LOCAL AND GLOBAL ANALYSIS

Garth Warner

Department of Mathematics

University of Washington

The objective of this book is to give an introduction to p-adic analysis along the lines of Tate's thesis, as well as incorporating material of a more recent vintage, for example Weil groups.

CONTENTS

§1. *ABSOLUTE VALUES*

1: DEFINITION Let F be a field -- then an absolute value (a.k.a. a valuation of order 1) is a function

$$|.|:F \to R_{\geq 0}$$

satisfying the following conditions.

AV-1 $|a| = 0 \iff a = 0$.

AV-2 $|ab| = |a||b|$.

AV-3 $\exists$ M > 0:

$$|a + b| \leq M \sup(|a|, |b|).$$

2: EXAMPLE Let F = R or C with the usual absolute value $|.|_\infty$ -- then one can take M = 2.

3: DEFINITION The trivial absolute value is defined by the rule

$$|a| = 1 \ \forall \ a \neq 0.$$

4: LEMMA If $|.|$ is an absolute value, then

$$|1| = 1.$$

5: APPLICATION If $a^n = 1$, then

$$|a^n| = |a|^n = |1| = 1$$

$$\Rightarrow |a| = 1.$$

6: RAPPEL Let G be a cyclic group of order $r < \infty$ -- then the order of any subgroup of G is a divisor of r and if $n|r$, then G possesses one and only one subgroup of order n (and this subgroup is cyclic).

7: RAPPEL Let G be a cyclic group of order $r < \infty$ — then the order of $x \in G$ is, by definition, $\#\langle x \rangle$, the latter being the smallest positive integer n such that $x^n = 1$.

8: SCHOLIUM Every absolute value on a finite field F_q is trivial.

[In fact, $F_q^\times$ is cyclic of order $q - 1$.]

9: DEFINITION Two absolute values $|\cdot|_1$, $|\cdot|_2$ on a field F are equivalent if $\exists\, r > 0$:

$$|\cdot|_2 = |\cdot|_1^r.$$

[Note: Equivalence is an equivalence relation.]

10: N.B. If $|\cdot|$ is an absolute value, then so is $|\cdot|^r$ $(r > 0)$, the M per $|\cdot|$ being M^r per $|\cdot|^r$.

11: LEMMA Every absolute value is equivalent to one with $M \leq 2$.

PROOF Assume from the beginning that $M > 2$, hence

$$M^r \leq 2 \quad (r > 0)$$

if

$$r \log M \leq \log 2$$

or still, if

$$r \leq \frac{\log 2}{\log M} \quad (< 1).$$

12: DEFINITION An absolute value $|.|$ satisfies the triangle inequality if

$$|a + b| \le |a| + |b|.$$

13: LEMMA Suppose given a function $|.|:F \to R_{\ge 0}$ satisfying AV-1 and AV-2 -- then AV-3 holds with $M \le 2$ iff the triangle inequality obtains.

PROOF Obviously, if

$$|a + b| \le |a| + |b|,$$

then

$$|a + b| \le 2 \sup(|a|,|b|).$$

In the other direction, by induction on m,

$$\left|\sum_{k=1}^{2^m} a_k\right| \le 2^m \sup_k |a_k| \quad (1 \le k \le 2^m).$$

Next, given n choose m: $2^m \ge n > 2^{m-1}$, so upon inserting 2^m-n zero summands,

$$\left|\sum_{k=1}^{n} a_k\right| \le M \sup\left(\left|\sum_{k=1}^{2^{m-1}} a_k\right|, \left|\sum_{k=2^{m-1}+1}^{2^m} a_k\right|\right)$$

$$\le 2 \sup\left(\left|\sum_{k=1}^{2^{m-1}} a_k\right|, \left|\sum_{k=2^{m-1}+1}^{2^{m-1}+2^{m-1}} a_k\right|\right)$$

$$\le 2 \sup\left(2^{m-1} \sup_{k \le 2^{m-1}} |a_k|, 2^{m-1} \sup_{k > 2^{m-1}} |a_k|\right)$$

$$\le 2 \cdot 2^{m-1} \sup_{1 \le k \le n} |a_k| \le 2 \cdot n \sup_{1 \le k \le n} |a_k|.$$

I.e.:

$$\left|\sum_{k=1}^{n} a_k\right| \le 2n \sup_{1\le k\le n} |a_k| \le 2n \sum_{k=1}^{n} |a_k|.$$

In particular:

$$\left|\sum_{k=1}^{n} 1\right| = |n| \le 2n.$$

Finally,

$$\begin{aligned}
|a + b|^n &= |(a + b)^n| \quad \text{(AV-2)} \\
&= \left|\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right| \\
&\le 2(n+1) \sum_{k=0}^{n} \left|\binom{n}{k} a^k b^{n-k}\right| \\
&= 2(n+1) \sum_{k=0}^{n} \left|\binom{n}{k}\right| |a^k b^{n-k}| \quad \text{(AV-2)} \\
&\le 2(n+1)2 \sum_{k=0}^{n} \binom{n}{k} |a^k b^{n-k}| \\
&= 4(n+1)(|a| + |b|)^n
\end{aligned}$$

=>

$$\begin{aligned}
|a + b| &\le 4^{1/n}(n+1)^{1/n}(|a| + |b|) \\
&\to (|a| + |b|) \quad (n \to \infty).
\end{aligned}$$

14: SCHOLIUM Every absolute value is equivalent to one that satisfies the triangle inequality.

15: DEFINITION A place of F is an equivalence class of nontrivial absolute values.

Accordingly, every place admits a representative for which the triangle inequality is in force.

16: DEFINITION An absolute value $|.|$ is non-archimedean if it satisfies the ultrametric inequality:

$$|a + b| \leq \sup(|a|,|b|) \quad (\text{so } M = 1).$$

17: N.B. A non-archimedean absolute value satisfies the triangle inequality.

18: LEMMA Suppose that $|.|$ is non-archimedean and let $|b| < |a|$ -- then

$$|a + b| = |a|.$$

PROOF

$$|a| = |(a + b) - b| \leq \sup(|a + b|,|b|)$$

$$= |a + b|$$

since $|a| \leq |b|$ is untenable. Meanwhile,

$$|a + b| \leq \sup(|a|,|b|) = |a|.$$

19: EXAMPLE Fix a prime p and take $F = Q$. Given a rational number $x \neq 0$, write

$$x = p^k \frac{m}{n} \quad (k \in Z),$$

where $p \nmid m$, $p \nmid n$, and then define the <u>p-adic absolute value</u> $|\cdot|_p$ by the prescription

$$|x|_p = p^{-k} \quad (|0|_p = 0).$$

[AV-1 is obvious. To check AV-2, write

$$x = p^k \frac{m}{n}, \quad y = p^\ell \frac{u}{v},$$

where m,n,u,v are coprime to p -- then

$$xy = p^{k+\ell} \frac{mu}{nv}$$

=>

$$|xy|_p = p^{-(k+\ell)} = p^{-k}p^{-\ell} = |x|_p \; |y|_p.$$

As for AV-3, $|\cdot|_p$ satisfies the ultrametric inequality. To establish this, assume without loss of generality that $k \le \ell$ and write

$$x + y = p^k\left(\frac{m}{n} + p^{\ell-k} \frac{u}{v}\right)$$

$$= p^k \frac{mv + p^{\ell-k}nu}{nv}.$$

- $|x|_p \neq |y|_p$, so $\ell - k > 0$, hence

$$mv + p^{\ell-k}nu$$

is coprime to p (otherwise

$$mv = p^r N - p^{\ell-k}nu \quad (r \ge 1)$$

$$= p(p^{r-1}N - p^{\ell-k-1}nu) \Rightarrow p|mv)$$

=>

$$|x + y|_p = p^{-k}$$

$$= |x|_p = \sup(|x|_p, |y|_p),$$

since

$$\ell - k > 0 \Rightarrow p^{-\ell} < p^{-k}$$

$$\Rightarrow |y|_p < |x|_p.$$

- $|x|_p = |y|_p$, so $\ell = k$, hence

$$mv + nu = p^r N \quad (r \geq 0) \quad (p \nmid N)$$

=>

$$x + y = p^{k+r} \frac{N}{nv}$$

=>

$$|x + y|_p = p^{-k-r}.$$

And

$$p^{-k-r} \leq \begin{cases} p^{-k} = |x|_p \\ \\ p^{-k} = |y|_p \end{cases}$$

=>

$$|x + y|_p \leq \sup(|x|_p, |y|_p).]$$

<u>20:</u> REMARK It can be shown that every nontrivial absolute value on Q is equivalent to a $|.|_p$ for some p or to $|.|_\infty$.

<u>21:</u> LEMMA $\forall\, x \in Q^{\times}$,

$$\prod_{p\leq\infty} |x|_p = 1,$$

all but finitely many of the factors being equal to 1.

PROOF Write

$$x = \pm\, p_1^{k_1} \cdots p_n^{k_n} \quad (k_1,\ldots,k_n \in Z)$$

for pairwise distinct primes p_j -- then $|x|_p = 1$ if p is not equal to any of the p_j. In addition,

$$|x|_{p_j} = p_j^{-k_j}, \quad |x|_\infty = p_1^{k_1} \cdots p_n^{k_n}$$

=>

$$\prod_{p\leq\infty} |x|_p = \left(\prod_{j=1}^{n} p_j^{-k_j}\right) \cdot p_1^{k_1} \cdots p_n^{k_n}$$

$$= 1.$$

<u>22:</u> REMARK If p_1, p_2 are distinct primes, then $|\cdot|_{p_1}$ is not equivalent to $|\cdot|_{p_2}$.

[Consider the sequence $\{p_1^n\}$:

$$|p_1|_{p_1} = p_1^{-1} \Rightarrow |p_1^n|_{p_1} = p_1^{-n} \to 0.$$

Meanwhile,

$$|p_1|_{p_2} = |p_2^0 p_1|_{p_2} = p_2^{-0} = 1$$

$$\Rightarrow |p_1^n|_{p_2} \equiv 1.]$$

<u>23:</u> CRITERION Let $|\cdot|$ be an absolute value on F -- then $|\cdot|$ is non-archimedean iff $\{|n|:n \in N\}$ is bounded.

[Note: In either case, $|n|$ is bounded by 1:

$$|n| = |1 + 1 + \cdots + 1| \leq 1.]$$

§2. *TOPOLOGICAL FIELDS*

Let $|.|$ be an absolute value on a field F. Given $a \in F$, $r > 0$, put

$$N_r(a) = \{b: |b - a| < r\}.$$

1: LEMMA There is a topology on F in which a basis for the neighborhoods of a are the $N_r(a)$.

PROOF The nontrivial point is to show that given $V \in \mathcal{B}_a$, there is a $V_0 \in \mathcal{B}_a$ such that if $a_0 \in V_0$, then there is a $W \in \mathcal{B}_{a_0}$ such that $W \subset V$. So let $V = N_r(a)$, $V_0 = N_{r/2M}(a)$, $W = N_{r/2M}(a_0)$ $(a_0 \in V_0)$ -- then $W \subset V$:

$$\begin{aligned} b \in W \Rightarrow |b - a| &= |(b - a_0) + (a_0 - a)| \\ &\leq M \sup(|b - a_0|, |a_0 - a|) \\ &\leq M \sup(r/2M, r/2M) \\ &= M(r/2M) = r/2 < r. \end{aligned}$$

2: EXAMPLE The topology induced by $|.|$ is the discrete topology iff $|.|$ is the trivial absolute value.

3: FACT Absolute values $|.|_1$, $|.|_2$ are equivalent iff they give rise to the same topology.

4: LEMMA The topology induced by $|.|$ is metrizable.

PROOF This is because $|.|$ is equivalent to an absolute value satisfying the triangle inequality (cf. §1, #14), the underlying metric being

$$d(a,b) = |a - b|.$$

<u>5:</u> THEOREM A field with a topology defined by an absolute value is a <u>topological field</u>, i.e., the operations sum, product, and inversion are continuous.

Assume now that $|.|$ is non-archimedean, hence that the ultrametric inequality

$$|a - b| \leq \sup(|a|,|b|)$$

is in force.

<u>6:</u> LEMMA $N_r(a)$ is closed (open is automatic).

PROOF Let p be a limit point of $N_r(a)$ -- then $\forall\ t > 0$,

$$(N_t(p) - \{p\}) \cap N_r(a) \neq \emptyset.$$

Take $t = \frac{r}{2}$ and choose $b \in N_r(a)$:

$$d(p,b) < \frac{r}{2} \quad (p \neq b).$$

Then

$$d(a,p) \leq \sup(d(a,b), d(b,p))$$

$$< r$$

$$\Rightarrow$$

$$p \in N_r(a).$$

Therefore $N_r(a)$ contains all its limit points, hence is closed.

<u>7:</u> LEMMA If $a' \in N_r(a)$, then $N_r(a') = N_r(a)$.

PROOF E.g.:

$$b \in N_r(a) \Rightarrow |b - a| < r$$

$$\Rightarrow |b - a'| = |(b - a) + (a - a')|$$

$$\leq \sup(|b - a|, |a - a'|)$$

$$< r \Rightarrow N_r(a) \subset N_r(a').$$

8: REMARK Put

$$B_r(a) = \{b : |b - a| \leq r\}.$$

Then a priori, $B_r(a)$ is closed. But $B_r(a)$ is also open and if $a' \in B_r(a)$, then $B_r(a') = B_r(a)$.

9: LEMMA If

$$a_1 + a_2 + \cdots + a_n = 0,$$

then $\exists$ $i \neq j$ such that

$$|a_i| = |a_j| = \sup|a_k|.$$

§3. *COMPLETIONS*

Let $|.|$ be an absolute value on a field F which satisfies the triangle inequality -- then per $|.|$, F might or might not be complete.

1: EXAMPLE Take F = R or Q and let $|.| = |.|_\infty$ -- then R is complete but Q is not.

2: EXAMPLE Take F = Q and let $|.| = |.|_p$ -- then Q is not complete.

[To illustrate this, choose p = 5 and starting with $x_1 = 2$, define inductively a sequence $\{x_n\}$ of integers subject to

$$\begin{cases} x_n^2 + 1 \equiv 0 \mod 5^n \\ x_{n+1} \equiv x_n \mod 5^n. \end{cases}$$

Then

$$|x_m - x_n|_5 \leq 5^{-n} \quad (m > n),$$

so $\{x_n\}$ is a Cauchy sequence and, to get a contradiction, assume that it has a limit x in Q, thus

$$|x_n^2 + 1|_5 \leq 5^{-n} \Rightarrow |x^2 + 1|_5 = 0$$

$$\Rightarrow x^2 + 1 = 0 \ldots .]$$

3: DEFINITION If an absolute value is not non-archimedean, then it is said to be archimedean.

4: FACT Suppose that F is a field which is complete with respect to an archimedean absolute value $|.|$ -- then F is isomorphic to either R or C and $|.|$ is equivalent to $|.|_\infty$.

5: RAPPEL Every metric space X has a completion $\bar{X}$. Moreover, there is an isometry $\phi:X \to \bar{X}$ such that $\phi(X)$ is dense in $\bar{X}$ and $\bar{X}$ is unique up to isometric isomorphism.

