Fujisaki's Compactness Lemma and corollaries:
finiteness of class number, Dirichlet units theorem

Fujisaki's lemma: $\mathbb{J}^1/k^\times$ is *compact.*

Corollary: The class number of $\mathfrak{o}$ is finite.

Let $k \otimes_{\mathbb{Q}} \mathbb{R} \approx \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. That is, k has r_1 *real* archimedean completions, and r_2 *complex* archimedean completions. The global degree is the sum of the local degrees: $[k:\mathbb{Q}] = r_1 + 2r_2$.

Corollary: *(Dirichlet's Units Theorem)* The unit group $\mathfrak{o}^\times$, modulo roots of unity, is a free $\mathbb{Z}$-module of rank $r_1 + r_2 - 1$.

Remark: It is amazing that these first two big theorems of general number theory, finiteness of class number, and the Units Theorem, follow from a *compactness* assertion.

Proof: Haar measure on $\mathbb{A} = \mathbb{A}_k$ and Haar measure on the (topological group) quotient $\mathbb{A}/k$ are inter-related by

$$\int_{\mathbb{A}} f(x)\,dx \;=\; \int_{\mathbb{A}/k} \sum_{\gamma\in k} f(\gamma + x)\,dx$$

Normalize the measure on $\mathbb{A}$ so that, mediated by this relation, $\mathbb{A}/k$ has measure 1.

We have the Minkowski-like claim, a measure-theory *pigeon-hole principle*, that a compact subset C of $\mathbb{A}$ with measure greater than 1 cannot *inject* to the quotient $\mathbb{A}/k$. Suppose, to the contrary, that C injects to the quotient. With f the characteristic function of C,

$$1 < \int_{\mathbb{A}} f(x)\,dx = \int_{\mathbb{A}/k} \sum_{\gamma\in k} f(\gamma + x)\,dx \le \int_{\mathbb{A}/k} 1\,dx = 1$$

with the last inequality by injectivity. Contradiction.

For *idele* α, we will see later that the change-of-measure on $\mathbb{A}$ is given conveniently by

$$\frac{\text{meas}\,(\alpha E)}{\text{meas}\,(E)} = |\alpha| \qquad\qquad \text{(for measurable } E \subset \mathbb{A}\text{)}$$

Given $\alpha \in \mathbb{J}^1$, we will adjust α by $k^\times$ to lie in a compact subset of $\mathbb{J}^1$. Fix compact $C \subset \mathbb{A}$ with measure > 1.

The topology on $\mathbb{J}$ is *strictly finer* than the subspace topology with $\mathbb{J} \subset \mathbb{A}$: the genuine topology is by imbedding $\mathbb{J} \to \mathbb{A} \times \mathbb{A}$ by $\alpha \to (\alpha, \alpha^{-1})$.

For $\alpha \in \mathbb{J}^1$, both αC and $\alpha^{-1}C$ have measure > 1, neither injects to the quotient $k\backslash\mathbb{A}$. So there are $x \neq y$ in k so that $x + \alpha C = y + \alpha C$. Subtracting,

$$0 \neq a = x - y \in \alpha(C - C) \cap k$$

That is,

$$a \cdot \alpha^{-1} \in C - C$$

Likewise, there is $0 \neq b \in \alpha^{-1}(C - C) \cap k$, and $b \cdot \alpha \in C - C$. There is an obvious constraint

$$ab = (a \cdot \alpha)(b \cdot \alpha^{-1}) \in (C - C)^2 \cap k^\times = \text{compact} \cap \text{discrete} \;=\; \text{finite}$$

Let $\Xi = (C - C)^2 \cap k^\times$ be this finite set. Paraphrasing: given $\alpha \in \mathbb{J}^1$, there are $a \in k^\times$ and $\xi \in \Xi$ ($\xi = ab$ above) such that $(a \cdot \alpha^{-1},\ (a \cdot \alpha^{-1})^{-1}) \in (C - C) \times \xi^{-1}(C - C)$.

That is, α^{-1} can be adjusted by $a \in k^\times$ to be in the compact $C - C$, and, simultaneously, for one of the finitely-many $\xi \in \Xi$, $(a \cdot \alpha^{-1})^{-1} \in \xi \cdot (C - C)$.

In the topology on $\mathbb{J}$, for each $\xi \in \Xi$,

$$\Big((C - C) \times \xi^{-1}(C - C)\Big) \cap \mathbb{J} \;=\; \text{compact in } \mathbb{J}$$

The continuous image in $\mathbb{J}/k\times$ of each of these finitely-many compacts is compact. Their union covers the *closed* subset $\mathbb{J}^1/k^\times$, so the latter is compact. ///

Proof of finiteness of class number: Let i be the *ideal map* from ideles to non-zero fractional ideals of the integers $\mathfrak{o}$ of k. That is,

$$i(\alpha) \;=\; \prod_{v<\infty} \mathfrak{p}_v^{\mathrm{ord}_v \alpha} \qquad\qquad (\text{for } \alpha \in \mathbb{J})$$

where $\mathfrak{p}_v$ is the prime ideal in $\mathfrak{o}$ attached to the place v. Certainly the subgroup $\mathbb{J}^1$ of $\mathbb{J}$ still surjects to the group of non-zero fractional ideals. The kernel in $\mathbb{J}$ of the ideal map is

$$G \;=\; \prod_{v|\infty} k_v^\times \;\times\; \prod_{v<\infty} \mathfrak{o}_v^\times$$

and the kernel on $\mathbb{J}^1$ is $G^1 \;=\; G \cap J^1$. The principal ideals are the image $i(k^\times)$. The map of $\mathbb{J}^1$ to the ideal class group factors through the idele class group $\mathbb{J}^1/k^\times$, noting as usual that the product formula implies that $k^\times \subset \mathbb{J}^1$.

