beta) \equiv 0 \bmod p^{n+1}$

We can use this to solve equations in $\mathbb{Z}_p$

Harder exercise: Analyze the group $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ $\forall p$ ($\mathbb{Z}$ $p=2$!)

Prop: Let $f(x_1, \dots, x_m) \in \mathbb{Z}_p[x_1, \dots, x_m]$, $n, k \in \mathbb{Z}_{\geq 0}$ s.t. $n \geq 2k+1$, $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}_p^m$.
Suppose $\exists\ j$ s.t. $f(\alpha) \equiv 0 \bmod p^n$ and $v_p\left(\frac{\partial f}{\partial x_j}(\alpha)\right) = k$.
Then $\exists\ \beta \in \mathbb{Z}_p^m$: $f(\beta) = 0$ ($=$ in $\mathbb{Z}_p$!) and $\beta \equiv \alpha \bmod p^{n-k}$.

Pf: $m=1$: as above get $(\alpha_d)_{d \geq n}$ sequence $f(\alpha_d) \equiv 0 \ (p^{d+1})$ $\alpha_{d+1} \equiv \alpha_d \bmod p^{d-k}$
($\alpha = \alpha_1 = \alpha_n$). The sequence $(\alpha_d \bmod p^{d-k}) \in \mathbb{Z}_p$ is a solution. $v_p(f'(\alpha_d)) = k$

For $m > 1$: Take j s.t. $v_p\left(\frac{\partial f}{\partial x_j}(\alpha)\right) = k$ as in Prop. Fix α_i, $i \neq j$ and let $\tilde{f}(X_j) \in \mathbb{Z}_p[X_j]$ be $f(\alpha_1, \alpha_2, \dots, X_j, \alpha_{j+1}, \dots, \alpha_m)$. $m=1$ case gives $\tilde{\alpha}_j \in \mathbb{Z}_p$: $\tilde{f}(\tilde{\alpha}_j) = 0$ as within, so $f(\alpha_1, \dots, \alpha_{j-1}, \tilde{\alpha}_j, \dots, \alpha_m) = 0$. ∎

We'll apply this to quadratics

[L#3]

Hilbert symbol. Let v be a prime number or ∞. Set $\mathbb{Q}_\infty = \mathbb{R}$. OR: just write $K \in \{\mathbb{Q}_p, \mathbb{R}\}$

Dfn: For $a, b \in \mathbb{Q}_v^\times$, set $(a,b) = \begin{cases} +1 & \text{if } z^2 = ax^2 + by^2 \text{ has a solution} \\ & (z,x,y) \neq (0,0,0) \text{ in } \mathbb{Q}_v^3 \\ -1 & \text{if not} \end{cases}$

(a,b) is the Hilbert symbol. (write $(a,b)_v$ when we want v explicit). It is a function

$$\mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \times \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \to \pm 1$$

We'll eventually show $(\ ,\ )$ is a non-degenerate (symmetric) bilinear form on the $\mathbb{Z}/2$-vect sp $\mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$

Lemma: Let $a, b \in K^\times$, set $K_b = K[\sqrt{b}]$. $(a,b) = 1$ iff $a \in NK_b^\times$. Here $N: K_b^\times \to K$ ($= N_{K_b^\times/K}$) is the norm, $N(x + y\sqrt{b}) = x^2 - by^2$ if $\sqrt{b} \notin K$; $N(x) = x$ if $K_b = K$.

Pf: Case 1: $\sqrt{b} = c \in K^\times$. Then $z^2 = ax^2 + by^2$ has $(0,1,c)$ as soln, so $(a,b) = 1$ $\forall a$ and $NK_b^\times = K^\times$ so ✓.

Case 2: $\sqrt{b} \notin K$. If $a \in NK_b^\times$, then $a = z^2 - by^2$ & $(1,y,z)$ solves our eqtn.

If $(a,b) = 1$, with soln $z^2 = ax^2 + by^2$, then $x \neq 0$ (else b a square), so $a = \frac{z^2 - by^2}{x^2} = N\left(\frac{z}{x} + \frac{y}{x}\sqrt{b}\right)$. ✓

Easy lemma: (i) $(a,b) = (b,a)$ $(a,c^2) = 1$ ✓

(ii) $(a,-a) = 1$ and $(a,1-a) = 1$ $(\forall a \neq 0,1)$ — $z^2 = ax^2 - ay^2$ has obv soln $(1,1,a)$; $z^2 = ax^2 + (1-a)y^2$ " $(1,1,1)$

(iii) $(a,b) = 1 \Rightarrow (aa',b) = (a',b)$ b/c $(a,b) = 1 \Rightarrow a \in NK_b^\times$, and $a' \in NK_b^\times$ iff $aa' \in NK_b^\times$

(iv) $(a,b) = (a,-ab) = (a,(1-a)b)$

[$(-a,a) = 1$ so $(-ab,a) = (b,a)$ by (iii). Else others].