6: CONSTRUCTION The standard model for $\bar{X}$ is the set of all Cauchy sequences in X modulo the equivalence relation ~, where

$$\{x_n\} \sim \{y_n\} \iff d(x_n,y_n) \to 0,$$

the map $\phi:X \to \bar{X}$ being the rule that sends $x \in X$ to the equivalence class of the constant sequence $x_n = x$.

[Note: The metric on $\bar{X}$ is specified by

$$\bar{d}(\{x_n\},\{y_n\}) = \lim_{n \to \infty} d(x_n,y_n).]$$

Take X = F and

$$d(x,y) = |x - y|.$$

Then the claim is that $\bar{F}$ is a field. E.g.: Let us deal with addition. Given $\bar{x},\bar{y} \in \bar{F}$, how does one define $\bar{x} + \bar{y}$? To this end, choose sequences $\begin{cases} x_n \\ y_n \end{cases}$ in F such that $\begin{cases} x_n \to \bar{x} \\ y_n \to \bar{y} \end{cases}$ -- then

$$d(x_n + y_n, x_m + y_m)$$

$$= |x_n + y_n - x_m - y_m|$$

$$= |(x_n - x_m) + (y_n - y_m)|$$

$$\le |x_n - x_m| + |y_n - y_m|.$$

Therefore $\{x_n + y_n\}$ is a Cauchy sequence in F, hence converges in $\bar{F}$ to an element $\bar{z}$. If $\begin{cases} x_n' \\ y_n' \end{cases}$ are sequences in F converging to $\begin{cases} \bar{x} \\ \bar{y} \end{cases}$ as well, then $\{x_n' + y_n'\}$ converges in $\bar{F}$ to an element $\bar{z}'$. And

$$\bar{z} = \bar{z}'.$$

Proof: Choose $n \in N$ such that

$$\begin{cases} |\bar{z} - (x_n + y_n)| < \frac{\varepsilon}{3} \\ |\bar{z}' - (x_n' + y_n')| < \frac{\varepsilon}{3} \end{cases}$$

and

$$|(x_n + y_n) - (x_n' + y_n')| \le |x_n - x_n'| + |y_n - y_n'| < \frac{\varepsilon}{3}.$$

Then

$$|\bar{z} - \bar{z}'| \le |\bar{z} - (x_n + y_n)| + |\bar{z}' - (x_n + y_n)|$$

$$\le |\bar{z} - (x_n + y_n)| + |\bar{z}' - (x_n' + y_n')| + |(x_n' + y_n') - (x_n + y_n)| < \varepsilon$$

$$\Rightarrow \bar{z} = \bar{z}'.$$

Therefore addition in F extends to $\bar{F}$. The same holds for multiplication and inversion. Bottom line: $\bar{F}$ is a field. Furthermore, the prescription

$$|\bar{x}| = \bar{d}(x,0) \quad (\bar{x} \in \bar{F})$$

is an absolute value on $\bar{F}$ whose underlying topology is the metric topology. It thus follows that $\bar{F}$ is a topological field (cf. §2, #5).

7: EXAMPLE Take $F = Q$, $|\cdot| = |\cdot|_p$ -- then the completion $\bar{F} = \bar{Q}$ is denoted by Q_p, the field of p-adic numbers.

8: LEMMA If $|\cdot|$ is non-archimedean per F, then $|\cdot|$ is non-archimedean per $\bar{F}$.

PROOF Given $\begin{bmatrix} \bar{x} \\ \bar{y} \end{bmatrix} \in \bar{F}$, choose $\begin{bmatrix} x_n \\ y_n \end{bmatrix}$ in F such that $\begin{bmatrix} x_n \to \bar{x} \\ y_n \to \bar{y} \end{bmatrix}$ in $\bar{F}$:

$$|\bar{x} - \bar{y}| \leq |\bar{x} - x_n + x_n - y_n + y_n - \bar{y}|$$

$$\leq \underset{\downarrow \atop 0}{|\bar{x} - x_n|} + |x_n - y_n| + \underset{\downarrow \atop 0}{|\bar{y} - y_n|}.$$

And

$$|x_n - y_n| \leq \sup(|x_n|,|y_n|)$$

$$= \frac{1}{2}(|x_n| + |y_n| + |x_n - y_n|)$$

$$\to \frac{1}{2}(|\bar{x}| + |\bar{y}| + |\bar{x} - \bar{y}|)$$

$$= \sup(|\bar{x}|,|\bar{y}|).$$

<u>9:</u> LEMMA If $|.|$ is non-archimedean per $|.|$, then

$$\{|\bar{x}|:\bar{x} \in \bar{F}\} = \{|x|:x \in F\}.$$

PROOF Take $\bar{x} \in \bar{F}:\bar{x} \neq 0$. Choose $x \in F:|\bar{x} - x| < |\bar{x}|$. Claim: $|\bar{x}| = |x|$. Thus consider the other possibilities.

- $|x| < |\bar{x}|$:

$$|\bar{x} - x| = |\bar{x} + (-x)| = |\bar{x}| \text{ (cf. §1, \#18)} < |\bar{x}| \ldots .$$

- $|\bar{x}| < |x|$:

$$|\bar{x} - x| = |- x + \bar{x}| = |- x| \text{ (cf. §1, \#18)} = |x| < |\bar{x}| \ldots .$$

<u>10:</u> EXAMPLE The image of Q_p under $|.|_p$ is the same as the image of Q under $|.|_p$, namely

$$\{p^k:k \in Z\} \cup \{0\}.$$

Let K be a field, $L \supset K$ a finite field extension.

<u>11:</u> EXTENSION PRINCIPLE Let $|.|_K$ be a complete absolute value on K -- then there is one and only one extension $|.|_L$ of $|.|_K$ to L and it is given by

$$|x|_L = |N_{L/K}(x)|_K^{1/n},$$

where $n = [L:K]$. In addition, L is complete with respect to $|.|_L$.

[Note: $|.|_L$ is non-archimedean if $|.|_K$ is non-archimedean.]

<u>12:</u> SCHOLIUM There is a unique extension of $|.|_K$ to the algebraic closure $K^{c\ell}$ of K.

[Note: It is not true in general that $K^{c\ell}$ is complete.]

Suppose further that $L \supset K$ is a Galois extension. Given $\sigma \in \text{Gal}(L/K)$, define $|\cdot|_\sigma$ by $|x|_\sigma = |\sigma x|_L$ — then

$$|\cdot|_\sigma | K = |\cdot|_K,$$

so by uniqueness, $|\cdot|_\sigma = |\cdot|_L$. But

$$N_{L/K}(x) = \prod_{\sigma \in \text{Gal}(L/K)} \sigma x$$

=>

$$\begin{aligned} &|N_{L/K}(x)|_K \\ &= |N_{L/K}(x)|_L = \left|\prod_{\sigma \in \text{Gal}(L/K)} \sigma x\right|_L \\ &= \prod_{\sigma \in \text{Gal}(L/K)} |\sigma x|_L \\ &= \prod_{\sigma \in \text{Gal}(L/K)} |x|_L \\ &= |x|_L^{\#(\text{Gal}(L/K))} \\ &= |x|_L^{[L:K]} = |x|_L^n. \end{aligned}$$

APPENDIX

APPROXIMATION PRINCIPLE Let $|\cdot|_1, \ldots, |\cdot|_N$ be pairwise inequivalent non-trivial absolute values on F. Fix elements $a_1, \ldots, a_N$ in F — then $\forall \, \varepsilon > 0$, $\exists \, a_\varepsilon \in F$:

$$|a_\varepsilon - a_k|_k < \varepsilon \quad (k = 1, \ldots, N).$$

Let $\bar{F}_1,\ldots,\bar{F}_N$ be the associated completions and let

$$\Delta:F \to \prod_{k=1}^{N} \bar{F}_k$$

be the diagonal map -- then the image ΔF is dense (i.e., its closure is the whole of $\prod_{k=1}^{N} \bar{F}_k$).

[Fix $\varepsilon > 0$ and elements $\bar{a}_1,\ldots,\bar{a}_N$ in $\bar{F}_1,\ldots,\bar{F}_N$ respectively -- then there exist elements $a_k \in F$:

$$|a_k - \bar{a}_k|_k < \varepsilon \quad (k = 1,\ldots,N).$$

Choose $a_\varepsilon \in F$:

$$|a_\varepsilon - a_k| < \varepsilon \quad (k = 1,\ldots,N).$$

Then

$$\begin{aligned} |a_\varepsilon - \bar{a}_k|_k &= |(a_\varepsilon - a_k) + (a_k - \bar{a}_k)|_k \\ &\leq |a_\varepsilon - a_k| + |a_k - \bar{a}_k|_k \\ &< 2\varepsilon.] \end{aligned}$$

<u>N.B.</u> The product $\prod_{k=1}^{N} \bar{F}_k$ carries the product topology and the prescription

$$\begin{aligned} &d((\bar{a}_1,\ldots,\bar{a}_N),(\bar{b}_1,\ldots,\bar{b}_N)) \\ &= \sup_{1\leq k\leq N} d_k(\bar{a}_k,\bar{b}_k) \\ &= \sup_{1\leq k\leq N} |\bar{a}_k - \bar{b}_k|_k \end{aligned}$$

metrizes the product topology. Therefore

$$d((a_\varepsilon,\ldots,a_\varepsilon),(\bar{a}_1,\ldots,\bar{a}_N))$$

$$= \sup_{1\le k\le N} d_k(a_\varepsilon,\bar{a}_k)$$

$$= \sup_{1\le k\le N} |a_\varepsilon - \bar{a}_k|_k$$

$$< 2\varepsilon.$$

§4. p-ADIC STRUCTURE THEORY

Fix a prime p and recall that Q_p is the completion of Q per the p-adic absolute value $|\cdot|_p$.

1: NOTATION Let

$$A = \{0,1,\ldots,p-1\}.$$

2: SCHOLIUM Structurally, Q_p is the set of all Laurent series in p with coefficients in A subject to the restriction that only finitely many negative powers of p occur, thus generically a typical element $x \neq 0$ of Q_p has the form

$$x = \sum_{n=N}^{\infty} a_n p^n \quad (a_n \in A,\ N \in Z).$$

3: N.B. It follows from this that Q_p is uncountable, so Q is not complete per $|\cdot|_p$.

The exact formulation of the algebraic rules (i.e., addition, multiplication, inversion) is elementary (but technically a bit of a mess) and will play no role in the sequel, hence can be omitted.

4: LEMMA Every positive integer N admits a base p expansion:

$$N = a_0 + a_1 p + \cdots + a_n p^n,$$

where the $a_k \in A$.

5: EXAMPLE

$$1 = 1 + 0p + 0p^2 + \cdots .$$

6: EXAMPLE Take p = 3 -- then

$$\begin{cases} 24 = 0 + 2 \times 3 + 2 \times 3^2 = 2p + 2p^2 \\ 17 = 2 + 2 \times 3 + 1 \times 3^2 = 2 + 2p + p^2 \end{cases}$$

=>

$$\frac{24}{17} = \frac{2p + 2p^2}{2 + 2p + p^2} = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \cdots .$$

7: LEMMA

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots .$$

PROOF Add 1:

$$1 + (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots$$

$$= p + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots$$

$$= p^2 + (p-1)p^2 + (p-1)p^3 + \cdots$$

$$= p^3 + (p-1)p^3 + \cdots = 0.$$

8: APPLICATION

$$-N = (-1) \cdot N$$

$$= (\sum_{i=0}^{\infty} (p-1)p^i)(a_0 + a_1 p + \cdots + a_n p^n)$$

$$= \cdots$$

9: LEMMA A p-adic series

$$\sum_{n=1}^{\infty} x_n \quad (x_n \in Q_p)$$

is convergent iff $|x_n|_p \to 0 \quad (n \to \infty)$.

PROOF The usual argument establishes necessity. So suppose that $|x_n|_p \to 0$ $(n \to \infty)$. Given $K > 0$, $\exists$ N:

$$n > N \Rightarrow |x_n|_p < p^{-K}.$$

Let

$$s_n = \sum_{k=1}^{n} x_k.$$

Then

$$\begin{aligned} m > n > N \Rightarrow |s_m - s_n|_p &= |x_{n+1} + \cdots + x_m|_p \\ &\leq \sup(|x_{n+1}|_p, \ldots, |x_m|_p) \\ &< p^{-K}. \end{aligned}$$

Therefore the sequence $\{s_n\}$ of partial sums is Cauchy, thus is convergent (Q_p being complete).

<u>10:</u> EXAMPLE The p-adic series

$$\sum_{i=0}^{\infty} p^i$$

is convergent (to $\frac{1}{1-p}$).

<u>11:</u> EXAMPLE The p-adic series

$$\sum_{n=0}^{\infty} n!$$

is convergent.

[Note that

$$|n!|_p = p^{-N},$$

where

$$N = [n/p] + [n/p^2] + \cdots .]$$

<u>12:</u> EXAMPLE The p-adic series

$$\sum_{n=0}^{\infty} n \cdot n!$$

is convergent (to -1).

<u>13:</u> LEMMA Q_p is a topological field (cf. §2, #5).

<u>14:</u> LEMMA Q_p is 0-dimensional, hence is totally disconnected.

PROOF A basic neighborhood $N_r(x)$ is open (by definition) and closed (cf. §2, #6).

<u>15:</u> NOTATION

- $Z_p = \{x \in Q_p : |x|_p \leq 1\}$
- $pZ_p = \{x \in Q_p : |x|_p < 1\}$
- $Z_p^{\times} = \{x \in Z_p : |x|_p = 1\}$

<u>16:</u> LEMMA Z_p is a commutative ring with unit (the ring of <u>p-adic integers</u>), in fact Z_p is an integral domain.

<u>17:</u> LEMMA pZ_p is an ideal in Z_p, in fact pZ_p is a maximal ideal in Z_p, in fact pZ_p is the unique maximal ideal in Z_p, hence Z_p is a local ring.

<u>18:</u> LEMMA $Z_p^{\times}$ is a group under multiplication, in fact $Z_p^{\times}$ is the set of

p-adic units in Z_p, i.e., the set of elements in Z_p that have a multiplicative inverse in Z_p.

