FUJISAKI'S LEMMA, AFTER WEIL

This writeup is modeled closely on a writeup by Paul Garrett.

Let k be a number field. Let $\mathbb{A}$ be the adele ring of k, let $\mathbb{J} = \mathbb{A}^\times$ be the idele group, and let $\mathbb{J}^1 = \{a \in \mathbb{J} : |a| = 1\}$ be the group of norm-1 ideles.

Fujisaki's Lemma. *The quotient* $k^\times \backslash \mathbb{J}^1$ *is compact.*

The first section to follow will give the main proof of Fujisaki's Lemma. However, the main proof relies on a description of the idele topology that may be unfamiliar, and so the second section will explain the natural topology on the unit subgroup of a topological ring, encompassing the idele topology.

1. Proof of Fujisaki's Lemma

Give $\mathbb{A}$ a measure μ. Take a compact set

$$C_o \subset \mathbb{A}, \qquad \mu(C_o) > \mu(k\backslash\mathbb{A}).$$

We show the Minkowski-like result that the natural quotient map

$$\mathbb{A} \longrightarrow k\backslash\mathbb{A}, \quad x \longmapsto k + x$$

is not injective on C_o. Indeed, suppose instead that the quotient map is injective on C_o. Then for any $\overline{x} \in k\backslash\mathbb{A}$ and for any distinct $\gamma, \gamma' \in k$, $\gamma + x$ and $\gamma' + x$ can not both lie in C_o. Let f be the characteristic function of C_o, and compute that consequently

$$\mu(C_o) = \int_{\mathbb{A}} f(x)\,dx = \int_{k\backslash\mathbb{A}} \sum_{\gamma\in k} f(\gamma + x)\,d\overline{x} \le \int_{k\backslash\mathbb{A}} d\overline{x} = \mu(k\backslash\mathbb{A}).$$

The display contradicts the fact that $\mu(C_o) > \mu(k\backslash\mathbb{A})$, and so injectivity on C_o is untenable.

Consider any norm-1 k-idele

$$a \in \mathbb{J}^1.$$

The associated change of measure on $\mathbb{A}$ is trivial, $d(ax) = |a|\,dx = dx$. It follows that $\mu(aC_o) > \mu(k\backslash\mathbb{A})$, and $\mu(a^{-1}C_o) > \mu(k\backslash\mathbb{A})$ similarly. By the previous paragraph, there exist distinct $x, y \in C_o$ such that $ax - ay \in k$, and the same statement holds with a^{-1} in place of a. With this in mind, define the set

$$C = C_o - C_o = \{x - y : x, y \in C_o\}.$$

We have just argued that $aC \cap k^\times$ and $a^{-1}C \cap k^\times$ are nonempty. Elementwise, there exist $\tilde{c}, c \in C$ and $\tilde{\alpha}, \alpha \in k^\times$ such that

$$a\tilde{c} = \tilde{\alpha}^{-1}, \quad a^{-1}c = \alpha^{-1}.$$

It follows that the quantity $\alpha^{-1}\tilde{\alpha}^{-1} = c\tilde{c}$ lies in the set

$$S = k^\times \cap (C \cdot C).$$

The set S is the intersection of discrete set and a compact set, making it finite. Also, S is independent of a. Since $c\tilde{c} \in S$ it follows that $c^{-1} \in C \cdot S^{-1}$. To summarize so far, we have shown that given $a \in \mathbb{J}^1$, there exist α and c such that

$$a = \alpha c, \qquad \alpha \in k^\times, \quad (c, c^{-1}) \in C \times C \cdot S^{-1}.$$

Let H denote the adelic hyperbola,

$$H = \{(x, x^{-1}) : x \in \mathbb{A}^\times\},$$

endowed with the subspace topology from $\mathbb{A} \times \mathbb{A}$. Since the set $C \times C \cdot S^{-1}$ is compact in $\mathbb{A} \times \mathbb{A}$, the intersection $K_o = (C \times C \cdot S^{-1}) \cap H$ is compact in H. By the nature of the idele topology (to be explained in the next section), this means precisely that the set of first coordinates of K_o-points,

$$K = \{c \in \mathbb{A}^\times : (c, c^{-1}) \in K_o\},$$

is compact in $\mathbb{A}^\times$, Now the summary at the end of the previous paragraph says that given $a \in \mathbb{J}^1$, there exist α and c such that

$$a = \alpha c, \qquad \alpha \in k^\times, \quad c \in K.$$

So the continuous map

$$K \longrightarrow k^\times \backslash \mathbb{J}^1, \quad c \longmapsto k^\times c$$

surjects, showing that the quotient is compact.

