Comments on subgroups of units

Let F be a number field, and let S be a finite set of places containing all archimedean ones. Consider the group of units $\mathcal{O}_F[\frac{1}{S}]^\times$. Intersecting with open compact subgroups U of $\widehat{\mathcal{O}}_F^\times$ defines so-called *congruent subgroups* $\mathcal{O}_F[\frac{1}{S}]^\times \cap U$ of $\mathcal{O}_F[\frac{1}{S}]^\times$.

Theorem 0.1. *All finite index subgroups of $\mathcal{O}_F[\frac{1}{S}]^\times$ are congruent subgroups.*

Remark: this generalizes to: for a torus T over F, all finite index subgroups of $T(\mathcal{O}_F[\frac{1}{S}])$ are congruent subgroups.

The proof we presented here follows Serre's paper: Serre, Sur les groupes de congruence des variétés abéliennes, which in my opinion, is a more systematic approach to the problem, although a bit longer.

For M a G_F-module, we introduce the following Galois cohomology group

$$H^1_S(G_F, M) := \mathrm{Ker}\left(H^1(G_F, M) \to \prod_{v \notin S} H^1(G_{F_v}, M)\right)$$

Lemma 0.1. *To prove Theorem 0.1, it suffices to show that, for each p, there exists r' such that $H^1_S(G_F, \mu_{p^r})$ is $p^{r'}$-torsion for every $r \geq r'$.*

Proof. We may enlarge S so that $\mathcal{O}_F[\frac{1}{S}]$ is a PID, or equivalently, the finite prime ideals in S generate the ideal class group $\mathrm{Cl}(F)$. We may also use finitely many places to deal with the torsion subgroups of $\mathcal{O}_F[\frac{1}{S}]$.

By Kummer theory,

$$H^1_S(G_F, \mu_{p^r}) \cong \mathrm{Ker}\left(F^\times/(F^\times)^{p^r} \to \prod_{v \notin S} F_v^\times/(F_v^\times)^{p^r}\right).$$

First, if each $H^1_S(G_F, \mu_{p^r})$ is zero (which is the case when $p \neq 2$ from our later discussions), then a global unit in $\mathcal{O}_F[\frac{1}{S}]^\times$ is a p^rth power if and only if it is a local p^rth power at each $v \notin S$. As $\mathcal{O}_F[\frac{1}{S}]^\times$ is a finitely generated abelian group, we in fact just need to use finitely many local congruence conditions to obtain the subgroup $(\mathcal{O}_F[\frac{1}{S}]^\times)^{p^r}$.

The general case is similar: our condition implies that, given $r \geq r'$, for a global element $x \in F^\times$, if x is locally (at places away from S) a p^rth power, then $x^{r'}$ is a p^rth power. The earlier argument still works because $\mathcal{O}_F[\frac{1}{S}]^\times$ is a finitely generated abelian group. □

Serre credited the following to Artin and Tate.

Definition 0.2. Let G be a profinite group, a *topologically monogenic closed subgroup* of G is a closed subgroup C of G, such that there exists $\gamma \in C$ such that $\gamma^{\mathbb{Z}}$ is dense in C. Or equivalently C is the closure of $\gamma^{\mathbb{Z}}$ for some $\gamma \in G$.

If M is an abelian group with continuous G-action, define

$$H^1_\bullet(G, M) := \mathrm{Ker}\left(H^1(G, M) \to \prod_{C} H^1(C, M)\right)$$

where the product runs over all topologically monogenic closed subgroups C of G.

In what follows, we will prove the following:

$$H^1_S(G_F, \mu_{p^r}) \subseteq H^1_\bullet(G_F, \mu_{p^r}) = \begin{cases} 0 & \text{if } p \neq 2 \\ \text{has order} \leq 2 & \text{if } p = 2. \end{cases}$$

Lemma 0.3. *Let U be a closed normal subgroup of G which acts trivially on M. Then the natural inclusion*

$$\mathrm{Inf} : H^1(G/U, M) \hookrightarrow H^1(G, M)$$

induces an isomorphism $H^1_\bullet(G/U, M) \cong H^1_\bullet(G, M)$.

Proof. We first show that Inf sends $H^1_\bullet(G/U, M)$ into $H^1_\bullet(G, M)$. If C is a topologically monogenic closed subgroup of G; its image $\overline{C}$ in G/U is still topologically monogenic and closed. So we have the following commutative diagram

$$\begin{array}{ccc} H^1(G/U, M) & \xrightarrow{\mathrm{Inf}} & H^1(G, M) \\ \downarrow & & \downarrow \\ H^1(\overline{C}, M) & \longrightarrow & H^1(C, M). \end{array}$$

From this, we see that an element $x \in H^1_\bullet(G/U, M)$ maps to zero in $H^1(\overline{C}, M)$ and thus $\mathrm{Inf}(x)$ maps to zero in $H^1(C, M)$.

Next, we show that $\mathrm{Inf} : H^1_\bullet(G/U, M) \to H^1_\bullet(G, M)$ is surjective. Let $f : G \to M$ be a cocycle in $H^1_\bullet(G, M)$. Since U acts trivially on M, $f|_U$ is a homomorphism $U \to M$. But each element $u \in U$ generates a topologically monogenic closed subgroup $\overline{u^{\mathbb{Z}}}$ of U, and our condition says that $f|_{\overline{u^{\mathbb{Z}}}}$ is the trivial cocycle *and thus a trivial homomorphism* as $\overline{u^{\mathbb{Z}}}$ acts trivially on M! From this, we deduce that $f(U) = 0$.

