Norm Groups, Kummer Theory, and Profinite Cohomology

Last time, we proved the vanishing theorem, which we saw implied that for every finite Galois $G$-extension $L/K$, we have $(L^\times)^G \simeq \mathbb{Z}^G[-2]$, which, taking zeroth cohomology, implies $K^\times/\mathcal{N}L^\times \simeq G^{ab}$, which we note cannot be trivial because $G$ must be a solvable group. However, in the first lecture, we formulated a different theorem:

$$\text{Gal}(\overline{K}/K)^{ab} := \lim_{\leftarrow L/K} \text{Gal}(L/K)^{ab} \simeq \hat{K}^\times,$$

where the inverse limit is over finite Galois extensions $L/K$. Recall that

$$\hat{K}^\times := \lim_{\leftarrow [K \times \Gamma] < \infty} K^\times / \Gamma,$$

is the profinite completion of $K$, where $\Gamma$ is a finite-index closed subgroup of $K$ (this is the only reasonable way to define profinite-completion for topological groups). Thus, we’d like to show that

$$\lim_{\leftarrow L/K} K^\times/\mathcal{N}L^\times \simeq \lim_{\leftarrow \Gamma < \infty} K^\times/\Gamma,$$

with $L$ and $\Gamma$ as above.

**Definition 18.1.** A subgroup $\Gamma$ of $K^\times$ is a norm group (or norm subgroup) if

$\Gamma = \mathcal{N}L^\times$ for some finite extension $L/K$.

**Theorem 18.2 (Existence Theorem).** A subgroup $\Gamma$ of $K^\times$ is a norm group if and only if $\Gamma$ is closed and of finite index.

This clearly suffices to prove the statement of LCFT above.

**Remark 18.3.** A corollary of LCFT is that if $L/K$ is $G$-Galois, and $L/L_0/K$ is the maximal abelian subextension of $K$ inside $L$, then $NL^\times = NL_0^\times$. This is because

$$K^\times/\mathcal{N}L^\times \simeq G^{ab} \simeq K^\times/\mathcal{N}L_0^\times.$$

We’ll prove the existence theorem in the case $\text{char}(K) = 0$, though it is true in other cases (but the proof is more complicated).

**Lemma 18.4.** If $\Gamma \subseteq K^\times$ is a norm subgroup, then $\Gamma$ is closed and of finite index.

**Proof.** Let $L/K$ be an extension of degree $n$ such that $\Gamma = \mathcal{N}L^\times$. Then $\Gamma \supseteq \mathcal{N}_{L/K}K^\times = (K^\times)^n$, which we’ve seen is a finite-index closed subgroup (because it contains $1 + p^nK$ for all sufficiently large $n$), hence $\Gamma$ is as well. Note that if $\text{char}(K) > 0$, then $(K^\times)^n$ actually has infinite index in $K^\times$! \qed
The content of the existence theorem is thus that \( \pi^nZ(1 + p^n) \) is a norm subgroup for all \( n \); we’ve shown that norm subgroups are “not too small,” and now we need to show that we can make them “small enough.”

**Lemma 18.5.** If \( \Gamma' \) is a subgroup of \( K^\times \) such that \( K^\times \supseteq \Gamma' \supseteq \Gamma \) for a norm subgroup \( \Gamma \), then \( \Gamma' \) is a norm subgroup as well.

**Proof.** Let \( L/K \) be a finite extension such that \( \Gamma = \text{N}L/K^\times \). As before, we may assume that \( L/K \) is abelian. Then by lcft,

\[
\Gamma'/\Gamma \subseteq K^\times/NL^\times \simeq \text{Gal}(L/K)
\]

is a normal subgroup as \( \text{Gal}(L/K) \) is abelian by assumption. Thus, there exists some intermediate extension \( L'/K' \) with \( \Gamma'/\Gamma = \text{Gal}(L'/K') \), and

\[
K^\times/N(K')^\times = \text{Gal}(K'/K) = \text{Gal}(L/K)/\text{Gal}(L/K') = (K^\times/NL^\times)/(\Gamma'/\Gamma)
\]

canonicaly. Thus, \( \Gamma' = N(K')^\times \), which is the desired result.

Note that we have implicitly used the fact that following diagram commutes (for abelian extensions \( L/K \)) by our explicit setup of lcft:

\[
\begin{array}{ccc}
\text{Gal}(L/K) & \simeq & K^\times/NL^\times \\
\downarrow & & \downarrow \alpha \\
\text{Gal}(K'/K) & \simeq & K^\times/N(K')^\times.
\end{array}
\]

Since the inverse image of \( \Gamma'/\Gamma = \text{Ker}(\alpha) \) in \( K^\times \) is both \( \Gamma' \) and \( N(K')^\times \), we again obtain \( \Gamma' = N(K')^\times \). \( \Box \)

Now, a digression: in the second lecture, we said that \( K^\times/(K^\times)^2 \simeq \text{Gal}^\text{ab}(K)/2 \simeq \text{Hom}(K^\times/(K^\times)^2, \mathbb{Z}/2\mathbb{Z}) \), assuming char\((K) = 0 \) (in particular, not 2) and where the first isomorphism is via lcft. That is, \( K^\times/(K^\times)^2 \) is self-dual. Now we ask, how do we generalize this beyond \( n = 2 ? \) The answer is to use Kummer theory.