Obviously,

$$Z_p = Z_p^\times \coprod (Z_p - Z_p^\times)$$

or still,

$$Z_p = Z_p^\times \coprod pZ_p.$$

19: LEMMA

$$Z_p = \bigcup_{0\leq k\leq p-1} (k + pZ_p).$$

PROOF Let $x \in Z_p$. Matters being clear if $|x|_p < 1$ (since in this case $x \in pZ_p$), suppose that $|x|_p = 1$. Choose $q = \frac{a}{b} \in Q: |q - x|_p < 1$, where $(a,b) = 1$ and $\begin{cases} (a,p) = 1 \\ (b,p) = 1 \end{cases}$ — then

$$x + pZ_p = q + pZ_p.$$

Choose k with $0 < k \leq p-1$ such that p divides $a - kb$, thus $|a - kb|_p < 1$ and, moreover, $\left|\frac{a - kb}{b}\right|_p < 1$. Therefore

$$\left|k - \frac{a}{b}\right|_p < 1 \Rightarrow k + pZ_p = q + pZ_p = x + pZ_p$$

$$\Rightarrow x \in k + pZ_p$$

Consider a p-adic series

$$\sum_{n=0}^{\infty} a_n p^n \quad (a_n \in A).$$

Then

$$\left|\sum_{n=0}^{\infty} a_n p^n\right|_p \le \sup_n \left|a_n p^n\right|_p$$

$$\le \sup_n \left|p^n\right|_p \le 1,$$

so it converges to an element x of Z_p. Conversely:

<u>20:</u> THEOREM Every $x \in Z_p$ admits a unique representation

$$x = \sum_{n=0}^{\infty} a_n p^n \quad (a_n \in A).$$

PROOF Let $x \in Z_p$ be given. Choose uniquely $a_0 \in A$ such that $|x - a_0|_p < 1$, hence $x = a_0 + px_1$ for some $x_1 \in Z_p$. Choose uniquely $a_1 \in A$ such that $|x_1 - a_1|_p < 1$, hence $x_1 = a_1 + px_2$ for some $x_2 \in Z_p$. Continuing: $\forall$ N,

$$x = a_0 + a_1 p + \cdots + a_N p^N + x_{N+1} p^{N+1},$$

where $a_n \in A$ and $x_{N+1} \in Z_p$. But

$$x_{N+1} p^{N+1} \to 0.$$

<u>21:</u> APPLICATION Z is dense in Z_p.

<u>22:</u> EXAMPLE Let $x \in Z_p$ -- then $\forall\ n \in N$,

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \in Z_p.$$

<u>23:</u> LEMMA

$$Z_p^{\times} = \bigcup_{1 \le k \le p-1} (k + pZ_p).$$

Consequently, if

$$x = \sum_{n=0}^{\infty} a_n p^n \quad (a_n \in A)$$

and if $x \in Z_p^{\times}$, then $a_0 \neq 0$.

[In fact, there is a unique k $(1 \leq k \leq p-1)$ such that $x \in k + pZ_p$ and this "k" is a_0.]

24: THEOREM An element

$$x = \sum_{n=0}^{\infty} a_n p^n \quad (a_n \in A)$$

in Z_p is a unit iff $a_0 \neq 0$.

PROOF To establish the characterization, construct a multiplicative inverse y for x as follows. First choose uniquely b_0 $(1 \leq b_0 \leq p-1)$ such that $a_0 b_0 \equiv 1 \bmod p$. Proceed from here by recursion and assume that $b_1, \ldots, b_M$ between 0 and $p-1$ have already been found subject to

$$x\Big(\sum_{0 \leq m \leq M} b_m p^m\Big) \equiv 1 \bmod p^{M+1}.$$

Then there is exactly one $0 \leq b_{M+1} \leq p - 1$ such that

$$x\Big(\sum_{0 \leq m \leq M+1} b_m p^m\Big) \equiv 1 \bmod p^{M+2}.$$

Now put $y = \sum_{m=0}^{\infty} b_m p^m$, thus $xy = 1$.

25: EXAMPLE $1 - p$ is invertible in Z_p but p is not invertible in Z_p.

26: REMARK The arrow

$$\varepsilon : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$$

that sends

$$x = \sum_{n=0}^{\infty} a_n p^n \quad (a_n \in A)$$

to a_0 mod p is a homomorphism of rings called reduction mod p. It is surjective with kernel $p\mathbb{Z}_p$, hence $[\mathbb{Z}_p : p\mathbb{Z}_p] = p$.

Consider now the topological aspects of $\mathbb{Z}_p$:

- $\mathbb{Z}_p$ is totally disconnected.
- $\mathbb{Z}_p$ is closed, hence complete.
- $\mathbb{Z}_p$ is open.

[As regards the last point, observe that

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < r\}$$

$$\equiv N_r(0) \quad (1 < r < p).]$$

27: THEOREM $\mathbb{Z}_p$ is compact.

PROOF Since $\mathbb{Z}_p$ is a metric space, it suffices to show that $\mathbb{Z}_p$ is sequentially compact. So let $x_1, x_2, \ldots$ be an infinite sequence in $\mathbb{Z}_p$. Choose $a_0 \in A$ such that $a_0 + p\mathbb{Z}_p$ contains infinitely many of the x_n. Write

$$a_0 + p\mathbb{Z}_p$$

$$= a_0 + p \left(\bigcup_{a \in A} (a + p\mathbb{Z}_p) \right)$$

$$= a_0 + \bigcup_{a \in A} (ap + p^2 Z_p)$$

$$= \bigcup_{a \in A} (a_0 + ap + p^2 Z_p).$$

Choose $a_1 \in A$ such that $a_0 + a_1 p + p^2 Z_p$ contains infinitely many of the x_n. ETC. The construction thus produces a descending sequence of cosets of the form

$$A_j + p^j Z_p,$$

each of which contains infinitely many of the x_n. But

$$A_j + p^j Z_p = \{x \in Z_p : |x - A_j|_p \le p^{-j}\}$$

$$\equiv B_{p^{-j}}(A_j),$$

a closed ball in the p-adic metric of radius $p^{-j} \to 0$ $(j \to \infty)$, hence by the completeness of Z_p,

$$\bigcap_{j=1}^{\infty} B_{p^{-j}}(A_j) = \{A\}.$$

Finally, choose

$$x_{n_1} \in B_{p^{-1}}(A_1),\ x_{n_2} \in B_{p^{-2}}(A_2), \ldots .$$

Then

$$\lim_{j \to \infty} x_{n_j} = A.$$

<u>28:</u> APPLICATION Q_p is locally compact.

[Since Q_p is Hausdorff, it is enough to prove that each $x \in Q_p$ has a compact neighborhood. But Z_p is a compact neighborhood of 0, so $x + Z_p$ is a compact neighborhood of x.]

The set $p^{-n}Z_p$ $(n \geq 0)$ is the set of all $x \in Q_p$ such that $|x|_p \leq p^n$. Therefore

$$Q_p = \bigcup_{n=0}^{\infty} p^{-n}Z_p.$$

Accordingly, Q_p is σ-compact (the $p^{-n}Z_p$ being compact).

29: SCHOLIUM A subset of Q_p is compact iff it is closed and bounded.

30: LEMMA Given $n,m \in Z$,

$$p^nZ_p \subset p^mZ_p \iff m \leq n.$$

31: REMARK Take $n \geq 1$ — then the p^nZ_p are principal ideals in Z_p and, apart from $\{0\}$, these are the only ideals in Z_p, thus Z_p is a principal ideal domain.

32: LEMMA For every $x_0 \in Q_p$ and $r > 0$, there is an integer n such that

$$N_r(x_0) = \{x \in Q_p : |x - x_0|_p < r\}$$

$$= N_{p^{-n}}(x_0) = \{x \in Q_p : |x - x_0|_p < p^{-n}\}$$

$$= x_0 + p^{n+1}Z_p.$$

33: SCHOLIUM The basic open sets in Q_p are the cosets of some power of pZ_p.

[Note: It is a corollary that every nonempty open subset of Q_p can be written as a disjoint union of cosets of the $p^n Z_p$ $(n \in Z)$.]

<u>34:</u> LEMMA

$$p^n Z_p^\times = p^n Z_p - p^{n+1} Z_p.$$

<u>35:</u> DEFINITION The $p^n Z^\times$ are called <u>shells</u>.

<u>36:</u> <u>N.B.</u> There is a disjoint decomposition

$$Q_p^\times = \bigcup_{n \in Z} p^n Z_p^\times,$$

where

$$p^n Z_p^\times = \bigcup_{1 \leq k \leq p-1} (p^n k + p^{n+1} Z_p).$$

[Note: For the record, $Q_p^\times$ is totally disconnected and, being open in Q_p, is Hausdorff and locally compact. Moreover, $Z_p^\times$ is open-closed (indeed, open-compact).]

Let $x \in Q_p^\times$ — then there is a unique $v(x) \in Z$ and a unique $u(x) \in Z_p^\times$ such that $x = p^{v(x)} u(x)$. Consequently,

$$Q_p^\times \approx \langle p \rangle \times Z_p^\times$$

or still,

$$Q_p^\times \approx Z \times Z_p^\times.$$

<u>37:</u> NOTATION For $n = 1,2,\ldots$, put

$$U_{p,n} = 1 + p^n Z_p.$$

[Note:

$$1 + p^n Z_p = \{x \in Z_p^\times : |1 - x|_p \leq p^{-n}\}.]$$

The $U_{p,n}$ are open-compact subgroups of $Z_p^\times$ and

$$Z_p^\times \supset U_{p,1} \supset U_{p,2} \supset \cdots .$$

38: LEMMA The collection $\{U_{p,n} : n \in N\}$ is a neighborhood basis at 1.

39: DEFINITION $U_{p,1} = 1 + pZ_p$ is called the group of principal units of Z_p.

40: LEMMA The quotient $Z_p^\times/U_{p,1}$ is isomorphic to $F_p^\times$ and the index of $U_{p,1}$ in $Z_p^\times$ is $p - 1$.

A generator of $F_p^\times$ can be "lifted" to $Z_p^\times$.

41: THEOREM There exists a $\zeta \in Z_p^\times$ such that $\zeta^{p-1} = 1$ and $\zeta^k \neq 1$ $(0 < k < p-1)$.

[This is a straightforward application of Hensel's lemma.]

42: N.B. $\zeta \notin U_{p,1}$ (p odd).

[If $x \in Z_p$ and if for some $n \geq 1$,

$$(1 + px)^n = 1,$$

then using the binomial theorem one finds that $x = 0$. This said, suppose that

$\zeta \in U_{p,1}$:

$$\zeta = 1 + pu(u \in Z_p) \Rightarrow (1 + pu)^{p-1} = 1 \Rightarrow u = 0,$$

a contradiction.]

<u>43:</u> SCHOLIUM Z_p can be written as a disjoint union

$$Z_p^\times = U_{p,1} \cup \zeta U_{p,1} \cup \zeta^2 U_{p,1} \cup \cdots \cup \zeta^{p-2} U_{p,1}.$$

Therefore

$$Q_p^\times \approx Z \times Z_p^\times \approx Z \times Z/(p-1)Z \times U_{p,1}.$$

<u>44:</u> LEMMA Any root of unity in Q_p lies in $Z_p^\times$.

PROOF If $x = p^{v(x)}u(x)$ and if $x^n = 1$, then $nv(x) = 0$, so $v(x) = 0$, thus $x \in Z_p^\times$.

The roots of unity in $Z_p^\times$ are a subgroup (as in any abelian group), call it T_p. If, on the other hand, G_{p-1} is the cyclic subgroup of $Z_p^\times$ generated by ζ, then G_{p-1} consists of $(p-1)^{st}$ roots of unity, hence $G_{p-1} \subset T_p$.

<u>45:</u> LEMMA If $p \neq 2$, then $G_{p-1} = T_p$ but if $p = 2$, then $T_p = \{\pm 1\}$.

<u>46:</u> APPLICATION If p_1, p_2 are distinct primes, then Q_{p_1} is not field isomorphic to Q_{p_2}.

<u>47:</u> REMARK Q_p is not field isomorphic to R.

[Q_p has algebraic extensions of arbitrarily large linear degree which is not the case of R (cf. §5, #26).]

<u>48:</u> LEMMA Let $x \in Q_p^\times$ -- then $x \in Z_p^\times$ iff x^{p-1} possesses n^{th} roots for infinitely many n.

PROOF If $x \in Z_p^\times$ and if n is not a multiple of p, then one can use Hensel's lemma to infer the existence of a $y_n \in Z_p$ such that $y_n^n = x^{p-1}$. Conversely, if $y_n^n = x^{p-1}$, then

$$nv(y_n) = (p-1)v(x),$$

thus n divides $(p-1)v(x)$. But this can happen for infinitely many n only if $v(x) = 0$, implying thereby that x is a unit.

<u>49:</u> APPLICATION Let $\phi:Q_p \to Q_p$ be a field automorphism -- then ϕ preserves units.

[In fact, if $x \in Z_p^\times$, then

$$y_n^n = x^{p-1} \Rightarrow \phi(y_n)^n = (\phi(x))^{p-1}.]$$

<u>50:</u> THEOREM The only field automorphism ϕ of Q_p is the identity.

PROOF Given $x \in Q_p^\times$, write $x = p^{v(x)}u(x)$, hence

$$\begin{aligned}\phi(x) &= \phi(p^{v(x)}u(x)) \\ &= \phi(p^{v(x)})\phi(u(x)) = p^{v(x)}\phi(u(x)),\end{aligned}$$

hence

$$v(\phi(x)) = v(x) \qquad (\phi(u(x)) \in Z_p^\times).$$

Therefore ϕ is continuous. Since Q is dense in Q_p, it then follows that $\phi = \mathrm{id}_{Q_p}$.

[Note:

$$x_k \to 0 \Rightarrow |x_k|_p \to 0 \Rightarrow p^{-v(x_k)} \to 0$$

$$\Rightarrow p^{-v(\phi(x_k))} \to 0 \Rightarrow |\phi(x_k)|_p \to 0 \Rightarrow \phi(x_k) \to 0.]$$

The final structural item to be considered is that of quadratic extensions and to this end it is necessary to explicate $(Q_p^\times)^2$, bearing in mind that

$$Q_p^\times \approx Z \times Z_p^\times \approx Z \times Z/(p-1)Z \times U_{p,1}.$$

<u>51:</u> LEMMA If $p \neq 2$, then $U_{p,1}^2 = U_{p,1}$ but if $p = 2$, then $U_{2,1}^2 = U_{2,3}$.

<u>52:</u> APPLICATION If $p \neq 2$, then

$$(Q_p^\times)^2 \approx 2Z \times 2(Z/(p-1)Z) \times U_{p,1}$$

but if $p = 2$, then

$$(Q_2^\times)^2 \approx 2Z \times U_{2,3}.$$

<u>53:</u> THEOREM If $p \neq 2$, then

$$[Q_p^\times : (Q_p^\times)^2] = 4$$

but if $p = 2$, then

$$[Q_2^\times : (Q_2^\times)^2] = 8.$$

<u>54:</u> REMARK If $p \neq 2$, then

$$Q_p^\times/(Q_p^\times)^2 \approx Z/2Z \times Z/2Z$$

but if $p = 2$, then

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

55: CRITERION Suppose that $p \neq 2$.

- p is not a square.

[If $p = x^2$, write $x = p^{v(x)}u(x)$ to get

$$1 = v(p) = v(x^2) = 2v(x),$$

an untenable relation.]

- ζ is not a square.

[Assume that $\zeta = x^2$ — then

$$\zeta^{p-1} = 1 \Rightarrow x^{2(p-1)} = 1,$$

thus x is a root of unity, thus $x \in T_p$, thus $x \in G_{p-1}$ (cf. #45), thus $x = \zeta^k$ $(0 < k < p-1)$, thus $\zeta = (\zeta^k)^2 = \zeta^{2k}$, thus $1 = \zeta^{2k-1}$. But

$$2k < 2p-2 \Rightarrow 2k-1 < 2p-1.$$

And

$$\left[\begin{array}{l} 2k - 1 = p - 1 \Rightarrow 2k = p \Rightarrow p \text{ even}\ldots \\ 2k - 1 = 2p - 2 \Rightarrow 2k - 1 = 2(p-1) \Rightarrow 2k - 1 \text{ even}\ldots \end{array}\right.$$.]