By restriction-inflation exact sequence (or just by hand), the map $f : G \to M$ factors through $\bar{f} : G/U \to M$. We need to show that $\bar{f}$ restricted to each topologically monogenic closed subgroup $\overline{C} \subset G/U$ is the trivial cocycle. Indeed, lift a topological generators $\bar{\gamma}$ to $\gamma \in G$, then $C := \overline{\gamma^{\mathbb{Z}}}$ maps surjectively onto $\overline{C}$. That $f|_C$ is the trivial cocycle implies that $\bar{f}|_{\overline{C}}$ is the trivial cocycle. So $\bar{f}$ belongs to $H^1_\bullet(G/U, M)$. □

Corollary 0.4. *In our number field case, $H^1_\bullet(G_F, \mu_{p^r}) \cong H^1_\bullet(\mathrm{Gal}(F(\mu_{p^r})/F), \mu_{p^r})$. In particular,*

1. *when $F(\mu_{p^r})/F$ is a cyclic extension, $H^1_\bullet(\mathrm{Gal}(F(\mu_{p^r})/F), \mu_{p^r})$ is zero;*
2. *when $p = 2$ and $F(\mu_{p^r})/F$ is not cyclic, $H^1_\bullet(\mathrm{Gal}(F(\mu_{2^r})/F), \mu_{2^r})$ has order at most 2.*

Proof. The isomorphism follows from applying the previous lemma with $U = G_{F(\mu_{p^r})}$.

(1) is clear from the definition.

(2) Say $\mathrm{Gal}(F(\mu_{2^r})/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r'}\mathbb{Z}$. In this case, we use inflation-restriction sequence

$$0 \to H^1(\mathbb{Z}/2, (\mu_{2^r})^{G_{F(\mu_4)}}) \to H^1(\mathrm{Gal}(F(\mu_{2^r})/F), \mu_{2^r}) \to H^1(\mathbb{Z}/2^{r'}\mathbb{Z}, \mu_{2^r})$$

As $H^1_\bullet(\mathrm{Gal}(F(\mu_{2^r})/F), \mu_{2^r})$ maps trivially to the last part, it is contained in $H^1(\mathbb{Z}/2, (\mu_{2^r})^{G_{F(\mu_4)}})$, which has order 2. □

Lemma 0.5. *Let F be a number field and S a finite set of places. Let M be any finite G_F-module. Then $H^1_S(G_F, M) \subseteq H^1_\bullet(G_F, M)$.*

Proof. By definite, each class $f \in H^1_S(G_F, M) \subseteq H^1(G_F, M)$ belongs to $H^1(G_F/U, M)$ for some open compact subgroup U of G_F (which we may assume to act trivially on M), corresponding to a finite Galois extension L/F.

Given a topologically monogenic closed subgroup C of G, say generated by γ. Let $\bar{\gamma}$ be the image of γ in $\mathrm{Gal}(L/F)$. By Chebaterov density theorem, there exists a place w of L above

a place $v \notin S$ of F that is unramified in L/F whose Frobenius element is $\bar{\gamma}$. In other words,

$$\mathrm{Gal}(L_w/F_v) \cong C \cdot U/U.$$

Now consider the following commutative diagram

$$\begin{array}{ccccc} H^1(\mathrm{Gal}(L/F), M) & & \xrightarrow{\quad\quad\mathrm{Inf}\quad\quad} & & H^1(\mathrm{Gal}_F, M) \\ \downarrow{\scriptstyle \mathrm{res}_v} & & & & \downarrow \\ H^1(\mathrm{Gal}(L_w/F_v), M) & \xrightarrow{\cong} & H^1(C \cdot U/U, M) & \xrightarrow{\mathrm{Inf}} & H^1(C, M) \end{array}$$

As the class f comes from a class in $H^1(\mathrm{Gal}(L/F), M)$ whose image under res_v is trivial. The restriction of f to $H^1(C, M)$ is also trivial. □

Theorem 0.1 follows from combining all ingredients above.

Remark 0.6. This proof appears to be longer than the one presented in terms of Grunwald-Wang's theorem, e.g. in Milne's book. But the upshot is that this proof is clearly generalizable to other situations, e.g. for algebraic tori over a number field F; or more generally, Serre considered the case when μ_{p^r} is replaced by $A[p^r]$ for an abelian variety over a number field, and proved that all finite index subgroups of $A(F)$ (which is a finitely generated abelian groups by Mordell–Weil Theorem) are congruent subgroups (given by open compact subgroups of $A(\widehat{\mathcal{O}}_F)$).

It is natural to ask whether finite index subgroups of integral points of an algebraic group are congruent subgroups (of course the Galois cohomolgical approach will not apply). This *fails* for $G = \mathrm{SL}_2$: there are finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which are NOT congruent subgroups. However, such property seems to hold when the semisimple group has rank > 1, by Margulis' arithmeticity theorem.

Remark 0.7. I do not know of other applications of the group $H^1_\bullet(G, M)$. As we already see, when $G = G_F$, this group $H^1_\bullet(G, M)$ tends to be very small or mostly zero.