Recall that, assuming \( n \not| \text{char}(K) \) and that the group of \( n \)th roots of unity \( \mu_n \subseteq K^\times \) has order \( n \), we have

\[
K^\times/(K^\times)^n \simeq \text{Hom}_{\text{cts}}(\text{Gal}(K), \mu_n),
\]

where these are group homomorphisms. The upshot is that if \( K \) is also local, we’d expect that

\[
(18.1) \quad K^\times/(K^\times)^n \simeq \text{Hom}(K^\times/(K^\times)^n, \mu_n).
\]

Indeed, we have a map defined by

\[
K^\times/(K^\times)^n = \text{Hom}_{\text{cts}}(\text{Gal}(K), \mu_n)
= \text{Hom}_{\text{cts}}(\text{Gal}^\text{ab}(K), \mu_n)
= \text{Hom}_{\text{cts}} \left( \lim_{L/K} K^\times/NL^\times, \mu_n \right)
= \lim_{L/K} \text{Hom}(K^\times/NL^\times, \mu_n)
\hookrightarrow \text{Hom}_{\text{cts}}(K^\times, \mu_n)
\]
where the second equality is because all such maps must factor through the abelianization of Gal(K) (since \( \mu_n \) is abelian), the third is by lcft, and the fourth is by duality. Note that the inverse limits are over finite extensions \( L/K \), and that “continuous” (which is unnecessary when the domain is finite) here means that a map kills some compact open subgroup, justifying the injection above. We’d like to show that this map is also an isomorphism. Note that \( K^\times / (K^\times)^n \) is a finite abelian group and \( n \)-torsion; thus, it suffices to show that both sides have the same order.

**Claim 18.6.** Let \( A \) be an \( n \)-torsion finite abelian group. Then
\[
\#A = \# \text{Hom}(A, \mathbb{Z}/n\mathbb{Z}).
\]

**Proof.** \( A \) is a direct sum of groups \( \mathbb{Z}/d\mathbb{Z} \) for \( d | n \), so we may reduce to the case where \( A = \mathbb{Z}/d\mathbb{Z} \) for such a \( d \) (for the general case, direct sums and \( \text{Hom} \) commute). Then
\[
\text{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})[d]
\]
which has order \( d = \#A \), as desired. \( \Box \)

This shows that (18.1) is a canonical isomorphism (though the general statement of the claim alone shows that it is an isomorphism). In the \( n = 2 \) case, one can easily see that this is just the Hilbert symbol.

**Corollary 18.7.** If \( \mu_n \subseteq K \), then \( (K^\times)^n \) is a norm subgroup.

**Proof.** If we dualize our Kummer theory “picture,” we obtain the following commutative diagram:
\[
\begin{array}{cccc}
\text{Gal}(K) & \xrightarrow{c} & \text{Hom}(K^\times / (K^\times)^n, \mu_n) & \\
\downarrow & & & \\
K^\times & \overset{\alpha}{\xrightarrow{c}} & \lim_{L/K} K^\times / NL^\times & \xrightarrow{\beta} \text{Gal}^{\text{ab}}(K),
\end{array}
\]

where \( \alpha \) is continuous as an open subgroup inside the inverse limit is a norm subgroup, hence its inverse image in \( K^\times \) is a finite-index open subgroup. As we just saw, \( \text{Ker}(\beta \circ \alpha) = (K^\times)^n \), which is open (i.e., the full inverse image under the canonical projection maps of a subset of \( K^\times / NL^\times \) for some \( L/K \) in the inverse limit as the maps are continuous. Thus, by Lemma 18.5, \( (K^\times)^n \) is a norm subgroup.

Note that the map \( \beta \) above is surjective since it is realized as \( \text{Gal}^{\text{ab}}(K) \) modulo \( n \)th powers.

**Remark 18.8.** “A priori” (i.e., if we forgot about the order of each group), the kernel of this composition could be bigger than \( (K^\times)^n \). By arguing that the two were equal, we’ve produced a “small” norm subgroup.