- $p\zeta$ is not a square.

[For if $p\zeta = p^{2n}u^2$ $(n \in \mathbb{Z})$, then

$$\zeta = p^{2n-1}u^2 \Rightarrow 1 = |\zeta|_p = |p^{2n-1}|_p = p^{1-2n}$$
$$\Rightarrow 1 - 2n = 0,$$

an untenable relation.]

56: THEOREM If $p \neq 2$, then up to isomorphism, Q_p has three quadratic extensions, viz.

$$Q_p(\sqrt{p}),\ Q_p(\sqrt{\zeta}),\ Q_p(\sqrt{p\zeta}).$$

[Note: If $\tau_1 = p$, $\tau_2 = \zeta$, $\tau_3 = p\zeta$, then these extensions of Q_p are inequivalent since $\tau_i\tau_j^{-1}$ $(i \neq j)$ is not a square in Q_p.]

57: REMARK Another choice for the three quadratic extensions of Q_p when $p \neq 2$ is

$$Q_p(\sqrt{p}),\ Q_p(\sqrt{a}),\ Q_p(\sqrt{pa}),$$

where $1 < a < p$ is an integer that is not a square mod p.

58: REMARK It can be shown that up to isomorphism, Q_2 has seven quadratic extensions, viz

$$Q_2(\sqrt{-1}),\ Q_2(\sqrt{\pm 2}),\ Q_2(\sqrt{\pm 5}),\ Q_2(\sqrt{\pm 10}).$$

59: EXAMPLE Take $p = 5$ -- then $2 \notin (Q_5^\times)^2$, $3 \notin (Q_5^\times)^2$ but $6 \in (Q_5^\times)^2$. And

$$Q_5(\sqrt{2}) = Q_5(\sqrt{3}).$$

[Working within $Z_5^\times$, consider the equation $x^2 = 2$ and expand x as usual:

$$x = \sum_{n=0}^{\infty} a_n 5^n \quad (a_n \in A).$$

Then

$$a_0^2 \equiv 2 \bmod 5.$$

But the possible values of a_0 are 0, 1, 2, 3, 4, thus the congruence is impossible, so $2 \notin (Q_5^\times)^2$. Analogously, $3 \notin (Q_5^\times)^2$. On the other hand, $6 \in (Q_5^\times)^2$ (by direct verification or Hensel's lemma), hence $6 = \gamma^2$ ($\gamma \in Q_5$). Finally, to see that

$$Q_5(\sqrt{2}) = Q_5(\sqrt{3}),$$

it need only be shown that $\sqrt{2} = a + b\sqrt{3}$ for certain $a,b \in Q_5$. To this end, note that $\sqrt{2}\,\sqrt{3} = \pm\gamma$, from which

$$\sqrt{2} = \pm\frac{\gamma}{\sqrt{3}} = \pm\frac{\gamma}{3}\sqrt{3}.]$$

60: EXAMPLE If p is odd, then $p - 1$ is even and $-1 \in G_{p-1}$. In addition, $-1 \in (Q_p^\times)^2$ iff $(p-1)/2$ is even, i.e., iff $p \equiv 1 \bmod 4$. Accordingly, to start $\sqrt{-1}$ exists in Q_5, Q_{13}, ...

[Note: $\sqrt{-1}$ does not exist in Q_2.]

APPENDIX

Let $Q_p^{c\ell}$ be the algebraic closure of Q_p -- then $|\cdot|_p$ extends uniquely to $Q_p^{c\ell}$ (cf. §3, #12) (and satisfies the ultrametric inequality). Furthermore, the range of $|\cdot|_p$ per $Q_p^{c\ell}$ is the set of all rational powers of p (plus 0).

1: THEOREM $Q_p^{c\ell}$ is not second category.

2: APPLICATION The metric space $Q_p^{c\ell}$ is not complete.

3: APPLICATION The Hausdorff space $Q_p^{c\ell}$ is not locally compact (cf. §5, #5).

4: NOTATION Put

$$C_p = \overline{(Q_p^{c\ell})},$$

the completion of $Q_p^{c\ell}$ per $|\cdot|_p$.

5: THEOREM C_p is algebraically closed.

6: N.B. The metric space C_p is separable but the Hausdorff space C_p is not locally compact (cf. §5, #5).

§5. *LOCAL FIELDS*

Let K be a field of characteristic 0 equipped with a non-archimedean absolute value $|.|$.

1: NOTATION Let

$$\begin{cases} R = \{a \in K: |a| \le 1\} \\ R^\times = \{a \in K: |a| = 1\}. \end{cases}$$

2: LEMMA R is a commutative ring with unit and $R^\times$ is its multiplicative group of invertible elements.

3: NOTATION Let

$$P = \{a \in K: |a| < 1\}.$$

4: LEMMA P is a maximal ideal.

Therefore the quotient R/P is a field, the residue field of K.

5: THEOREM K is locally compact iff the following conditions are satisfied.

1. K is a complete metric space.
2. R/P is a finite field.
3. $|K^\times|$ is a nontrivial discrete subgroup of $R_{>0}$.

6: DEFINITION A local field is a locally compact field of characteristic 0.

7. EXAMPLE R and C are local fields.

8. EXAMPLE Q_p is a local field.

Assume that K is a non-archimedean local field.

9: LEMMA R is compact.

10: LEMMA P is principal, say $P = \pi R$, and

$$|K^{\times}| = |\pi|^{Z},$$

where $0 < |\pi| < 1$.

[Note: Such a π is said to be a prime element.]

11: REMARK A nontrivial discrete subgroup Γ of $R_{>0}$ is free on one generator $0 < \gamma < 1$:

$$\Gamma = \{\gamma^{n} : n \in Z\}.$$

This said, choose π with the largest absolute value < 1, thus $\pi \in P \subset R \Rightarrow \pi R \subset P$. In the other direction,

$$a \in P \Rightarrow |a| \leq |\pi| \Rightarrow \frac{a}{\pi} \in R.$$

And

$$a = \pi \cdot \frac{a}{\pi} \Rightarrow a \in \pi R.$$

12: FACT A locally compact topological vector space over a local field is necessarily finite dimensional.

13: THEOREM K is a finite extension of Q_p for some p.

PROOF First, $K \supset Q$ (since char K = 0). Second, the restriction of $|.|$ to Q is equivalent to $|.|_p$ ($\exists$ p) (cf. §1, #20), hence the closure of Q in K "is" Q_p (since K is complete). Third, K is finite dimensional over Q_p (since K is locally compact).

There is also a converse.

<u>14:</u> THEOREM Let K be a finite extension of Q_p -- then K is a local field.

PROOF In view of #5, it suffices to equip K with a non-archimedean absolute value subject to conditions 1,2,3. But, by the extension principle (cf. §3, #11), $|\cdot|_p$ extends uniquely to K. This extension is non-archimedean and points 1,3 are manifest. As for point 2, it suffices to observe that the canonical arrow $Z_p/pZ_p \to R/P$ is injective and

$$[R/P:F_p] \le [K:Q_p] < \infty.$$

[Details: To begin with,

$$Q_p \cap P = pZ_p,$$

thus the inclusion $Z_p \to R$ induces an injection

$$Z_p/pZ_p \to R/P.$$

Put now $n = [K:Q_p]$ and let $A_1,\ldots,A_{n+1} \in R$ -- then the claim is that the residue classes $\bar{A}_1,\ldots,\bar{A}_{n+1} \in R/P$ are linearly dependent over Z_p/pZ_p. In any event, there are elements $x_1,\ldots,x_{n+1} \in Q_p$ such that

$$\sum_{i=1}^{n+1} x_i A_i = 0,$$

matters being arranged in such a way that

$$\max|x_i|_p = 1.$$

Therefore the $x_i \in Z_p$ and not every residue class $\bar{x}_i \in Z_p/pZ_p$ is zero. But then

$$\sum_{i=1}^{n+1} \bar{x}_i \bar{A}_i = 0$$

is a nontrivial dependence relation.]

15: SCHOLIUM A non-archimedean field of characteristic zero is a local field iff it is a finite extension of Q_p ($\exists$ p).

Let $K \supset Q_p$ be a finite extension of linear degree n -- then the canonical absolute value on K is given by

$$|a|_p = |N_{K/Q_p}(a)|_p^{1/n}.$$

[Note: The normalized absolute value on K is given by

$$|a|_K = |a|_p^n.$$

Its intrinsic significance will emerge in due course but for now observe that $|.|_K$ is equivalent to $|.|_p$ and is non-archimedean (cf. §1, #23).]

16: LEMMA The range of $|.|_p|K^\times$ is $|\pi|_p^Z$.

17: DEFINITION The ramification index of K over Q_p is the positive integer

$$e = [|K^\times|_p : |Q_p^\times|_p].$$

I.e.:

$$e = [|\pi|_p^Z : |p|_p^Z].$$

Therefore

$$|\pi|_p^e = |p|_p \ (= \frac{1}{p}).$$

[Consider Z and eZ -- then the generator 1 of Z is related to the generator e of eZ by the triviality $1 + \cdots + 1 = e \cdot 1 = e$.]

18: N.B. If π' has the property that $|\pi'|_p^e = |p|_p$, then π' is a prime element.

[Using obvious notation, write $\pi' = \pi^{v(\pi)}u$, thus

$$|p|_p = |\pi'|_p^e = (|\pi|_p^{v(\pi)})^e$$

$$= (|\pi|_p^e)^{v(\pi)} = |p|_p^{v(\pi)},$$

thus $v(\pi) = 1$.]

19: NOTATION

$$q \equiv \text{card } R/P = (\text{card } F_p)^f = p^f,$$

so

$$f = [R/P:F_p],$$

the residual index of K over Q_p.

20: THEOREM Let $K \supset Q_p$ be a finite extension of linear degree n -- then

$$n = [K:Q_p] = ef.$$

21: APPLICATION

$$|\pi|_K = |\pi|_p^n = |p|_p^{n/e}$$

$$= (\frac{1}{p})^{n/e} = (\frac{1}{p})^f = \frac{1}{p^f} = \frac{1}{q}.$$

View p as an element of K:

- $|p|_p = |N_{K/Q_p}(p)|_p^{1/n} = |p^n|_p^{1/n} = |p|_p$.

- $|p|_K = |N_{K/Q_p}(p)|_p = |p^n|_p = \frac{1}{p^n} = \frac{1}{p^{ef}} = (\frac{1}{p^f})^e = q^{-e}$.

<u>22:</u> DEFINITION A finite extension K of Q_p is

- <u>unramified</u> if e = 1
- <u>ramified</u> if f = 1.

Take the case $K = Q_p$ -- then e = 1, hence K is unramified, and f = 1, hence K is ramified.

<u>23:</u> LEMMA If $K \supset Q_p$ is unramified, then p is a prime element.

<u>24:</u> THEOREM $\forall$ n = 1,2,..., there is up to isomorphism one unramified extension K of Q_p of linear degree n.

Let K be a finite extension of Q_p.

<u>25:</u> LEMMA The group $M^\times$ of roots of unity of order prime to p in K is cyclic of order $p^f - 1$ (= q-1).

<u>26:</u> LEMMA The set $M = M^\times \cup \{0\}$ is a set of coset representatives for R/P.

Therefore (cf. §4, #43)

$$K^\times \approx Z \times R^\times \approx Z \times Z/(q-1)Z \times 1 + P.$$

27: NOTATION Let

$$K_{ur} = Q_p(M^{\times}).$$

28: LEMMA K_{ur} is the maximal unramified extension of Q_p in K and

$$[K_{ur}:Q_p] = f.$$

29: REMARK The maximal unramified extension $(Q_p^{c\ell})_{ur} \subset Q_p^{c\ell}$ is the field extension generated by all roots of unity of order prime to p.

30: QUADRATIC EXTENSIONS (cf. §4, #56) Suppose that $p \neq 2$, let $\tau \in Q_p^{\times} - (Q_p^{\times})^2$, and form the quadratic extension

$$Q_p(\tau) = \{x + y\sqrt{\tau}:x,y \in Q_p\}.$$

Then the canonical absolute value on $Q_p(\sqrt{\tau})$ is given by

$$|x + y\sqrt{\tau}|_p = |N_{Q_p(\sqrt{\tau})/Q_p}(x + y\sqrt{\tau})|_p^{1/2}$$

$$= |x^2 - \tau y^2|_p^{1/2}.$$

31: CLASSIFICATION Consider the three possibilities

$$Q_p(\sqrt{p}),\ Q_p(\sqrt{\tau}),\ Q_p(\sqrt{p\tau}),$$

thus here $2 = ef$.

- $Q_p(\sqrt{p})$ is ramified or still, $e = 2$.

[Note that

$$|\sqrt{p}|_p^2 = |0^2 - (p)1^2|_p = |p|_p = \frac{1}{p}.]$$

- $Q_p(\sqrt{p\zeta})$ is ramified or still, e = 2.

[Note that

$$|\sqrt{p\zeta}|^2 = |0^2 - (p\zeta)1^2|_p = |p\zeta|_p = |p|_p \cdot |\zeta|_p = |p|_p = \frac{1}{p}.]$$

If e = 1, then in either case, the value group would be p^Z, an impossibility since $\frac{1}{\sqrt{p}} \notin p^Z$, so e = 2.

- $Q_p(\sqrt{\zeta})$ is unramified or still, e = 1.

[There is up to isomorphism one unramified extension K of Q_p of linear degree 2 (cf. #24).]

[Instead of quoting theory, one can also proceed directly, it being simplest to work instead with $Q_p(\sqrt{a})$, where $1 < a < p$ is an integer that is not a square mod p (cf. §4, #57) -- then the residue field of $Q_p(\sqrt{a})$ is $F_p(\sqrt{a})$, hence f = 2, hence e = 1 (since n = 2).]

The preceding developments are absolute, i.e., based at Q_p. It is also possible to relativize the theory. Thus let $L \supset K \supset Q_p$ be finite extensions of Q_p. Append subscripts to the various quantities involved:

$$\begin{cases} R_K \supset P_K,\ R_K/P_K,\ e_K, f_K,\ M_K^\times \\ R_L \supset P_L,\ R_L/P_L,\ e_L, f_L,\ M_L^\times . \end{cases}$$

Introduce

$$\begin{cases} e(L/K) = [|L^\times| : |K^\times|] \\ f(L/K) = [R_L/P_L : R_K/P_K]. \end{cases}$$

32: LEMMA

$$[L:K] = e(L/K)f(L/K).$$

PROOF We have

$$\begin{cases} [L:Q_p] = e_L f_L \\ [K:Q_p] = e_K f_K. \end{cases} \qquad \text{(cf. \#20)}$$

Therefore

$$[L:K] = \frac{[L:Q_p]}{[K:Q_p]} = \frac{e_L f_L}{e_K f_K} = e(L/K)f(L/K).$$

33: THEOREM Let $L \supset K \supset Q_p$ be finite extensions of Q_p -- then there exists a unique maximal intermediate extension $K \subset K_{ur} \subset L$ that is unramified over K.

