Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
The Principal Ideal Theorem

Reference. Milne, section V.3 (but you won't find the proofs I've omitted there either); Neukirch, section VI.7 (see also IV.5); Lang, *Algebraic Number Theory*, section XI.5.

For a change, we're going to prove something, if only assuming the Artin reciprocity law which we haven't proved. Or rather, we're going to sketch a proof that you will fill in by doing the exercises. (Why should I have all the fun?)

The following theorem is due to Furtwängler, a student of Hilbert. (It's also called the "capitulation" theorem, because in the old days the word "capitulate" meant "to become principal". Etymology left to the reader.)

Theorem 1 (Principal ideal theorem). *Let L be the Hilbert class field of the number field K. Then every ideal of K becomes principal in L.*

(Warning: this does not mean that L has class number 1!) Example: if $K = \mathbb{Q}(\sqrt{-5})$, then $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$, and the nonprincipal ideal class of K is represented by $(2, 1+\sqrt{-5})$, which is generated by $1 + \sqrt{-1}$ in L.

The idea is that given Artin reciprocity, this reduces to a question in group theory. Namely, let M be the Hilbert class field of L; then an ideal of L is principal if and only if its image under the Artin map $I_L \to \mathrm{Gal}(M/L)$ is trivial. So what we need is to find a map V such that

$$\begin{tikzcd}
\mathrm{Cl}(K) \arrow[r] \arrow[d] & \mathrm{Gal}(L/K) \arrow[d, "V"] \\
\mathrm{Cl}(L) \arrow[r] & \mathrm{Gal}(M/L)
\end{tikzcd}$$

commutes, then show that V is the zero map. (The horizontal arrows are the Artin maps.)

Regarding the relationship between K, L and M:

(a) M is Galois over K (because its image under any element of $\mathrm{Gal}(\overline{K}/K)$ is still an abelian extension of L unramified at all finite and infinite places, so is contained in M) and unramified everywhere (since M/L and L/K are unramified).

(b) L is the maximal subextension of M/K which is abelian over K (since any abelian subextension is unramified over K, so contained in L).

Given a finite group G, let G^{ab} denote the maximal abelian quotient of G; that is, G^{ab} is the quotient of G by its commutator subgroup G'. Then (b) implies that $\mathrm{Gal}(M/L)$ is the commutator subgroup of $\mathrm{Gal}(M/K)$ and $\mathrm{Gal}(M/K)^{\mathrm{ab}} = \mathrm{Gal}(L/K)$.

Before returning to the principal ideal theorem, we need to do a bit of group theory. Let G be a finite group and H a subgroup (but not necessarily normal!). Let $g_1, \dots, g_n$ be left coset representatives of H in G: that is, $G = g_1 H \cup \cdots \cup g_n H$. For $g \in G$, put $\phi(g) = g_i$ if $g \in g_i H$ (i.e., $g_i^{-1} g \in H$). Put

$$V(g) = \prod_{i=1}^{n} \phi(gg_i)^{-1}(gg_i);$$

then $V(g)$ always lands in H. In particular, it induces a map $V : G \to H^{\mathrm{ab}}$.

Theorem 2. *The map $V : G \to H^{\mathrm{ab}}$ is a homomorphism, does not depend on the choice of the g_i, and induces a homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ (i.e., kills commutators in G).*

The map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is called the *transfer map* (in German, "Verlagerung", hence the V).

Now let's return to that diagram:

$$\begin{tikzcd}
\mathrm{Cl}(K) \arrow[r] \arrow[d] & \mathrm{Gal}(L/K) = \mathrm{Gal}(M/K)^{\mathrm{ab}} \arrow[d, "V"] \\
\mathrm{Cl}(L) \arrow[r] & \mathrm{Gal}(M/L) = \mathrm{Gal}(M/L)^{\mathrm{ab}}
\end{tikzcd}$$

and show that the transfer map V does actually make this diagram commute; it's enough to check this when we stick a prime $\mathfrak{p}$ of K in at the top left. For consistency of notation, put $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$, so that $G/H = \mathrm{Gal}(L/K)$. Choose a prime $\mathfrak{q}$ of L over $\mathfrak{p}$ and a prime $\mathfrak{r}$ of M over $\mathfrak{q}$, let $G_{\mathfrak{r}} \subseteq G$ be the decomposition group of $\mathfrak{r}$ over K (i.e., the set of automorphisms mapping $\mathfrak{r}$ to itself) and let $g \in G_{\mathfrak{r}}$ be the Frobenius of $\mathfrak{r}$. (Note: since G is not abelian, g depends on the choice of $\mathfrak{r}$, not just on $\mathfrak{q}$. I.e., there's no Artin map into G.)