**Proof (of Existence Theorem).** Let \( K \) be a general local field of characteristic 0. Let \( L := K(\zeta_n)/K \), where \( \zeta_n \) denotes the set of primitive \( n \)th roots of unity. Since \( (L^\times)^n \) is a norm subgroup in \( L^\times \) by Corollary 18.7, \( N(L^\times)^n = N((L^\times)^n) \subseteq K^\times \) is a norm subgroup in \( K^\times \). But \( N(L^\times)^n \subseteq (K^\times)^n \subseteq K^\times \), so Lemma 18.5 shows that \( (K^\times)^n \) is a norm subgroup in \( K^\times \).
Now, observe that for all \(N\), there exists some \(n\) such that
\[(O_K^\times)^n = (K^\times)^n \cap O_K^\times \subseteq 1 + p_K^N.
\]
Indeed, note that \((O_K^\times)^{q-1} \subseteq 1 + p_K^q\), where \(q = \#O_K/p_K\) (since the reduction mod \(p_K\) raised to the \((q-1)\)st power must be 1). Thus, for sufficiently large \(v(n)\) we have \((O_K^\times)^{(q-1)n} \subseteq 1 + p_K^{N}\), since in general \((1 + x)^n = 1 + nx + \cdots\) (where the ellipsis represents higher-order terms), and if \(v(n) \gg 0\) then all terms aside from 1 will be in \(p_K^N\).

As for finite-index subgroups “in the \(\mathbb{Z}\)-direction,” that is, where we restrict to multiples of \(\pi^N\), it suffices to simply replace \(n\) by \(nN\), so that only elements of valuation divisible by \(N\) are realized. Thus, every finite-index open subgroup of \(K^\times\) contains \((K^\times)^n\) for some \(n\), which is a norm subgroup as shown above, hence is itself a norm subgroup by Lemma 18.5. □

Let us now quickly revisit Kummer theory, which, as we will demonstrate, in fact says something very general about group cohomology. Let \(G\) be a profinite group, so that \(G = \lim \leftarrow G_i\) where the \(G_i\) are finite groups.

**Definition 18.9.** A \(G\)-module \(M\) is smooth if for all \(x \in M\), there exists a finite-index open subgroup \(K \subseteq G\) such that \(K \cdot x = x\).

**Example 18.10.** If \(G := \text{Gal}(\overline{K}/K)\), then \(G\) acts on both \(\overline{K}\) and \(\overline{K}^\times\), both of which are smooth \(G\)-modules. This is because every element of either \(G\)-module lies in some finite extension \(L/K\), hence fixed by \(\text{Gal}(\overline{K}/L)\) which is a finite-index open subgroup by definition.

Smoothness allows to reduce to the case of a finite group, from what is often a very complicated profinite group. We now must define a notion of group cohomology for profinite groups, as our original formulation was only for finite groups.

**Definition 18.11.** Let \(X\) be a complex of smooth \(G\)-modules bounded from below. Then
\[X^{\text{h}G} := \lim_{\leftarrow} \left( X^{K_i} \right)^{\text{h}G/K_i},\]
where \(K_i := \text{Ker}(G \to G_i)\) and \(X^{K_i}\) denotes the vectors stabilized (naively) by \(K_i\).

It’s easy to see that this forms a directed system. Note that \(G_i\) doesn’t act on \(X\), as it is only a quotient of \(G\), but it does act on the vectors stabilized by \(K_i\). The \(K_i\) are compact open subgroups of \(G\) that are decreasing in size. Taking “naive invariants” by \(K_i\) is worrisome, as it does not preserve quasi-isomorphism, but in fact we have the following:

**Claim 18.12.** If \(X\) is acyclic, then \(X^{\text{h}G}\) is too.

The proof is omitted, though we note that it is important that \(X\) is bounded from below. We have the following “infinite version” of Hilbert’s Theorem 90:

**Proposition 18.13.** If \(L/K\) is a (possibly infinite) \(G\)-Galois extension, then
\[H^1(G, L^\times) := H^1((L^\times)^{\text{h}G}) = 0.\]

**Proof.** We write \(L = \bigcup_i L_i\), where each \(L_i\) is a finite \(G_i\)-Galois extension of \(K\). Then by definition,
\[H^1(G, L^\times) = \lim_{\to}^n H^1(G_i, K_i^\times) = 0\]
Corollary 18.14. Let $G := \text{Gal}(\overline{K}/K)$ and $n$ be prime to $\text{char}(K)$. If $\mu_n \subseteq K$, then

$$K^\times / (K^\times)^n \simeq \text{Hom}_{cts}(G, \mu_n).$$

Proof. We have a short exact sequence of smooth $G$-modules

$$0 \to \mu_n \to K^\times \xrightarrow{x \mapsto x^n} K^\times \to 0.$$ 

The long exact sequence on cohomology then gives

$$0 \to \mu_n \to K^\times \xrightarrow{x \mapsto x^n} K^\times \to H^1(G, \mu_n) \to H^1(G, K^\times).$$

by Hilbert’s Theorem 90 (Proposition 18.13). Thus, $K^\times / (K^\times)^n \simeq H^1(G, \mu_n)$. Since $\mu_n \subseteq K$ as in the setting of Kummer theory, it is fixed by $G$; as we saw via cocycles, for the trivial group action we have $H^1(G, \mu_n) = \text{Hom}_{cts}(G, \mu_n)$, which gives the desired result.

Thus, we can actually derive Kummer theory very simply from abstract group cohomology and Hilbert’s Theorem 90.