[In fact,

$$K_{ur} = K(M_L^\times) \subset L.]$$

[Note: The extension $L \supset K_{ur}$ is ramified.]

§6. *HAAR MEASURE*

Let X be a locally compact Hausdorff space.

1: DEFINITION A Radon measure is a measure μ defined on the Borel σ-algebra of X subject to the following conditions.

1. μ is finite on compacta, i.e., for every compact set $K \subset X$, $\mu(K) < \infty$.
2. μ is outer regular, i.e., for every Borel set $A \subset X$,

$$\mu(A) = \inf_{U \supset A} \mu(U),$$

where $U \subset X$ is open.

3. μ is inner regular, i.e., for every open set $A \subset X$,

$$\mu(A) = \sup_{K \subset A} \mu(K),$$

where $K \subset X$ is compact.

Let G be a locally compact abelian group.

2: DEFINITION A Haar measure on G is a Radon measure μ_G which is translation invariant: $\forall$ Borel set A, $\forall\, x \in G$,

$$\mu_G(x+A) = \mu_G(A) = \mu_G(A+x)$$

or still, $\forall\, f \in C_c(G)$, $\forall\, y \in G$,

$$\int_G f(x+y)\,d\mu_G(x) = \int_G f(x)\,d\mu_G(x).$$

3: THEOREM G admits a Haar measure and any two Haar measures μ_G, ν_G differ by a positive constant: $\mu_G = c\nu_G$ $(c > 0)$.

4: LEMMA Every nonempty open subset of G has positive Haar measure.

5: LEMMA G is compact iff G has finite Haar measure.

6: LEMMA G is discrete iff every point of G has positive Haar measure.

7: EXAMPLE Take G = R -- then $\mu_R = dx$ (dx = Lebesgue measure) is a Haar measure $(\mu_R([0,1]) = \int_0^1 dx = 1)$.

8: EXAMPLE Take $G = R^\times$ -- then $\mu_{R^\times} = \frac{dx}{|x|}$ (dx = Lebesgue measure) is a Haar measure $(\mu_{R^\times}([1,e]) = \int_1^e \frac{dx}{|x|} = 1)$.

9: EXAMPLE Take G = Z -- then μ_Z = counting measure is a Haar measure.

10: LEMMA Let G' be a closed subgroup of G and put G'' = G/G'. Fix Haar measures μ_G, $\mu_{G'}$ on G, G' respectively -- then there is a unique determination of the Haar measure $\mu_{G''}$ on G'' such that $\forall\ f \in C_c(G)$,

$$\int_G f(x)d\mu_G(x) = \int_{G''} (\int_{G'} f(x+x')d\mu_{G'}(x'))d\mu_{G''}(x'').$$

[Note: The function

$$x \to \int_{G'} f(x+x')d\mu_{G'}(x')$$

is G'-invariant, hence is a function on G''.]

11: EXAMPLE Take G = R, G' = Z with the usual choice of Haar measures. Determine $\mu_{R/Z}$ per #10 -- then $\mu_{R/Z}(R/Z) = 1$.

[Let χ be the characteristic function of $[0,1[$ -- then

$$\sum_{n \in Z} \chi(x+n)$$

is $\equiv 1$, hence when integrated over R/Z gives the volume of R/Z. On the other hand, $\int_R \chi = 1$.]

Let K be a local field (cf. §5, #6). Given $a \in K^\times$, let $M_a:K \to K$ be the automorphism that sends x to $ax = xa$ -- then for any Haar measure μ_K on K, the composite $\mu_K \circ M_a$ is again a Haar measure on K, hence there exists a positive constant $\mathrm{mod}_K(a)$ such that for every Borel set A,

$$\mu_K(M_a(A)) = \mathrm{mod}_K(a)\mu_K(A)$$

or still, $\forall\ f \in C_c(K)$,

$$\int_K f(a^{-1}x)d\mu_K(x) = \mathrm{mod}_K(a)\int_K f(x)d\mu_K(x).$$

[Note: $\mathrm{mod}_K(a)$ is independent of the choice of μ_K.]

Extend mod_K to all of K by setting $\mathrm{mod}_K(0)$ equal to 0.

<u>12:</u> LEMMA Let K,L be local fields, where $L \supset K$ is a finite field extension -- then $\forall\ x \in L$,

$$\mathrm{mod}_L(x) = \mathrm{mod}_K(N_{L/K}(x))$$

$$\equiv \mathrm{mod}_K(\det(M_x)).$$

[Let $n = [L:K]$, view L as a vector space of dimension n, and identify L with K^n by choosing a basis. Proceed from here by breaking M_x into a product of n "elementary" transformations.]

13: EXAMPLE Take $K = R$, $L = R$ — then $\forall a \in R$,

$$\mathrm{mod}_R(a) = |a|.$$

[$\forall f \in C_c(R)$,

$$\int_R f(a^{-1}x)dx = |a| \int_R f(x)dx.]$$

14: EXAMPLE Take $K = R$, $L = C$ — then $\forall z \in C$,

$$\mathrm{mod}_C(z) = \mathrm{mod}_R(N_{C/R}(z))$$

$$= |z\bar{z}| = |z|^2.$$

15: LEMMA

$$\mathrm{mod}_{Q_p} = |.|_p.$$

To prove this, we need a preliminary.

16: LEMMA The arrow

$$\varepsilon_k : Z_p \to Z/p^k Z$$

that sends

$$x = \sum_{n=0}^{\infty} a_n p^n \quad (a_n \in A)$$

to

$$\sum_{n=0}^{k-1} a_n p^n \bmod p^k$$

is a homomorphism of rings. It is surjective with kernel $p^k Z_p$, so $[Z_p : p^k Z_p] = p^k$

(cf. §4, #26), thus there is a disjoint decomposition of Z_p:

$$Z_p = \bigcup_{j=1}^{p^k} (x_j + p^k Z_p).$$

Normalize the Haar measure on Q_p by stipulating that

$$\mu_{Q_p}(Z_p) = 1.$$

[Note: In this connection, recall that Z_p is an open-compact set.]

The claim now is that for every Borel set A,

$$\mu_{Q_p}(M_x(A)) = |x|_p \mu_{Q_p}(A).$$

Since the Borel σ-algebra is generated by the open sets, it is enough to take A open. But any open set can be written as a disjoint union of cosets of the subgroups $p^k Z_p$ (cf. §4, #33), hence, thanks to translation invariance, it suffices to deal with these alone:

$$\mu_{Q_p}(p^k Z_p) = \text{mod}_{Q_p}(p^k)\mu_{Q_p}(Z_p)$$

$$= \text{mod}_{Q_p}(p^k) = |p^k|_p.$$

1. $k \geq 0$:

$$1 = \mu_{Q_p}(Z_p) = \mu_{Q_p}\Big(\bigcup_{j=1}^{p^k} (x_j + p^k Z_p)\Big)$$

$$= p^k \mu_{Q_p}(p^k Z_p)$$

=>

$$\mu_{Q_p}(p^k Z_p) = p^{-k} = |p^k|_p.$$

2. $k < 0$:

$$1 = \mu_{Q_p}(Z_p) = \mu_{Q_p}(p^{-k}p^kZ_p)$$

$$= \mathrm{mod}_{Q_p}(p^{-k})\mu_{Q_p}(p^kZ_p)$$

$$= |p^{-k}|_p\mu_{Q_p}(p^kZ_p)$$

=>

$$\mu_{Q_p}(p^kZ_p) = |p^{-k}|_p^{-1} = |p^k|_p.$$

<u>17:</u> SCHOLIUM If K is a finite extension of Q_p, then $\forall\, a \in K$,

$$\mathrm{mod}_K(a) = |N_{K/Q_p}(a)|_p,$$

the normalized absolute value on K mentioned in §5:

$$\mathrm{mod}_K(a) = |a|_K \; (= |a|_p^n,\ n = [K:Q_p]).$$

<u>18:</u> CONVENTION Integration w.r.t. μ_{Q_p} will be denoted by dx:

$$\int_{Q_p} f(x)d\mu_{Q_p}(x) = \int_{Q_p} f(x)dx.$$

[Note: Points are of Haar measure zero:

$$\{0\} = \bigcap_{k=1}^{\infty} p^kZ_p$$

=>

$$\mu_{Q_p}(\{0\}) = \lim_{k \to \infty} \mu_{Q_p}(p^kZ_p)$$

$$= \lim_{k \to \infty} p^{-k} = 0.]$$

19: EXAMPLE

$$Z_p^\times = \bigcup_{1\le k\le p-1} (k + pZ_p) \quad \text{(cf. §4, \#23)}.$$

Therefore

$$\begin{aligned}\text{vol}_{dx}(Z_p^\times) &= (p-1)\text{vol}_{dx}(pZ_p) \\ &= \frac{p-1}{p}.\end{aligned}$$

20: EXAMPLE

$$\begin{aligned}\text{vol}_{dx}(p^n Z_p^\times) &= \text{vol}_{dx}(p^n Z_p - p^{n+1} Z_p) \quad \text{(cf. §4, \#34)} \\ &= \text{vol}_{dx}(p^n Z_p) - \text{vol}_{dx}(p^{n+1} Z_p) \\ &= |p^n|_p \, \text{vol}_{dx}(Z_p) - |p^{n+1}|_p \, \text{vol}_{dx}(Z_p) \\ &= p^{-n} - p^{-n-1}.\end{aligned}$$

21: EXAMPLE Write

$$Z_p - \{0\} = \bigcup_{n\ge 0} p^n Z_p^\times.$$

Then

$$\begin{aligned}\int_{Z_p-\{0\}} \log |x|_p dx &= \sum_{n=0}^{\infty} \int_{p^n Z_p^\times} \log |x|_p dx \\ &= \sum_{n=0}^{\infty} \log p^{-n} \, \text{vol}_{dx}(p^n Z_p^\times) \\ &= -\log p \sum_{n=0}^{\infty} n(p^{-n} - p^{-n-1})\end{aligned}$$

$$= - \log p \left(\sum_{n=0}^{\infty} \frac{n}{p^n} - \frac{1}{p} \sum_{n=0}^{\infty} \frac{n}{p^n} \right)$$

$$= - (1 - \frac{1}{p}) \log p \sum_{n=0}^{\infty} \frac{n}{p^n}$$

$$= - (1 - \frac{1}{p}) \log p \frac{p}{(p-1)^2}$$

$$= - \frac{\log p}{p-1} .$$

22: EXAMPLE

$$\int_{Z_p^\times} \log |1 - x|_p dx = - \frac{\log p}{p-1} .$$

[Break $Z_p^\times$ up via the scheme

$$(Z_p^\times : a_0 \neq 1) \cup (Z_p^\times : a_0 = 1, a_1 \neq 0) \cup (Z_p^\times : a_0 = 1, a_1 = 0, a_2 \neq 0) \cup \ldots .]$$

23: LEMMA The measure $\frac{dx}{|x|_p}$ is a Haar measure on the multiplicative group $Q_p^\times$.

PROOF $\forall\, y \in Q_p^\times$,

$$\int_{Q_p^\times} f(y^{-1}x) \frac{dx}{|x|_p}$$

$$= |y|_p^{-1} \int_{Q_p^\times} f(y^{-1}x) \frac{1}{|y^{-1}x|_p} dx$$

$$= |y|_p^{-1} \operatorname{mod}_{Q_p}(y) \int_{Q_p^\times} f(x) \frac{dx}{|x|_p}$$

$$= |y|_p^{-1} \, |y|_p \int_{Q_p^\times} f(x) \frac{dx}{|x|_p}$$

$$= \int_{Q_p^\times} f(x) \frac{dx}{|x|_p} .$$

<u>24:</u> EXAMPLE

$$\mathrm{vol}_{\frac{dx}{|x|_p}} (p^n Z_p^\times) = \mathrm{vol}_{\frac{dx}{|x|_p}} (Z_p^\times)$$

$$= \int_{Z_p^\times} \frac{dx}{|x|_p} = \int_{Z_p^\times} dx$$

$$= \mathrm{vol}_{dx} (Z_p^\times) = \frac{p-1}{p} .$$

<u>25:</u> DEFINITION The <u>normalized Haar measure</u> on the multiplicative group $Q_p^\times$ is given by

$$d^\times x = \frac{p}{p-1} \frac{dx}{|x|_p} .$$

Accordingly,

$$\mathrm{vol}_{d^\times x} (Z_p^\times) = 1,$$

this condition characterizing $d^\times x$.

<u>26:</u> EXAMPLE Let s be a complex variable with $\mathrm{Re}(s) > 1$. Write

$$Z_p - \{0\} = \bigcup_{n \geq 0} p^n Z_p^\times .$$

Then

$$\int_{\mathbb{Z}_p-\{0\}} |x|_p^s \, d^\times x$$

$$= \sum_{n=0}^{\infty} p^{-ns} \int_{\mathbb{Z}_p^\times} d^\times x$$

$$= \sum_{n=0}^{\infty} p^{-ns} = \frac{1}{1-p^{-s}} ,$$

the p^{th} factor in the Euler product for the Riemann zeta function.

Let K be a finite extension of $\mathbb{Q}_p$. Given a Haar measure da on K, put

$$d^\times a = \frac{q}{q-1} \frac{da}{|a|_K} .$$

Then $\frac{da}{|a|_K}$ is a Haar measure on $K^\times$ and we have

$$\mathrm{vol}_{d^\times a}(R^\times) = \int_{R^\times} \frac{q}{q-1} \frac{da}{|a|_K}$$

$$= \frac{q}{q-1} \int_{R^\times} da$$

$$= \sum_{n=0}^{\infty} q^{-n} \int_{R^\times} da$$

$$= \sum_{n=0}^{\infty} \int_{R^\times} q^{-n} da$$

$$= \sum_{n=0}^{\infty} \int_{\pi^n R^\times} da$$

$$= \int_{\bigcup_{n\geq 0} \pi^n R^\times} da$$

$$= \int_R da = \mathrm{vol}_{da}(R).$$

§7. *HARMONIC ANALYSIS*

Let G be a locally compact abelian group.

1: DEFINITION A character of G is a continuous homomorphism $\chi:G \to C^\times$.

2. NOTATION Write $\tilde{G}$ for the group whose elements are the characters of G.

3: DEFINITION A unitary character of G is a continuous homomorphism $\chi:G \to T$.

4: NOTATION Write $\hat{G}$ for the group whose elements are the unitary characters of G.

5: LEMMA There is a decomposition

$$\tilde{G} \approx \tilde{G}_+ \times \hat{G},$$

where $\tilde{G}_+$ is the group of positive characters of G.

PROOF The only positive unitary character is trivial, so $\tilde{G}_+ \cap \hat{G} = \{1\}$. On the other hand, if χ is a character, then $|\chi|$ is a positive character, $\chi/|\chi|$ is a unitary character, and $\chi = |\chi| \ (\frac{\chi}{|\chi|})$.

6: LEMMA Every bounded character of G is a unitary character.

PROOF The only compact subgroup of $R_{>0}$ is the trivial subgroup $\{1\}$.

7: APPLICATION If G is compact, then every character of G is unitary.

8: EXAMPLE Take $G = Z$ -- then $\tilde{G} \approx C^\times$, the isomorphism being given by the map $\chi \to \chi(1)$.