G^1 is open in $\mathbb{J}^1$, so its image K in the quotient $\mathbb{J}^1/k^\times$ is open, since quotient maps are open. The cosets of K cover $\mathbb{J}^1/k^\times$, and by compactness there is a finite subcover. Thus, $\mathbb{J}^1/k^\times K$ is finite, and this finite group is the ideal class group. ///

A continuation proves the units theorem!

Since K is open, its cosets are open. Thus, K is closed. Since $\mathbb{J}^1/k^\times$ is Hausdorff and compact, K is compact. That is, we have compactness of

$$K \;=\; (G^1 \cdot k^\times)/k^\times \;\approx\; G^1/(k^\times \cap G^1) \;=\; G^1/\mathfrak{o}^\times$$

with the global units $\mathfrak{o}^\times$ imbedded on the diagonal.

Since $\prod_{v<\infty} \mathfrak{o}_v^\times$ is compact, its image U under the continuous map to $G^1/\mathfrak{o}^\times$ is compact. By Hausdorff-ness, the image U is closed. Thus, we can take a further (Hausdorff) quotient by U,

$$G^1/(U \cdot \mathfrak{o}^\times) \;=\; \text{compact}$$

With $k_\infty^1 = \{\alpha \in \prod_{v|\infty} k_v^\times \;:\; \prod_v |\alpha_v|_v = 1\}$,

$$k_\infty^1/\mathfrak{o}^\times \;\approx\; G^1/(U \cdot \mathfrak{o}^\times) \;=\; (\text{compact})$$

This compactness is essentially the units theorem! (See below...) ///

Remark: To compare with the classical formulation, one wants the accompanying result that a *discrete* subgroup L of $\mathbb{R}^n$ with $\mathbb{R}^n/L$ is *compact* is a free $\mathbb{Z}$-module on n generators.

Generalized ideal class numbers:

The class number above is the *absolute* class number.

An element $\alpha \in k$ is *totally positive* when $\sigma(\alpha) > 0$ for every *real* imbedding $\sigma : k \to \mathbb{R}$. For example, $2 + \sqrt{2}$ is totally positive, while $1 + \sqrt{2}$ is *not*.

The *narrow* class number is ideals modulo principal ideals generated by *totally positive* elements.

Congruence conditions can be imposed at *finite* places: given an ideal $\mathfrak{a}$, we can form an ideal class group of ideals modulo principal ideals possessing generators $\alpha = 1 \bmod \mathfrak{a}$, for example.

Positivity conditions can be combined with *congruence* conditions: *generalized ideal class groups* are quotients of (fractional) ideals by principal ideals meeting the positivity and congruence constraints. The ideal class groups corresponding to conditions $\alpha = 1 \bmod \mathfrak{a}$ are called *ray class groups*.

Proposition: Generalized ideal class groups are presentable as *idele* class groups, specifically, as quotients of $\mathbb{J}^1/k^\times$ by *open* subgroups. [Proof later]

Corollary/Theorem: Generalized ideal class groups are *finite.*

Proof: First, note that an *open* subgroup of a topological group is also *closed*, because it the *complement* of the union of its cosets *not* containing the identity.

For U be an open subgroup of a *compact* abelian topological group K (such as $\mathbb{J}^1/k^\times$), K/U is *finite*, because the cover of K by (disjoint!) cosets of U has a *finite* subcover. Thus, K/U is *finite.* It is Hausdorff because U is also *closed.* ///

Remark: The ray class groups with total-positivity thrown in are visibly *cofinal* in the collection of all generalized ideal class groups.

Generalized units:

Let S be a finite collection of places of k, including all archimedean places. The S-integers $\mathfrak{o}_S$ in k are

$$\mathfrak{o}_S \;=\; k \cap \Big(\prod_{v \in S} k_v \times \prod_{v \notin S} \mathfrak{o}_v\Big) \;=\; \{\alpha \in k : \alpha \text{ is } v\text{-integral for } v \notin S\}$$

The group of S-units is $\mathfrak{o}_S^\times = k^\times \cap \big(\prod_{v \in S} k_v^\times \times \prod_{v \notin S} \mathfrak{o}_v^\times\big)$

Theorem: *(Generalized Units Theorem)* $\mathfrak{o}_S^\times$ modulo roots of unity is free of rank $|S| - 1$.

[Proof...]