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

\[ \downarrow \]

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

\[ \Pi_v (a, b)_v = 1 \]

\[ \downarrow \]

Quadratic Reciprocity (‘main part’): For $\pi$ and $\varpi$ 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 $\mathcal{O}$ integral over $\mathfrak{o}$ and prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there is at least one prime ideal $\mathfrak{P}$ of $\mathcal{O}$ 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, $\mathfrak{p} \cdot \mathcal{O} \neq \mathcal{O}$, keeping in mind that

$$p \cdot \mathcal{O} = \left\{ \sum_j p_j \cdot y_j : p_j \in \mathfrak{p}, y_j \in \mathcal{O} \right\}$$

There a natural commutative diagram

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

We do not necessarily assume $\mathfrak{o}$ or $\mathcal{O}$ is a domain.
Proof: This is easiest reduced to \textit{local} questions.

The set $S = \mathfrak{o} - \mathfrak{p}$ is \textit{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 $\mathfrak{o}$ \textit{local}.

For local $\mathfrak{o}$, if $\mathfrak{m} \cdot \mathfrak{O} = \mathfrak{O}$, then $1 \in \mathfrak{O}$ has an expression

$$1 = m_1y_1 + \ldots + m_ny_n,$$

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 $\mathfrak{o}$-\textit{algebra}, so by integrality is a finitely-generated $\mathfrak{o}$-\textit{module}. 
Nakayama’s Lemma says that if $aM = M$ 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

$$m_1 = a_1 m_1 + \ldots + a_n m_n$$

(for some $a_j \in \mathfrak{a}$)

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

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
\[
\mathfrak{O} \longrightarrow S^{-1}\mathfrak{O} \\
\uparrow \quad \uparrow \\
\mathfrak{o} \longrightarrow S^{-1}\mathfrak{o}
\]

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

$\mathfrak{M}$ 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
\[
o \cap \mathfrak{P} = o \cap (\mathfrak{O} \cap \mathfrak{M}) = o \cap \mathfrak{M} = o \cap (S^{-1}\mathfrak{o} \cap \mathfrak{M}) = o \cap m = \mathfrak{p}
\]
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 $\mathcal{O} = \mathfrak{o}[y]$, with $y$ satisfying minimal (monic) $f(y) = 0$, have a bijection

\[
\{\text{irreducible factors of } f \bmod \mathfrak{p}\} \leftrightarrow \{\text{primes over } \mathfrak{p}\}
\]

by

\[
\text{factor } \overline{f_j} \text{ of } f(Y) \bmod \mathfrak{p} \quad \longrightarrow \quad \ker \left( \mathcal{O} \rightarrow \mathfrak{o}/\mathfrak{p}[Y]/\langle \overline{f_j}(Y) \rangle \right)
\]

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 $\mathcal{O}$ 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 $S^{-1}\mathcal{O} = S^{-1}\mathfrak{o}[y]$ for almost all $\mathfrak{o}$, so the calculational device applies almost everywhere locally.
Proof: Localizing, reduce to \( p \) maximal. As earlier,

\[
\mathcal{O} \rightarrow \mathcal{O}/p \approx \mathfrak{o}[y]/p \approx \mathfrak{o}[Y]/\langle f(Y), p \rangle
\]

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

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

On the other hand, \( \mathfrak{o}[y] = \mathcal{O} \rightarrow \mathcal{O}/\mathfrak{P} \) sends \( y \) to a root of some irreducible factor \( \overline{f}_j \) of \( f \mod p \). Two roots of \( \overline{f} \) are Galois-conjugate over \( \mathfrak{o}/p \) if and only if they are roots of the same irreducible mod \( p \).
Sun-Ze’s theorem: For ideals \( a_j \) in \( o \) such that \( a_i + a_j = o \) for \( i \neq j \), given \( x_j \), there is \( x \in o \) such that \( x = x_j \mod a_j \) for all \( j \).

Proof: The hypothesis gives \( a_1 \in a_1, a_2 \in a_2 \) 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 \( b_j \in a_1 \) and \( c_j \in a_j \) such that \( b_j + c_j = 1 \). Then
\[
1 = \prod_{j>1} (b_j + c_j) \in a_1 + \prod_{j>1} a_j
\]
That is, \( a_1 + \prod_{j>1} a_j = o \). Thus, there is \( y_1 \in o \) such that \( y_1 = 1 \mod a_1 \) and \( y_1 = 0 \mod \prod_{j>1} a_j \). Similarly, find \( y_i = 1 \mod a_i \) and \( y_i = 0 \mod \prod_{j \neq i} a_j \). Then \( x = \sum_j x_j y_j \) is \( x_i \mod a_i \). ///
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 \( G = \text{Gal}(K/k) \) is transitive on primes lying over \( \mathfrak{p} \) in \( \mathfrak{O} \).

...