9: EXAMPLE Take $G = R$ -- then $\tilde{G} \approx R \times R$ and every character has the form $\chi(x) = e^{zx}$ $(z \in C)$.

10: EXAMPLE Take $G = C$ -- then $\tilde{G} \approx C \times C$ and every character has the form $\chi(x) = \exp(z_1 \operatorname{Re}(x) + z_2 \operatorname{Im}(x))$ $(z_1, z_2 \in C)$.

11: EXAMPLE Take $G = R^\times$ -- then $\tilde{G} \approx Z/2Z \times C$ and every character has the form $\chi(x) = (\operatorname{sgn} x)^\sigma |x|^s$ $(\sigma \in \{0,1\},\ s \in C)$.

12: EXAMPLE Take $G = C^\times$ -- then $\tilde{G} \approx Z \times C$ and every character has the form $\chi(x) = \exp(\sqrt{-1}\, n \arg x)|x|^s (n \in Z,\ s \in C)$.

13: DEFINITION The dual group of G is $\hat{G}$.

14: RAPPEL Let X,Y be topological spaces and let F be a subspace of C(X,Y). Given a compact set $K \subset X$ and an open subset $V \subset Y$, let W(K,V) be the set of all $f \in F$ such that $f(K) \subset V$ -- then the collection $\{W(K,V)\}$ is a subbasis for the compact open topology on F.

[Note: The family of finite intersections of sets of the form W(K,V) is then a basis for the compact open topology: Each member has the form $\bigcap_{i=1}^{n} W(K_i, V_i)$, where the $K_i \subset X$ are compact and the $V_i \subset Y$ are open.]

Equip $\hat{G}$ with the compact open topology.

15: FACT The compact open topology on $\hat{G}$ coincides with the topology of uniform convergence on compact subsets of G.

16: LEMMA $\hat{G}$ is a locally compact abelian group.

17: REMARK $\tilde{G}$ is also a locally compact abelian group and the decomposition

$$\tilde{G} \approx \tilde{G}_+ \times \hat{G}$$

is topological.

18: EXAMPLE Take $G = R$ and given a real number t, let $\chi_t(x) = e^{\sqrt{-1}\, tx}$ -- then χ_t is a unitary character of G and for any $\chi \in \hat{G}$, there is a unique $t \in R$ such that $\chi = \chi_t$, hence G can be identified with $\hat{G}$.

19: EXAMPLE Take $G = R^2$ and given a point (t_1,t_2), let $\chi_{(t_1,t_2)}(x_1,x_2) = e^{\sqrt{-1}\,(t_1x_1 + t_2x_2)}$ -- then $\chi_{(t_1,t_2)}$ is a unitary character of G and for any $\chi \in \hat{G}$, there is a unique $(t_1,t_2) \in R^2$ such that $\chi = \chi_{(t_1,t_2)}$, hence G can be identified with $\hat{G}$.

20: EXAMPLE Take $G = Z/nZ$ and given an integer $m = 0,1,\ldots, n-1$, let $\chi_m(k) = \exp(2\pi\sqrt{-1}\,\frac{km}{n})$ -- then $\chi_0,\chi_1,\ldots,\chi_{n-1}$ are the characters of G, hence G can be identified with $\hat{G}$.

21: LEMMA If G is compact, then $\hat{G}$ is discrete.

22: EXAMPLE Take $G = T$ and given $n \in Z$, let $\chi_n(e^{\sqrt{-1}\,\theta}) = e^{\sqrt{-1}\,n\theta}$ -- then χ_n is a unitary character of G and all such have this form, so $\hat{T} \approx Z$.

23: LEMMA If G is discrete, then $\hat{G}$ is compact.

24: EXAMPLE Take G = Z and given $e^{\sqrt{-1}\,\theta} \in T$, let $\chi_\theta(n) = e^{\sqrt{-1}\,\theta n}$ -- then χ_θ is a unitary character of G and all such have this form, so $\hat{Z} \approx T$.

25: LEMMA If G_1, G_2 are locally compact abelian groups, then $\widehat{G_1 \times G_2}$ is topologically isomorphic to $\hat{G}_1 \times \hat{G}_2$.

26: EXAMPLE Take $G = R^\times$ -- then $G \approx Z/2Z \times R^\times_{>0} \approx Z/2Z \times R$, thus $\hat{G}$ is topologically isomorphic to $Z/2Z \times R$:

$$(u,t) \rightarrow \chi_{u,t} \quad (u \in Z/2Z,\ t \in R),$$

where

$$\chi_{u,t}(x) = \left(\frac{x}{|x|}\right)^u |x|^{\sqrt{-1}\,t}.$$

27: EXAMPLE Take $G = C^\times$ -- then $G \approx T \times R^\times_{>0} \approx T \times R$, thus $\hat{G}$ is topologically isomorphic to $Z \times R$:

$$(n,t) \rightarrow \chi_{n,t} \quad (n \in Z,\ t \in R),$$

where

$$\chi_{n,t}(z) = \left(\frac{z}{|z|}\right)^n |z|^{\sqrt{-1}\,t}.$$

Denote by ev_G the canonical arrow $G \rightarrow \hat{\hat{G}}$:

$$ev_G(x)(\chi) = \chi(x).$$

28: REMARK If G,H are locally compact abelian groups and if $\phi:G \to H$ is a continuous homomorphism, then there is a commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\ ev_G\ } & \hat{\hat{G}} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\hat{\hat{\phi}}} \\ H & \xrightarrow[\ ev_H\ ]{} & \hat{\hat{H}} \end{array} .$$

29: PONTRYAGIN DUALITY ev_G is an isomorphism of groups and a homeomorphism of topological spaces.

30: SCHOLIUM Every compact abelian group is the dual of a discrete abelian group and every discrete abelian group is the dual of a compact abelian group.

31: REMARK Every finite abelian group G is isomorphic to its dual $\hat{G}$: $G \approx \hat{G}$ (but the isomorphism is not "functorial").

Let H be a closed subgroup of G.

32: NOTATION Put

$$H^{\perp} = \{\chi \in \hat{G}:\chi|H = 1\}.$$

33: LEMMA $H^{\perp}$ is a closed subgroup of $\hat{G}$ and $H = H^{\perp\perp}$.

Let $\pi_H:G \to G/H$ be the projection and define

$$\begin{cases} \Phi:\widehat{G/H} \to H^{\perp} \\ \Psi:\hat{G}/H^{\perp} \to \hat{H} \end{cases}$$

by

$$\begin{cases} \Phi(\chi) = \chi \circ \pi_H \\ \Psi(\chi H^\perp) = \chi|H. \end{cases}$$

34: LEMMA Φ and Ψ are isomorphisms of topological groups.

35: APPLICATION Every unitary character of H extends to a unitary character of G.

36: EXAMPLE Let G be a finite abelian group and let H be a subgroup of G -- then G contains a subgroup isomorphic to G/H.

[In fact,

$$G/H \approx \widehat{G/H} \approx H^\perp \subset \hat{G} \approx G.]$$

37: REMARK Denote by LCA the category whose objects are the locally compact abelian groups and whose morphisms are the continuous homomorphisms -- then

$$\wedge : \text{LCA} \to \text{LCA}$$

is a contravariant functor. This said, consider the short exact sequence

$$1 \longrightarrow H \longrightarrow G \xrightarrow{\pi_H} G/H \longrightarrow 1$$

and apply $\wedge$:

$$1 \longrightarrow \widehat{G/H} \approx H^\perp \longrightarrow \hat{G} \longrightarrow \hat{H} \approx \hat{G}/H^\perp \longrightarrow 1,$$

which is also a short exact sequence.

Given $f \in L^1(G)$, its Fourier transform is the function

$$\hat{f}:\hat{G} \to C$$

defined by the rule

$$\hat{f}(\chi) = \int_G f(x)\chi(x)d\mu_G(x).$$

38: EXAMPLE Take $G = R$ -- then $\hat{R} \approx R$ and

$$\hat{f}(\chi_t) \equiv \hat{f}(t) = \int_{-\infty}^{\infty} f(x)e^{\sqrt{-1}\,tx}dx.$$

39: EXAMPLE Take $G = R^2$ -- then $\hat{R}^2 \approx R^2$ and

$$\hat{f}(\chi_{(t_1,t_2)}) \equiv \hat{f}(t_1,t_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x_1,x_2)e^{\sqrt{-1}(t_1x_1 + t_2x_2)}dx_1dx_2.$$

40: EXAMPLE Take $G = T$ -- then $\hat{T} \approx Z$ and

$$\hat{f}(\chi_n) \equiv \hat{f}(n) = \int_0^{2\pi} f(\theta)e^{\sqrt{-1}\,n\theta}d\theta.$$

41: EXAMPLE Take $G = Z$ -- then $\hat{Z} \approx T$ and

$$\hat{f}(\chi_\theta) \equiv \hat{f}(\theta) = \sum_{n=-\infty}^{\infty} f(n)e^{\sqrt{-1}\,n\theta}.$$

42: EXAMPLE Take $G = Z/nZ$ -- then $\widehat{Z/nZ} \approx Z/nZ$ and

$$\hat{f}(\chi_m) \equiv \hat{f}(m) = \sum_{k=0}^{n-1} f(k)\exp(2\pi\sqrt{-1}\,\frac{km}{n}).$$

43: LEMMA $\hat{f}:\hat{G} \to C$ is a continuous function on $\hat{G}$ that vanishes at infinity and

$$||\hat{f}||_\infty \leq ||f||_1.$$

<u>44:</u> NOTATION INV(G) is the set of continuous functions $f \in L^1(G)$ with the property that $\hat{f} \in L^1(\hat{G})$.

<u>45:</u> FOURIER INVERSION Given a Haar measure μ_G on G, there exists a unique Haar measure $\mu_{\hat{G}}$ on $\hat{G}$ such that $\forall\ f \in$ INV(G),

$$f(x) = \int_{\hat{G}} \hat{f}(\chi)\overline{\chi(x)}d\mu_{\hat{G}}(\chi).$$

If G is compact, then it is customary to normalize μ_G by the requirement $\int_G 1 d\mu_G = 1$.

<u>46:</u> LEMMA

$$\int_G \chi(x)d\mu_G(x) = \begin{cases} 1 \text{ if } \chi = 0 \\ 0 \text{ if } \chi \neq 0. \end{cases}$$

PROOF The case $\chi = 0$ is clear. On the other hand, if $\chi \neq 0$, then there exists $x_0 : \chi(x_0) \neq 1$, hence

$$\int_G \chi(x)d\mu_G(x) = \int_G \chi(x-x_0 + x_0)d\mu_G(x)$$

$$= \chi(x_0)\int_G \chi(x-x_0)d\mu_G(x)$$

$$= \chi(x_0)\int_G \chi(x)d\mu_G(x)$$

$\Rightarrow$

$$\int_G \chi(x)d\mu_G(x) = 0.$$

Assuming still that G is compact (=> $\hat{G}$ is discrete), take $f \equiv 1$:

$$\hat{f}(0) = 1, \ \hat{f}(\chi) = 0 \quad (\chi \neq 0).$$

I.e.: $\hat{f}$ is the characteristic function of $\{0\}$, hence is integrable, thus $f \in \text{INV}(G)$. Accordingly, if $\mu_{\hat{G}}$ is the Haar measure on $\hat{G}$ per Fourier inversion, then

$$1 = f(0) = \int_{\hat{G}} \hat{f}(\chi) d\mu_{\hat{G}}(\chi)$$

$$= \mu_{\hat{G}}(\{0\}),$$

so $\forall \ \chi \in \hat{G}$,

$$\mu_{\hat{G}}(\{\chi\}) = 1.$$

<u>47:</u> EXAMPLE Take $G = T$ -- then $d\mu_G = \frac{d\theta}{2\pi}$, so for $f \in \text{INV}(G)$,

$$f(\theta) = \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{-\sqrt{-1}\, n\theta},$$

where

$$\hat{f}(n) = \int_0^{2\pi} f(\theta) e^{\sqrt{-1}\, n\theta} \frac{d\theta}{2\pi}.$$

If G is discrete, then it is customary to normalize μ_G by stipulating that singletons are assigned measure 1.

<u>48:</u> REMARK There is a conflict if G is both compact and discrete, i.e., if G is finite.

Assuming still that G is discrete (=> $\hat{G}$ is compact), take $f(0) = 1$,

$f(x) = 0 \ (x \neq 0)$:

$$\hat{f}(\chi) = \int_G f(x)\chi(x)d\mu_G(x)$$

$$= f(0)\chi(0)\mu_G(\{0\})$$

$$= 1.$$

I.e.: $\hat{f}$ is the constant function 1, hence is integrable, thus $f \in \text{INV}(G)$. Accordingly, if $\mu_{\hat{G}}$ is the Haar measure on $\hat{G}$ per Fourier inversion, then

$$\mu_{\hat{G}}(\hat{G}) = \int_{\hat{G}} 1 d\mu_{\hat{G}}(\chi)$$

$$= \int_{\hat{G}} \hat{f}(\chi)d\mu_{\hat{G}}(\chi)$$

$$= \int_{\hat{G}} \hat{f}(\chi)\chi(0)d\mu_{\hat{G}}(\chi)$$

$$= f(0) = 1.$$

<u>49:</u> EXAMPLE Take $G = Z/nZ$ and let μ_G be the counting measure (thus here $\mu_G(G) = n$) -- then $\mu_{\hat{G}}$ is the counting measure divided by n and for $f \in \text{INV}(G)$,

$$f(k) = \frac{1}{n}\sum_{m=0}^{n-1} \hat{f}(m)\exp(-\ 2\pi\sqrt{-1}\ \frac{km}{n}),$$

where

$$\hat{f}(m) = \sum_{k=0}^{n-1} f(k)\exp(2\pi\sqrt{-1}\ \frac{km}{n}).$$

<u>50:</u> EXAMPLE Take $G = R$ and let $\mu_G = \alpha dx \ (\alpha > 0)$, hence $\mu_{\hat{G}} = \beta dt \ (\beta > 0)$

and we claim that

$$1 = 2\alpha\beta\pi.$$

To establish this, recall first that the formalism is

$$\begin{cases} \hat{f}(t) = \int_{-\infty}^{\infty} f(x) e^{\sqrt{-1}\, tx} \alpha dx \\ f(x) = \int_{-\infty}^{\infty} \hat{f}(t) e^{-\sqrt{-1}\, tx} \beta dt. \end{cases}$$

Let $f(x) = e^{-|x|}$ — then

$$\frac{2\alpha}{1+t^2} = \int_{-\infty}^{\infty} e^{-|x|} e^{\sqrt{-1}\, tx} \alpha dx,$$

so $f \in \text{INV}(G)$, thus

$$\begin{aligned} e^{-|x|} &= \int_{-\infty}^{\infty} \frac{2\alpha}{1+t^2} e^{-\sqrt{-1}\, tx} \beta dt \\ &= 2\alpha\beta \int_{-\infty}^{\infty} \frac{e^{-\sqrt{-1}\, tx}}{1+t^2} dt. \end{aligned}$$

Now put $x = 0$:

$$1 = 2\alpha\beta \int_{-\infty}^{\infty} \frac{dt}{1+t^2} = 2\alpha\beta\pi,$$

as claimed. One choice is to take

$$\alpha = \beta = \frac{1}{\sqrt{2\pi}},$$

the upshot then being that the Haar measure of $[0,1]$ is not 1 but rather $\frac{1}{\sqrt{2\pi}}$.