(steps toward bilinearity, which is not obvious).

Thm ① If $K = \mathbb{R}$, $(a,b) = 1$ if a or $b > 0$. $(a,b) = -1$ if a and $b < 0$.

② If $K = \mathbb{Q}_p$, write $a = p^\alpha u$, $p^\beta v$ with $u, v \in \mathbb{Z}_p^\times$. Then

$$(a,b) = (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \text{if } p \neq 2$$

$$(a,b) = (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2} + \alpha\frac{v^2-1}{8} + \beta\frac{u^2-1}{8}} \quad \text{if } p = 2$$

③ $(a,b): K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \pm 1$ is a nondeg. symm. bil. form. (do a couple calc)

Cor: $b \notin (K^\times)^2 \Rightarrow [K^\times : NK_b^\times] = 2$

Pf: ① easy. ② uses Hensel's lemma: 3 cases: $(\alpha,\beta) = (0,0), (1,0), (1,1)$ $\left[(0,1) \leftrightarrow (1,0)\right]$

Take $p \neq 2$

Case (i) $\alpha = \beta = 0$. Want $(a,b) = 1$, ie $(u,v) = 1$, ie need to solve $z^2 - ux^2 - vy^2 = 0$. Since $(a,b) = (b,a)$ in $\mathbb{Q}_p^3$, (a,a,a). It has a non-zero solution in $\mathbb{F}_p$ (Ross sols: ux^2, vy^2 take $\frac{p+1}{2}$ values each, $x, y \in \mathbb{Z}/p$ so ~~their sums $ux^2 + vy^2$ take~~ $1 - ux^2$ and vy^2 take $\frac{p+1}{2}$ values each; these sets must overlap since $|\mathbb{Z}/p| = p$ (some set a soln w $z = 1$)). $\frac{\partial f}{\partial x} = -2ux$, $\frac{\partial f}{\partial y} = -2vy$, $\frac{\partial f}{\partial z} = 2z$, and at our soln $(x_0, y_0, 1)$, $v_p\left(\frac{\partial f}{\partial z}(\alpha)\right) = 0$ ($p \neq 2$), so we get a p-adic solution $\equiv (x_0, y_0, 1) \bmod p$ ∎

L4 #4 | Hilbert calc ctd

(ii) $\overset{\alpha=1\beta=0}{(pu,v)} = (p,v)$ (since $(u,v)=1 \Rightarrow$ (eq $(bu,v)=(b,v)\ \forall\ b$)

so need $(p,v)=\left(\frac{v}{p}\right)$. If v is a square in $\mathbb{Z}_p^\times$, both sides clearly 1.

If $v \notin (\mathbb{Z}_p^\times)^2$ then we claim $\left(\frac{v}{p}\right)=-1$. Indeed if $\alpha^2 \equiv v \bmod p$, then again by Hensel α lifts to $\tilde{\alpha} \in \mathbb{Z}_p$ s.t. $\tilde{\alpha}^2 = v$. Now check $(p,v)=-1$

Else $z^2 - px^2 - vy^2 = 0$ has a solution, hence a primitive solution

But then $\equiv$ considerations force $z, y \in \mathbb{Z}_p^\times$ (& thus $\left(\frac{v}{p}\right)=1$ by reducing)

(iii) $\overset{\alpha+\beta=1}{(pu,pv)} = (pu, -p^2uv) = (pu, -uv)$ (formula (ii) last page)

$\overset{\text{above}}{=} (p,-uv) = \left(\frac{-uv}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$, as desired.

$p=2$ is more intricate but uses the same ideas. Here is $\alpha=\beta=0$:

want $(u,v) = (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}}$ for $(u,v) \in \mathbb{Z}_2^\times$.

- $u \equiv 1 \bmod 4$ (or $v \equiv 1 \pmod 4$)
  - $u \equiv 1 \bmod 8$. Then $u \in (\mathbb{Z}_2^\times)^2$ (Hensel), so both sides are 1
  - $u \equiv 5 \bmod 8$. Then $u+4v \equiv 1 \pmod 8$, so $\omega^2 = u+4v$, $\omega \in \mathbb{Z}_2^\times$, and $z^2 - ux^2 - vy^2$ has $(\omega, 1, 2)$ as soln
- $u \equiv v \equiv 3 \bmod 4$. RHS $=-1$. Suppose $(u,v)=1$, so $z^2 = ux^2+vy^2$ has some primitive soln, hence $z^2 \equiv x^2+y^2 \equiv 0 \bmod 4$ has a soln w/ at least one a unit. Checking squares mod 4, all x,y,z even, contradicting primitive.