Let $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ be the primes of L above K; then the image of $\mathfrak{p}$ in L is $\prod_i \mathfrak{q}_i$, and the image of that product under the Artin map is $\prod_i \mathrm{Frob}_{M/L}(\mathfrak{q}_i)$; we're trying to show this equals $V(g) = \prod_i \phi(gg_j)^{-1}gg_j$.

We do this by carefully picking the coset representatives g_i in the definition of V. Namely, decompose G as a union of double cosets $G_{\mathfrak{r}}\tau_i H$. Then the primes of L above $\mathfrak{p}$ correspond to these double cosets, where the double coset $G_{\mathfrak{r}}\tau_i H$ corresponds to $L \cap \mathfrak{r}^{\tau_i}$. Choose the left coset representatives of H by writing $G_{\mathfrak{r}}\tau_i H = \tau_i H \cup g\tau_i H \cup \cdots \cup g^{m-1}\tau_i H$ for each i, then using $g_{ij} = g^j \tau_i$ as the left coset representatives to define ϕ and V. (Here m is the order of $\mathrm{Frob}_{L/K}(\mathfrak{p})$.) Thus the equality $V(g) = \prod_i \mathrm{Frob}_{M/L}(\mathfrak{q}_i)$ follows from the following lemma.

Lemma 3. *If $L \cap \mathfrak{r}^{\tau_i} = \mathfrak{q}_i$, then $\mathrm{Frob}_{M/L}(\mathfrak{q}_i) = \prod_{j=0}^{m-1} \phi(gg_{ij})^{-1}gg_{ij}$.*

Thus the principal ideal theorem now follows from the following fact.

Theorem 4. *Let G be a finite group and H its commutator subgroup. Then the transfer map $V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is zero.*

Exercises.

1. Prove Theorem 2. (Hint: one approach to proving independence from choices is to change one g_i at a time. Also, show that $\phi(gg_1), \dots, \phi(gg_n)$ are a permutation of $g_1, \dots, g_n$.)

2. Prove Lemma 3.

3. Let $\mathbb{Z}[G]$ be the group algebra of G (formal linear combinations $\sum_{g \in G} n_g[g]$ with $n_g \in \mathbb{Z}$, multiplied by putting $[g][h] = [gh]$) and let I_G be the ideal of sums $\sum n_g[g]$ with $\sum n_g = 0$. Show that the following diagram commutes:

$$\begin{tikzcd} G/G' \arrow[r, "V"] \arrow[d, "\delta"] & G'/G'' \arrow[d, "\delta"] \\ I_G/I_G^2 \arrow[r, "S"] & (I_{G'} + I_G I_{G'})/I_G I_{G'} \end{tikzcd}$$

where the maps δ are induced by $g \mapsto [g] - 1$ and S is given by $S(x) = x \sum_h [h]$, for h running over a set of left coset representatives of G/H. Also, show that each δ is an isomorphism. (Hint: do the second part first. For more hints, see Neukirch, Lemma VI.7.7; but try it first before peeking!)

4. Prove Theorem 4. (Hint: quotient by the commutator subgroup of H to reduce to the case where H is abelian. Pick generators $g_1, \ldots, g_n$ of G, then write down an integer matrix m_{ij} of determinant G/H such that $\prod_{i=1}^n g_i^{m_{ij}} \in H$ for all j. Now apply δ to get relations in $\mathbb{Z}[G]/\mathbb{Z}[G]I_{G'}$. For more hints, see Neukirch, Theorem VI.7.6; again, try first before peeking.)