51: NOTATION Given $f \in L^1(R)$, let

$$F_R f(t) = \int_{-\infty}^{\infty} f(x) e^{2\pi\sqrt{-1}\, tx} dx.$$

Therefore

$$F_R f(t) = \sqrt{2\pi} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{2\pi\sqrt{-1}\, tx} dx$$

$$= \sqrt{2\pi}\, \hat{f}(2\pi t).$$

52: STANDARDIZATION $(G = R)$ Let $f \in \mathrm{INV}(R)$ -- then

$$F_R F_R f(x) = f(-x).$$

[In fact,

$$F_R F_R f(x) = \int_{-\infty}^{\infty} F_R f(t) e^{2\pi\sqrt{-1}\, tx} dt$$

$$= \int_{-\infty}^{\infty} \sqrt{2\pi}\, \hat{f}(2\pi t) e^{2\pi\sqrt{-1}\, tx} dt$$

$$= \sqrt{2\pi} \int_{-\infty}^{\infty} \hat{f}(u) e^{\sqrt{-1}\, ux} \frac{du}{2\pi}$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \hat{f}(t) e^{\sqrt{-1}\, tx} dt$$

$$= f(-x).]$$

Fourier inversion in the plane takes the form

$$\left[\begin{array}{l} \hat{f}(t_1,t_2) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_1,x_2) e^{\sqrt{-1}(t_1x_1+t_2x_2)} dx_1 dx_2 \\ \\ f(x_1,x_2) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \hat{f}(t_1,t_2) e^{-\sqrt{-1}(t_1x_1+t_2x_2)} dt_1 dt_2. \end{array}\right.$$

One may then introduce

$$F_{R^2} f(t_1,t_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_1,x_2) e^{2\pi\sqrt{-1}(t_1x_1+t_2x_2)} dx_1 dx_2$$

$$= 2\pi\hat{f}(2\pi t_1, 2\pi t_2)$$

and, proceeding as above, find that

$$F_{R^2} F_{R^2} f(x_1, x_2) = f(-x_1, -x_2).$$

Now identify R^2 with C and recall that $\mathrm{tr}_{C/R}(z) = z + \bar{z}$. Write

$$\begin{cases} w = a + \sqrt{-1}\, b \\ z = x + \sqrt{-1}\, y. \end{cases}$$

Then

$$wz + \overline{wz} = 2\mathrm{Re}(wz) = 2(ax - by).$$

Therefore

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x,y) e^{2\sqrt{-1}(ax-by)} dxdy$$

$$= \hat{f}(2a, -2b).$$

[Note: Let $\chi_w(z) = \exp(\sqrt{-1}\ (wz + \overline{wz}))$ -- then χ_w is a unitary character of C and for any $\chi \in \hat{C}$, there is a unique $w \in C$ such that $\chi = \chi_w$, hence $\hat{C} \approx C$.]

<u>53:</u> NOTATION Given $f \in L^1(R^2)$, let

$$F_C f(w) = F_C f(a,b)$$

$$= 2F_{R^2} f(2a, -2b)$$

$$= 4\pi\hat{f}(4\pi a, -4\pi b)$$

$$= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x,y) e^{4\pi\sqrt{-1}(ax-by)} 2dxdy.$$

54: STANDARDIZATION $(G = \mathbf{C})$ Let $f \in \mathrm{INV}(\mathbf{C})$ — then

$$F_{\mathbf{C}} F_{\mathbf{C}} f(x,y) = f(-x,-y).$$

[In fact,

$$\begin{aligned} F_{\mathbf{C}} F_{\mathbf{C}} f(x,y) &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} F_{\mathbf{C}} f(a,b) e^{4\pi\sqrt{-1}(ax-by)} 2dadb \\ &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} 4\pi \hat{f}(4\pi a,-4\pi b) e^{4\pi\sqrt{-1}(ax-by)} 2dadb \\ &= \frac{4\pi}{(4\pi)^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \hat{f}(u,-v) e^{\sqrt{-1}(ux-vy)} 2dudv \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \hat{f}(u,-v) e^{\sqrt{-1}(ux-vy)} dudv \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \hat{f}(u,-v) e^{-\sqrt{-1}(-ux+vy)} dudv \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \hat{f}(u,v) e^{-\sqrt{-1}(-ux-vy)} dudv \\ &= f(-x,-y).] \end{aligned}$$

55: PLANCHEREL THEOREM The Fourier transform restricted to $L^1(G) \cap L^2(G)$ is an isometry (with respect to L^2 norms) onto a dense linear subspace of $L^2(\hat{G})$, hence can be extended uniquely to an isometric isomorphism $L^2(G) \to L^2(\hat{G})$.

56: PARSEVAL FORMULA $\forall\ f,g \in L^2(G)$,

$$\int_G f(x)\overline{g(x)} d_G(x) = \int_{\hat{G}} \hat{f}(\chi)\overline{\hat{g}(\chi)} d_{\hat{G}}(\chi).$$

57: N.B. In both of these results, the Haar measure on $\hat{G}$ is per Fourier inversion.

§8. *ADDITIVE* p-*ADIC CHARACTER THEORY*

1: FACT Every proper closed subgroup of T is finite.

Suppose that G is compact abelian and totally disconnected.

2: LEMMA If $\chi \in \hat{G}$, then the image $\chi(G)$ is a finite subgroup of T.

PROOF Ker χ is closed and

$$\chi(G) \approx G/\text{Ker}\ \chi.$$

But the quotient G/Ker χ is 0-dimensional, hence totally disconnected. Therefore $\chi(G)$ is totally disconnected. Since T is connected, it follows that $T \neq \chi(G)$, thus $\chi(G)$ is finite.

3: N.B. The torsion of R/Z is Q/Z, so χ factors through the inclusion $Q/Z \to R/Z$, i.e., $\chi(G) \subset Q/Z$.

The foregoing applies in particular to $G = Z_p$.

4: LEMMA Every character of Q_p is unitary.

PROOF This is because

$$Q_p = \bigcup_{n \in Z} p^n Z_p,$$

where the $p^n Z_p$ are compact, thus §7, #7 is applicable.

5: If $\chi \in \hat{Q}_p$ is nontrivial, then there exists an $n \in Z$ such that $\chi \equiv 1$ on $p^n Z_p$ but $\chi \not\equiv 1$ on $p^{n-1} Z_p$.

PROOF Consider a ball B of radius $\frac{1}{2}$ about 1 in $C^\times$ — then the only subgroup of $C^\times$ contained in B is the trivial subgroup and, by continuity, $\chi(p^n Z_p)$ must be inside B for all sufficiently large n, thus must be identically 1 there.

6: DEFINITION The conductor con χ of a nontrivial $\chi \in \hat{Q}_p$ is the largest subgroup $p^n Z_p$ on which χ is trivial (and n is the minimal integer with this property).

A typical $x \neq 0$ of Q_p has the form

$$x = \sum_{n=v(x)}^{\infty} a_n p^n \quad (a_n \in A,\ v(x) \in Z)$$

$$= f(x) + [x].$$

Here the fractional part $f(x)$ of x is defined by the prescription

$$f(x) = \begin{cases} \sum_{n=v(x)}^{-1} a_n p^n & \text{if } v(x) < 0 \\ 0 & \text{if } v(x) \geq 0 \end{cases}$$

and the integral part $[x]$ of x is defined by the prescription

$$[x] = \sum_{n=0}^{\infty} a_n p^n,$$

with $f(0) = 0$, $[0] = 0$ by convention.

7: N.B.

$$f(x) \in Z[\tfrac{1}{p}] \subset Q,$$

where

$$Z[\tfrac{1}{p}] = \{\tfrac{n}{p^k} : n \in Z,\ k \in Z\},$$

while $[x] \in Z_p$.

8: OBSERVATION

$$0 \le f(x) = \sum_{1\le j\le -v(x)} \frac{a_{-j}}{p^j}$$

$$< (p-1) \sum_{j=1}^{\infty} \frac{1}{p^j} = 1$$

$$\Rightarrow$$

$$f(x) \in [0,1[\cap Z[\tfrac{1}{p}].$$

Let μ_{p^∞} stand for the group of roots of unity in $C^\times$ having order a power of p, thus μ_{p^∞} is a p-group and there is an increasing sequence of cyclic groups

$$\begin{cases} \mu_p \subset \mu_{p^2} \subset \dots \subset \mu_{p^k} \subset \dots \\ \mu_{p^\infty} = \bigcup_{k\ge 0} \mu_{p^k}, \end{cases}$$

where

$$\mu_{p^k} = \{z \in C^\times : z^{p^k} = 1\}.$$

9: REMARK Denote by μ the group of all roots of unity in $C^\times$, hence

$$\mu = \bigcup_{m\ge 1} \mu_m,\ \mu_m = \{z \in C^\times : z^m = 1\}.$$

Then μ is an abelian torsion group and μ_{p^∞} is the p-Sylow subgroup of μ, i.e., the maximal p-subgroup of μ.

Put

$$\chi_p(x) = \exp(2\pi\sqrt{-1}\ f(x)) \qquad (x \in Q_p).$$

Then

$$\chi_p : Q_p \to T$$

and $Z_p \subset \mathrm{Ker}\ \chi_p$.

<u>10:</u> EXAMPLE Suppose that $v(x) = -1$, so $x = \frac{k}{p} + y$ with $0 < k \leq p-1$ and $y \in Z_p$:

$$\chi_p(x) = \exp(2\pi\sqrt{-1}\ \frac{k}{p}) = \zeta^k,$$

where $\zeta = \exp(2\pi\sqrt{-1}/p)$ is a primitive p^{th} root of unity.

<u>11:</u> LEMMA χ_p is a unitary character.

PROOF Given $x,y \in Q_p$, write

$$\begin{aligned} &f(x+y) - f(x) - f(y) \\ &\quad = x + y - [x+y] - (x - [x]) - (y - [y]) \\ &\quad = [x] + [y] - [x+y] \in Z_p. \end{aligned}$$

But at the same time

$$f(x+y) - f(x) - f(y) \in Z[\tfrac{1}{p}].$$

Thus

$$f(x+y) - f(x) - f(y) \in Z[\tfrac{1}{p}] \cap Z_p = Z$$

and so

$$\exp(2\pi\sqrt{-1}(f(x+y) - f(x) - f(y)) = 1$$

or still,

$$\chi_p(x+y) = \chi_p(x)\chi_p(y).$$

Therefore $\chi_p : Q_p \to T$ is a homomorphism. As for continuity, it suffices to check this at 0, matters then being clear (since χ_p is trivial in a neighborhood of 0) (Z_p is open and $0 \in Z_p$).

<u>12:</u> LEMMA The kernel of χ_p is Z_p.

[A priori, the kernel of χ_p consists of those $x \in Q_p$ such that $f(x) \in Z$. Therefore

$$\text{Ker } \chi_p = Z_p.]$$

<u>13:</u> LEMMA The image of χ_p is μ_{p^∞}.

[A priori, the image of χ_p consists of the complex numbers of the form

$$\exp(2\pi\sqrt{-1}\,\frac{k}{p^m}) = \exp(2\pi\sqrt{-1}/p^m)^k.$$

Since $\exp(2\pi\sqrt{-1}/p^m)$ is a root of unity of order p^m, these roots generate μ_{p^∞} as m ranges over the positive integers.]

<u>14:</u> SCHOLIUM χ_p implements an isomorphism

$$Q_p/Z_p \approx \mu_{p^\infty}.$$

<u>15:</u> REMARK

$$x \in p^{-k}Z_p \iff p^k x \in Z_p$$

$$\iff \chi_p(p^k x) = 1$$

$$\iff \chi_p(x)^{p^k} = 1$$

$$\iff \chi_p(x) \in \mu_{p^k}.$$

<u>16:</u> RAPPEL Let p be a prime -- then a group is <u>p-primary</u> if every element has order a power of p.

<u>17:</u> RAPPEL Every abelian torsion group G is a direct sum of its p-primary subgroups G_p.

[Note: The p-primary component G_p is the p-Sylow subgroup of G.]

<u>18:</u> NOTATION $Z(p^\infty)$ is the p-primary component of Q/Z.

Therefore

$$Q/Z = \bigoplus_p Z(p^\infty).$$

<u>19:</u> LEMMA $Z(p^\infty)$ is isomorphic to μ_{p^∞}.

[$Z(p^\infty)$ is generated by the $1/p^n$ in Q/Z.]

Therefore

$$Q/Z \approx \bigoplus_p \mu_{p^\infty} \approx \bigoplus_p Q_p/Z_p.$$

[Note: Consequently,

$$\mathrm{End}(Q/Z) \approx \mathrm{End}(\bigoplus_p Q_p/Z_p)$$

$$\approx \prod_p \text{End}(Q_p/Z_p)$$

$$\approx \prod_p Z_p.]$$

<u>20:</u> REMARK $\hat{Z}_p$ is isomorphic to μ_{p^∞} (cf. #26 infra).

Given $t \in Q_p$, let L_t be left multiplication by t and put $\chi_{p,t} = \chi_p \circ L_t$ -- then $\chi_{p,t}$ is continuous and $\forall\ x \in Q_p$,

$$\chi_{p,t}(x) = \chi_p(tx).$$

[Note: Trivially, $\chi_{p,0} \equiv 1$. And $\forall\ t \neq 0$,

$$\text{con}\ \chi_{p,t} = p^{-v(t)}Z_p.$$

Proof:

$$\begin{aligned} x \in \text{con}\ \chi_{p,t} &\iff tx \in Z_p \\ &\iff |tx|_p \leq 1 \\ &\iff |x|_p \leq \frac{1}{|t|_p} = p^{v(t)} \\ &\iff x \in p^{-v(t)}Z_p.] \end{aligned}$$

Next

$$\begin{aligned} \chi_{p,t}(x+y) &= \chi_p(t(x+y)) \\ &= \chi_p(tx+ty) \\ &= \chi_p(tx)\chi_p(ty) \end{aligned}$$

$$= \chi_{p,t}(x)\chi_{p,t}(y).$$

Therefore $\chi_{p,t} \in \hat{Q}_p$.

Next

$$\chi_{p,t+s}(x) = \chi_p((t+s)x)$$

$$= \chi_p(tx+sx)$$

$$= \chi_p(tx)\chi_p(sx)$$

$$= \chi_{p,t}(x)\chi_{p,s}(x).$$

Therefore the arrow $\Xi_p:Q_p \to \hat{Q}_p$ that sends t to $\chi_{p,t}$ is a homomorphism.

<u>21:</u> LEMMA If $t \neq s$, then $\chi_{p,t} \neq \chi_{p,s}$.

PROOF If to the contrary, $\chi_{p,t} = \chi_{p,s}$, then $\forall\, x \in Q_p$, $\chi_p(tx) = \chi_p(sx)$ or still, $\forall\, x \in Q_p$, $\chi_p((t-s)x) = 1$. But $L_{t-s}:Q_p \to Q_p$ is an automorphism, hence χ_p is trivial, which it isn't.

