(memorable, if obscure) big *global* Theorem: The global norm residue symbol, the product of all local ones, ν, is a $k^\times$-invariant function on $\mathbb{J}$: it *factors through* $\mathbb{J}/k^\times$.

$$\Downarrow$$

Memorable theorem: For $a, b \in k^\times$, Hilbert reciprocity is

$$\Pi_v \ (a,b)_v \ = \ 1$$

$$\Downarrow$$

Quadratic Reciprocity ('main part'): For π and ϖ two elements of $\mathfrak{o}$ generating distinct odd prime ideals,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 \ = \ \Pi_v \, (\pi, \varpi)_v$$

where v runs over all *even or infinite* primes, and $(,)_v$ is the (quadratic) Hilbert symbol.

Next!!!

Primes lying over/under

Theorem: For $\mathfrak{O}$ *integral* over $\mathfrak{o}$ and prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there is at least one prime ideal $\mathfrak{P}$ of $\mathfrak{O}$ such that $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$.

That is, $\mathfrak{P}$ *lies over* $\mathfrak{p}$. $\mathfrak{P}$ is maximal if and only if $\mathfrak{p}$ is maximal.

Further, $\mathfrak{p} \cdot \mathfrak{O} \neq \mathfrak{O}$, keeping in mind that

$$\mathfrak{p} \cdot \mathfrak{O} \;=\; \{\sum_j p_j \cdot y_j \;:\; p_j \in \mathfrak{p},\; y_j \in \mathfrak{O}\}$$

There a natural commutative diagram

$$\begin{array}{ccc} \mathfrak{O} & \longrightarrow & \mathfrak{O}/\mathfrak{P} \\ \text{inj}\uparrow & & \uparrow\text{inj} \\ \mathfrak{o} & \longrightarrow & \mathfrak{o}/\mathfrak{p} \end{array}$$

We do not necessarily assume $\mathfrak{o}$ or $\mathfrak{O}$ is a domain.

Proof: This is easiest reduced to *local* questions.

The set $S = \mathfrak{o} - \mathfrak{p}$ is *multiplicative* because $\mathfrak{p}$ is prime. It is easy that $S^{-1}\mathfrak{O}$ is integral over $S^{-1}\mathfrak{o}$, and that $S^{-1}\mathfrak{o}$ has the unique maximal ideal $\mathfrak{m} = \mathfrak{p} \cdot S^{-1}\mathfrak{o}$.

To show $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, it suffices to consider the local version, and show $\mathfrak{m} \cdot S^{-1}\mathfrak{O} \neq S^{-1}\mathfrak{O}$, because

$$\mathfrak{p} \cdot S^{-1}\mathfrak{O} \;=\; \mathfrak{p} \cdot S^{-1}\mathfrak{o} \cdot S^{-1}\mathfrak{O} \;=\; \mathfrak{m} \cdot S^{-1}\mathfrak{O}$$

That is, it suffices to prove $\mathfrak{m} \cdot \mathfrak{O} \neq \mathfrak{O}$, with $\mathfrak{o}$ *local.*

For local $\mathfrak{o}$, if $\mathfrak{m} \cdot \mathfrak{O} = \mathfrak{O}$, then $1 \in \mathfrak{O}$ has an expression $1 = m_1 y_1 + \ldots + m_n y_n$, with $m_j \in \mathfrak{m}$ and $y_j \in \mathfrak{O}$. Let $\mathfrak{O}_1$ be the ring $\mathfrak{O}_1 = \mathfrak{o}[y_1, \ldots, y_n]$. It is a finitely-generated $\mathfrak{o}$-*algebra*, so by integrality is a finitely-generated $\mathfrak{o}$-*module.*

Nakayama's Lemma says that if $\mathfrak{a}M = M$ for an ideal contained in all maximal ideals of $\mathfrak{o}$, and M a finitely-generated $\mathfrak{o}$-module, then $M = \{0\}$.