And so on.

---

(3) Non-degenerate bilinear follows directly from the formulas. (To show non-deg, $\forall\ a \in k^\times/(k^\times)^2$, $k^\times \setminus (k^\times)^2$, $\exists$ some b with $(a,b)=-1$. ☒ Do the previous exercise and find reps of $k^\times/(k^\times)^2$. For $K=\mathbb{Q}_p$, p odd, there are $1, p, u, pu$ where $u \in \mathbb{Z}_p^\times$ is not $\left(\frac{u}{p}\right)=-1$

So for $a = p, u, pu$, take $b = bu, p, u$ respectively

For $\mathbb{R}$ it is trivial.

For $\mathbb{Q}_2$ reps are $\{\pm 1, \pm 5, \pm 2, \pm 10\}$. Finding suitable b an exercise.

(e.g. for $a=2$ (0.5) $(5,2)=-1$ ...)

$a=-5$ $(-5,-1)=-1$ (w-1)

" $(-1)^{\frac{-5-1}{2}\cdot\frac{-1}{2}} + \left(\frac{(-1)^2-1}{8}\cdot\frac{-1}{2} + \frac{(-5)^2-1}{8}\cdot\frac{-1-1}{2}\right) = -1$

L4 #5 | Application: the local-global principle.

Let $V = \{\text{primes } p\} \cup \infty$. For $v \in V$, $\mathbb{Q}_v := \begin{cases} \mathbb{Q}_p & v = p \\ \mathbb{R} & v = \infty \end{cases}$

Thm For $a, b \in \mathbb{Q}^\times$, $\prod_{v \in V} (a,b)_v = 1$. ($(a,b)_v = 1$ for a.e. $v \in V$ and

- we'll show this is equivalent to QR

Pf: By bilinearity, STP for $a, b \in \{-1, \text{primes}\}$.

Key case: For $a = p$, $b = q$ distinct odd primes

$$\prod_{v \in V} (p,q)_v = (p,q)_2 (p,q)_p (p,q)_q \quad \text{(other } (p,q)_v = 1 \text{ since } p, q \text{ units in } \mathbb{Z}_v\text{)}$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \underbrace{\left(\frac{q}{p}\right)}_{(p,q)_p} \cdot \underbrace{\left(\frac{p}{q}\right)}_{(p,q)_q} \quad \text{— use the formula}$$

so the formula is equiv. to QR.

- For $a = p$, $b = 2$ distinct primes

$$\prod_{v \in V} (p,2)_v = \underbrace{(-1)^{\frac{p^2-1}{8}}}_{(p,2)_2} \cdot \underbrace{\left(\frac{2}{p}\right)}_{(p,2)_p}$$, so the formula is equiv. to the evaluation of $\left(\frac{2}{p}\right)$

- $a = p$ odd, $b = -1$ $\quad \prod_v (p,-1)_v = (-1)^{\frac{p-1}{2}(-1)} \cdot \left(\frac{-1}{p}\right)$, the formula for $\left(\frac{-1}{p}\right)$.
  $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (p,-1)_2 \qquad (p,-1)_p$

The remaining cases are easy exercises. (and are "elementary" from the formulas)

$\mathbb{Q}[\sqrt{b}] = L$

$\mathbb{Q}$

$\mathrm{rec}_{L/\mathbb{Q}} : \mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times N\mathbb{A}_L^\times \xrightarrow{\sim} \pm 1$

$\mathrm{rec}_{L/\mathbb{Q}}(x_v) = \prod \mathrm{rec}_{L_w/\mathbb{Q}_v}(x_v)$ (choose $w|v$)

$1 = \mathrm{rec}_{L/\mathbb{Q}}(a) = \prod \mathrm{rec}_{L_w/\mathbb{Q}_v}(a) = \prod (a,b)_v$ (loc-glob)

$\mathrm{rec}_{L_w/\mathbb{Q}_v} : \frac{\mathbb{Q}_v^\times}{N L_w^\times} \hookrightarrow \pm 1$

$(a,b)_v = 1 \Leftrightarrow a \in N L_w^\times \in \mathrm{rec}_{L_w/\mathbb{Q}_v}(a) = 1$

$\mathbb{Q}_v[\sqrt{b}]$

($L_w/\mathbb{Q}_v$ unr. and $a \in \mathbb{Z}_v^\times \Rightarrow a \in N\mathbb{Q}_v^\times$, so $(a,b)_v = 1$ for a.e. v)

Can we prove the thm w/o invoking QR? YES: it follows from a general property of the reciprocity map of GCFT.

(which goes by checking first for cyclotomic extensions & deducing for subexts, $\mathbb{Q}[\sqrt{p}]$ or $\mathbb{Q}[\sqrt{p^*}]$ in this case.