2. The Unit Topology

To justify the description of the idele topology from a moment ago, we work in slightly more generality. The ideles are the unit group of the adeles, a topological ring.

Let R be an associative ring with identity, and let U denote its unit group, i.e., the multiplicative group of the multiplicatively invertible elements of R. Suppose further that R is a topological ring, meaning that its underlying set is endowed with a topology, and that addition and multiplication are continuous on R under the topology. This makes additive inversion continuous as well. The multiplicative subgroup U inherits a topology from R. Under this topology, the restriction of multiplication to U is automatically continuous, but multiplicative inversion on U need not be. So the question is:

> *Given the topology on R, what topology naturally should be put on U to make multiplicaton and inversion continuous*?

Again, the answer is not the subspace topology that U inherits from R.

To answer the question, define

$$\begin{aligned} P &= R \times R && (P \text{ stands for } \textit{product}), \\ H &= \{(u, u^{-1}) : u \in U\} \subset P && (H \text{ stands for } \textit{hyperbola}). \end{aligned}$$

Identify the unit group U and the hyperbola H as follows,

$$u \longleftrightarrow (u, u^{-1}).$$

Since R has a topology, the product $P = R \times R$ carries the product topology. The hyperbola H inherits a topology from P. The unit group thus acquires a topology from H via their identification. This topology on U is the unit group topology. We next discuss it.

The unit topology on U is at least as fine as the subspace topology. Indeed, letting $\pi_1 : P \longrightarrow R$ be $\pi_1(x,y) = x$, the composition

$$U_{\text{unit}} \longrightarrow H \xrightarrow{\pi_1} U_{\text{subspace}}$$

is the identity as a set-map and is continuous.

Any topology on U that is at least as fine as the subspace topology and makes inversion continuous is at least as fine as the unit topology. To see this, let $\widetilde{U}$ denote the set U with a topology that is at least as fine as the subspace topology and makes inversion continuous. Then the map

$$\widetilde{U} \longrightarrow H, \quad u \longmapsto (u, u^{-1})$$

is continuous, giving the desired result.

Summarizing so far: The unit topology is the unique candidate topology to refine the subspace topology just enough to make inversion on U continuous while keeping multiplication on U continuous as well.

Inversion is continuous on U under the unit topology. This fact is essentially instant from the definition. Inversion on U is the map

$$u \longmapsto u^{-1}.$$

So on the copy H of U, inversion is the map

$$(u, u^{-1}) \longmapsto (u^{-1}, u).$$

But this map is the restriction to H of the coordinate-exchange map on P,

$$(r, \tilde{r}) \longmapsto (\tilde{r}, r).$$

The coordinate-exchange map on P is certainly continuous. Hence so is the inversion map on U.

Finally, multiplication is continuous on U under the unit topology. Because the unit topology refines the subspace topology, this fact is not automatic. To see that it is true nonetheless, first note that the product $H \times H$ can be identified with the subspace $H \times H$ of $P \times P$. (It is best to forget for the moment that P itself is again a product.) This is easily seen by checking that the two spaces have the same basis.

Now, since multiplication on P,

$$P \times P \longrightarrow P, \quad \big((x,y),(z,w)\big) \longmapsto (xz, yw),$$

is continuous, so is its restriction to H,

$$H \times H \longrightarrow H, \quad \big((u,u^{-1}),(\tilde{u},\tilde{u}^{-1})\big) \longmapsto (u\tilde{u}, u^{-1}\tilde{u}^{-1}),$$

viewing $H \times H$ as a subspace of $P \times P$. But also we may view $H \times H$ as a product in the previous display, and then it follows that the restriction to first coordinates,

$$U \times U \longrightarrow U, \quad (u, \tilde{u}) \longmapsto u\tilde{u},$$

is again continuous.