Proof: (of Lemma) For M generated by $m_1, \ldots, m_n$, the hypothesis gives

$$m_1 \ = \ a_1 m_1 + \ldots + a_n m_n \qquad\qquad \text{(for some } a_j \in \mathfrak{a}\text{)}$$

$$(1 - a_1) m_1 \ = \ a_2 m_2 + \ldots + a_n m_n$$

Either $1 - a_1$ is a unit, or it is contained in some maximal ideal. But $\mathfrak{a}$ is contained in *all* maximal ideals, so $1 - a_1$ is a unit. Thus, m_1 is expressible in terms of the other generators. Induction proves the lemma. ///

Applying this to $\mathfrak{O}_1$ gives $\mathfrak{O}_1 \ = \ \{0\}$, contradiction. Thus, $\mathfrak{m} \cdot \mathfrak{O} \neq \mathfrak{O}$.

Reverting to not-necessarily-local $\mathfrak{o}$, in

$$\begin{array}{ccc} \mathfrak{O} & \longrightarrow & S^{-1}\mathfrak{O} \\ \uparrow & & \uparrow \\ \mathfrak{o} & \longrightarrow & S^{-1}\mathfrak{o} \end{array}$$

$\mathfrak{m} \cdot S^{-1}\mathfrak{O} \neq S^{-1}\mathfrak{O}$, so is in some maximal ideal $\mathfrak{M}$ of $S^{-1}\mathfrak{O}$, and $\mathfrak{M} \cap S^{-1}\mathfrak{o} \supset \mathfrak{m}$. By maximality of $\mathfrak{m}$, $\mathfrak{M} \cap S^{-1}\mathfrak{o} = \mathfrak{m}$.

$\mathfrak{M}$ is non-zero prime, so $\mathfrak{P} = \mathfrak{M} \cap \mathfrak{O}$ is prime, because intersecting a prime ideal with a subring gives a prime ideal. $\mathfrak{P}$ is not $\{0\}$, because of integrality: $0 \neq m \in \mathfrak{M}$ satisfies $m^n + a_{n-1}m^{n-1} + \ldots + a_o = 0$ with $a_i \in \mathfrak{o}$ and $0 \neq a_o \in \mathfrak{o} \cap \mathfrak{M}$. Then

$$\mathfrak{o} \cap \mathfrak{P} \;=\; \mathfrak{o} \cap (\mathfrak{O} \cap \mathfrak{M}) \;=\; \mathfrak{o} \cap \mathfrak{M} \;=\; \mathfrak{o} \cap (S^{-1}\mathfrak{o} \cap \mathfrak{M}) \;=\; \mathfrak{o} \cap \mathfrak{m} \;=\; \mathfrak{p}$$

Finally, prove $\mathfrak{P}$ maximal if and only if $\mathfrak{p}$ is.

For $\mathfrak{p}$ maximal, $\mathfrak{o}/\mathfrak{p}$ is a field, and $\mathfrak{O}/\mathfrak{P}$ is an integral domain, in any case. Show that an integral domain R *integral over* a field k is a field. Indeed, for $f(y) = 0$ minimal, with $a_i \in k$ and $0 \neq y \in R$, $k[y]$ is the field $k[Y]/\langle f(Y) \rangle$. In particular, y is invertible.

On the other hand, for $\mathfrak{P}$ maximal, the field $\mathfrak{O}/\mathfrak{P}$ is integral over $\mathfrak{o}/\mathfrak{p}$. If $\mathfrak{o}/\mathfrak{p}$ were not a field, it would have a maximal ideal $\mathfrak{m}$, which would be prime. By lying-over, there would be a prime of $\mathfrak{O}/\mathfrak{P}$ lying over $\mathfrak{m}$, impossible. Thus, $\mathfrak{p}$ is maximal. ///

Opportunistic calculation device: *If* $\mathfrak{O} = \mathfrak{o}[y]$, with y satisfying minimal (monic) $f(y) = 0$, have a bijection

$$\{\text{irreducible factors of } f \bmod \mathfrak{p}\} \longleftrightarrow \{\text{primes over } \mathfrak{p}\}$$

by

$$\text{factor } \overline{f}_j \text{ of } f(Y) \bmod \mathfrak{p} \quad \longrightarrow \quad \ker\Big(\mathfrak{O} \to \mathfrak{o}/\mathfrak{p}[Y] \,/\, \langle \overline{f}_j(Y)\rangle\Big)$$

Remark: For $\mathfrak{o}$ the ring of algebraic integers in a number field k (=integral closure of $\mathbb{Z}$ in k), it is *not* generally true that the integral closure $\mathfrak{O}$ of $\mathfrak{o}$ in a further finite extension K is of the form $\mathfrak{o}[y]$, although this *is true* for cyclotomic fields and some other examples.

Nevertheless, the *local* rings $S^{-1}\mathfrak{o}$ for $S = \mathfrak{o} - \mathfrak{p}$ *do have* the form $S^{-1}\mathfrak{O} = S^{-1}\mathfrak{o}[y]$ for almost all $\mathfrak{o}$, so the calculational device applies *almost everywhere locally.*

Proof: Localizing, reduce to $\mathfrak{p}$ maximal. As earlier,

$$\mathfrak{O} \longrightarrow \mathfrak{O}/\mathfrak{p} \approx \mathfrak{o}[y]/\mathfrak{p} \approx \mathfrak{o}[Y]\Big/\langle f(Y), \mathfrak{p}\rangle$$

$$\approx \mathfrak{o}/\mathfrak{p}[Y]\Big/\langle f(Y) \bmod \mathfrak{p}\rangle \approx \bigoplus_j \mathfrak{o}/\mathfrak{p}[Y]\Big/\overline{f}_j(Y)^{e_j}$$

where $\overline{f}_j$ are the distinct irreducible factors. Typically, the exponents e_j will be 1. In any case, this maps to $\mathfrak{o}/\mathfrak{p}[Y]/\overline{f}_j(Y)$, which is a *field*. Thus, the kernel is a maximal, hence prime, ideal $\mathfrak{P}$ containing $\mathfrak{p}$.

On the other hand, $\mathfrak{o}[y] = \mathfrak{O} \to \mathfrak{O}/\mathfrak{P}$ sends y to a root of some irreducible factor $\overline{f}_j$ of f mod $\mathfrak{p}$. Two roots of $\overline{f}$ are Galois-conjugate over $\mathfrak{o}/\mathfrak{p}$ if and only if they are roots of the same irreducible mod $\mathfrak{p}$. ///

Sun-Ze's theorem: For ideals $\mathfrak{a}_j$ in $\mathfrak{o}$ such that $\mathfrak{a}_i + \mathfrak{a}_j = \mathfrak{o}$ for $i \neq j$, given x_j, there is $x \in \mathfrak{o}$ such that $x = x_j \bmod \mathfrak{a}_j$ for all j.

Proof: The hypothesis gives $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. Then $x = x_2 a_1 + x_1 a_2$ solves the problem for two ideals.

Induction: for $j > 1$, let $b_j \in \mathfrak{a}_1$ and $c_j \in \mathfrak{a}_j$ such that $b_j + c_j = 1$. Then

$$1 \;=\; \prod_{j>1} (b_j + c_j) \;\in\; \mathfrak{a}_1 + \prod_{j>1} \mathfrak{a}_j$$

That is, $\mathfrak{a}_1 + \prod_{j>1} \mathfrak{a}_j \;=\; \mathfrak{o}$. Thus, there is $y_1 \;\in\; \mathfrak{o}$ such that $y_1 \;=\; 1 \bmod \mathfrak{a}_1$ and $y_1 \;=\; 0 \bmod \prod_{j>1} \mathfrak{a}_j$. Similarly, find $y_i \;=\; 1 \bmod \mathfrak{a}_i$ and $y_i \;=\; 0 \bmod \prod_{j \neq i} \mathfrak{a}_j$. Then $x \;=\; \sum_j x_j y_j$ is $x_i \bmod \mathfrak{a}_i$. ///

next:

Transitivity of Galois groups on primes lying over $\mathfrak{p}$

Let K/k be finite *Galois*, $\mathfrak{o}$ integrally closed in k, $\mathfrak{O}$ its integral closure in K. Let $\mathfrak{p}$ be prime in $\mathfrak{o}$. The Galois group $G = \mathrm{Gal}(K/k)$ is *transitive* on primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

...