<u>22:</u> LEMMA The set

$$\Xi_p(Q_p) = \{\chi_{p,t}:t \in Q_p\}$$

is dense in $\hat{Q}_p$.

PROOF Let H be the closure in $\hat{Q}_p$ of the $\chi_{p,t}$. Consider the quotient $\hat{Q}_p/H$ and to get a contradiction, assume that $H \neq \hat{Q}_p$, thus that there is a nontrivial $\xi \in \hat{\hat{Q}}_p$ ∨ By definition, $H^\perp$ is computed in $\hat{\hat{Q}}_p$, which by Pontryagin duality, is
which is trivial on H.

identified with Q_p, so spelled out

$$H^\perp = \{x \in Q_p : ev_{Q_p}(x) | H = 1\}.$$

Accordingly, for some x, $\xi = ev_{Q_p}(x)$, hence $\forall$ t,

$$\xi(\chi_{p,t}) = ev_{Q_p}(x)(\chi_{p,t})$$

$$= \chi_{p,t}(x) = \chi_p(tx) = 1,$$

which is possible only if x = 0 and this implies that ξ is trivial.

<u>23:</u> LEMMA The arrows

$$\begin{bmatrix} Q_p \to \Xi_p(Q_p) \\ \Xi_p(Q_p) \to Q_p \end{bmatrix}$$

are continuous.

Therefore $\Xi_p(Q_p)$ is a locally compact subgroup of $\hat{Q}_p$. But a locally compact subgroup of a locally compact group is closed. Therefore $\Xi_p(Q_p) = \hat{Q}_p$.

In summary:

<u>24:</u> THEOREM $\hat{Q}_p$ is topologically isomorphic to Q_p (via the arrow $\Xi_p : Q_p \to \hat{Q}_p$).

<u>25:</u> LEMMA Fix t -- then $\chi_{p,t} | Z_p = 1$ iff $t \in Z_p$.

PROOF Recall that the kernel of χ_p is Z_p.

- $t \in Z_p$, $x \in Z_p \Rightarrow tx \in Z_p \Rightarrow \chi_p(tx) = 1 \Rightarrow \chi_{p,t} | Z_p = 1$.

- $\chi_{p,t}|Z_p = 1 \Rightarrow \chi_{p,t}(1) = 1 \Rightarrow \chi_p(t) = 1 \Rightarrow t \in Z_p$.

<u>26:</u> APPLICATION $\hat{Z}_p$ is isomorphic to μ_{p^∞}.

[$\hat{Z}_p$ can be computed as $\hat{Q}_p/Z_p^\perp$. But $Z_p^\perp$, when viewed as a subset of Q_p, consists of those t such that $\chi_{p,t}|Z_p = 1$. Therefore

$$\hat{Z}_p \approx \hat{Q}_p/Z_p \approx Q_p/Z_p \approx \mu_{p^\infty}.]$$

<u>27:</u> NOTATION Let

$$\chi_\infty(x) = \exp(-2\pi\sqrt{-1}\,x) \quad (x \in R).$$

<u>28:</u> PRODUCT PRINCIPLE $\forall\ x \in Q$,

$$\prod_{p\leq\infty} \chi_p(x) = 1.$$

PROOF Take x positive -- then there exist primes $p_1,\ldots,p_n$ such that x admits a representation

$$x = \frac{N_1}{p_1^{\alpha_1}} + \frac{N_2}{p_2^{\alpha_2}} + \cdots + \frac{N_n}{p_n^{\alpha_n}} + M,$$

where the α_k are positive integers, the N_k are positive integers $(1 \leq N_k < p_k^{\alpha_k} - 1)$, and $M \in Z$. Appending a subscript to f, we have

$$f_{p_k}(x) = \frac{N_k}{p_k^{\alpha_k}},\ f_p(x) = 0\ (p \neq p_k,\ k = 1,2,\ldots,n).$$

Therefore

$$\prod_{p<\infty} \chi_p(x) = \prod_{1\leq k\leq n} \chi_{p_k}(x)$$

$$= \prod_{1\le k\le n} \exp(2\pi\sqrt{-1}\ f_{p_k}(x))$$

$$= \exp(2\pi\sqrt{-1}\ \sum_{k=1}^{n} f_{p_k}(x))$$

$$= \exp(2\pi\sqrt{-1}\ (x-M))$$

$$= \exp(2\pi\sqrt{-1}\ x)$$

=>

$$\prod_{p\le\infty} \chi_p(x) = \prod_{p<\infty} \chi_p(x)\chi_\infty(x)$$

$$= \exp(2\pi\sqrt{-1}\ x)\exp(-\ 2\pi\sqrt{-1}\ x)$$

$$= 1.$$

APPENDIX

Let K be a finite extension of Q_p.

<u>1:</u> THEOREM The topological groups K and $\hat{K}$ are topologically isomorphic.

[Put

$$\chi_{K,p}(a) = \exp(2\pi\sqrt{-1}\ f(\mathrm{tr}_{K/Q_p}(a)))$$

$$= \chi_p(\mathrm{tr}_{K/Q_p}(a))$$

and given $b \in K$, put

$$\chi_{K,p,b}(a) = \chi_{K,p}(ab).$$

Proceed from here as above.]

2: REMARK Every character of K is unitary.

3: LEMMA

$$\left[\begin{array}{l} a \in R \Rightarrow tr_{K/Q_p}(a) \in Z_p \\ \\ a \in P \Rightarrow tr_{K/Q_p}(a) \in pZ_p. \end{array}\right.$$

4: DEFINITION The <u>differential of K</u> is the set

$$\Delta_K = \{b \in K : tr_{K/Q_p}(Rb) \subset Z_p\}.$$

5: LEMMA Δ_K is a proper R-submodule of K containing R.

6: LEMMA There exists a unique nonnegative integer d -- <u>the differential exponent of K</u> -- characterized by the condition that

$$\pi^{-d}R = \Delta_K.$$

[This follows from the theory of "fractional ideals" (details omitted).]

[Note: $\chi_{K,p}$ is trivial on $\pi^{-d}R$ but is nontrivial on $\pi^{-d-1}R$.]

7: LEMMA Let e be the ramification index of K over Q_p (cf. §5, #17) -- then

$$a \in P^{-e+1} \Rightarrow tr_{K/Q_p}(a) \in Z_p.$$

PROOF Let

$$a \in P^{-e+1} = \pi^{-e+1}R = \pi^{-e}(\pi R) = \pi^{-e}P,$$

so $a = \pi^{-e}b$ $(b \in P)$. Write $p = \pi^{e}u$ and consider pa:

$$pa = \pi^{e}u\pi^{-e}b = ub.$$

But

$$|u| = 1,\ |b| < 1 \Rightarrow |ub| < 1$$

$$\Rightarrow ub \in P$$

$$\Rightarrow tr_{K/Q_p}(ub) \in pZ_p$$

$$\Rightarrow tr_{K/Q_p}(pa) \in pZ_p$$

$$\Rightarrow p\ tr_{K/Q_p}(a) \in pZ_p \Rightarrow tr_{K/Q_p} \in Z_p.$$

<u>8:</u> APPLICATION

$$d \geq e-1.$$

[It suffices to show that

$$P^{-e+1} \subset \Delta_K \ (\equiv \pi^{-d}R).$$

Thus let $a \in P^{-e+1}$, say $a = \pi^{e}b$ $(b \in P)$, and let $r \in R$ -- then the claim is that

$$tr_{K/Q_p}(ar) \in Z_p.$$

But

$$ar = \pi^{-e}br \in \pi^{e}P \quad (|br| < 1)$$

or still,

$$ar \in P^{-e+1} \Rightarrow tr_{K/Q_p}(ar) \in Z_p.]$$

9: REMARK Therefore $d = 0 \Rightarrow e = 1$, hence in this situation, K is unramified.

[Note: There is also a converse, viz. if K is unramified, then $d = 0$.]

10: N.B. It can be shown that

$$\mathrm{tr}_{K/\mathbb{Q}_p}(R) = \mathbb{Z}_p$$

iff $d = e-1$.

11: CRITERION Fix $b \in K$ -- then

$$b \in \Delta_K \Leftrightarrow \forall\, a \in R,\ \chi_{K,p}(ab) = 1.$$

PROOF

- $a \in R,\ b \in \Delta_K \Rightarrow ab \in \Delta_K$

$$\Rightarrow \mathrm{tr}_{K/\mathbb{Q}_p}(ab) \in \mathbb{Z}_p$$

$\Rightarrow$

$$\chi_{K,p}(ab) = \chi_p(\mathrm{tr}_{K/\mathbb{Q}_p}(ab)) = 1.$$

- $\forall\, a \in R,\ \chi_{K,p}(ab) = 1$

$$\Rightarrow \forall\, a \in R,\ \mathrm{tr}_{K/\mathbb{Q}_p}(ab) \in \mathbb{Z}_p \Rightarrow b \in \Delta_K.$$

Normalize the Haar measure on K by the condition

$$\mu_K(R) = \int_R da = q^{-d/2}.$$

Let χ_R be the characteristic function of R -- then

$$\int_K \chi_R(a)\chi_{K,p}(ab)da = \int_R \chi_{K,p}(ab)da.$$

- $b \in \Delta_K \Rightarrow \chi_{K,p}(ab) = 1 \quad (\forall\ a \in R)$

$$\Rightarrow \int_R \chi_{K,p}(ab)da = \mu_K(R) = q^{-d/2}.$$

- $b \notin \Delta_K \Rightarrow \chi_{K,p}(ab) \neq 1 \quad (\exists\ a \in R)$

$$\Rightarrow \int_R \chi_{K,p}(ab)da = 0.$$

Consequently, as a function of b,

$$\int_R \chi_{K,p}(ab)da = q^{-d/2}\chi_{\Delta_K}(b),$$

χ_{Δ_K} the characteristic function of Δ_K.

<u>12:</u> LEMMA

$$[\pi^{-d}R:R] = q^d.$$

Therefore

$$\mu_K(\Delta_K) = \mu_K(\pi^{-d}R)$$

$$= q^d\mu_K(R)$$

$$= q^d q^{-d/2} = q^{d/2}.$$

<u>13:</u> LEMMA $\forall\ a \in K$,

$$\int_K q^{-d/2}\chi_{\Delta_K}(b)\chi_{K,p}(ab)db = \chi_R(a).$$

PROOF The left hand side reduces to

$$q^{-d/2} \int_{\Delta_K} \chi_{K,p}(ab)\,db$$

and there are two possibilities.

- $a \in R \Rightarrow ab \in \Delta_K \quad (\forall\, b \in \Delta_K)$

  $\Rightarrow tr_{K/\mathbb{Q}_p}(ab) \in \mathbb{Z}_p \Rightarrow \chi_{K,p}(ab) = 1$

  $\Rightarrow$

  $$q^{-d/2} \int_{\Delta_K} \chi_{K,p}(ab)\,db$$

  $$= q^{-d/2}\mu_K(\Delta_K) = q^{-d/2}q^{d/2}$$

  $$= 1.$$

- $a \notin R: \chi_{K,p}(ab) \neq 1 \quad (\exists\, b \in \Delta_K)$

  $\Rightarrow$

  $$q^{-d/2} \int_{\Delta_K} \chi_{K,p}(ab)\,db = 0.$$

To detail the second point of this proof, work with the normalized absolute value (cf. §6, #18) and recall that $|\pi|_K = \frac{1}{q}$ (cf. §5, #21). Accordingly,

$$x \in \pi^n R \iff |x|_K \leq q^{-n}.$$

Fix $a \notin R$ -- then the claim is that $b \to \chi_{K,p}(ab)$ $(b \in \Delta_K)$ is nontrivial. For

$$\chi_{K,p}(ab) = 1 \iff ab \in \pi^{-d}R$$

$$\iff |ab|_K \leq q^d$$

$$\iff |a|_K |b|_K \leq q^d$$

$$\iff |b|_K \leq \frac{q^d}{|a|_K} = q^{d+v(a)}.$$

But

$$a \notin R \Rightarrow v(a) < 0$$

$$\Rightarrow -v(a) > 0 \Rightarrow -d-v(a) > -d$$

$$\Rightarrow \pi^{-d-v(a)}R \subset \pi^{-d}R,$$

a proper containment.

§9. *MULTIPLICATIVE p-ADIC CHARACTER THEORY*

Recall that

$$Q_p^\times \approx Z \times Z_p^\times,$$

the abstract reflection of the fact that for every $x \in Q_p^\times$, there is a unique $v(x) \in Z$ and a unique $u(x) \in Z_p^\times$ such that $x = p^{v(x)}u(x)$. Therefore

$$\widehat{(Q_p^\times)} \approx \hat{Z} \times \widehat{(Z_p^\times)} \approx T \times \widehat{(Z_p^\times)}.$$

<u>1:</u> <u>N.B.</u> A character of Q_p is necessarily unitary (cf. §8, #4) but this is definitely not the case for $Q_p^\times$ (cf. infra).

<u>2:</u> DEFINITION A character $\chi:Q_p^\times \to C^\times$ is <u>unramified</u> if it is trivial on $Z_p^\times$.

<u>3:</u> EXAMPLE Given any complex number s, the arrow $x \to |x|_p^s$ is an unramified character of $Q_p^\times$.

<u>4:</u> LEMMA If $\chi:Q_p^\times \to C^\times$ is an unramified character, then there exists a complex number s such that $\chi = |\cdot|_p^s$.

PROOF Such a χ factors through the projection $Q_p^\times \to p^Z$ defined by $x \to |x|_p$, hence gives rise to a character $\tilde{\chi}:p^Z \to C^\times$ which is completely determined by its value on p, say $\tilde{\chi}(p) = p^s$ for the complex number

$$s = \frac{\log \tilde{\chi}(p)}{\log p},$$

itself determined up to an integral multiple of

$$\frac{2\pi\sqrt{-1}}{\log p}.$$

Therefore

$$\begin{aligned}\chi(x) &= \tilde{\chi}(|x|_p) \\ &= \tilde{\chi}(p^{-v(x)}) \\ &= (\tilde{\chi}(p))^{-v(x)} \\ &= (p^s)^{-v(x)} = (p^{-v(x)})^s = |x|_p^s.\end{aligned}$$

[Note: For the record,

$$\begin{aligned}|x|_p^{2\pi\sqrt{-1}/\log p} &= (p^{-v(x)})^{2\pi\sqrt{-1}/\log p} \\ &= (e^{-v(x)\log p})^{2\pi\sqrt{-1}/\log p} \\ &= e^{-v(x)2\pi\sqrt{-1}} = 1.]\end{aligned}$$

Suppose that $\chi:Q_p^\times \to C^\times$ is a character -- then χ can be written as

$$\chi(x) = |x|_p^s \, \underline{\chi}(u(x)),$$

where $s \in C$ and $\underline{\chi} \equiv \chi|Z_p^\times \in \widehat{(Z_p^\times)}$, thus χ is unitary iff s is pure imaginary.

<u>5:</u> LEMMA If $\underline{\chi} \in \widehat{(Z_p^\times)}$ is nontrivial, then there is an $n \in N$ such that $\underline{\chi} \equiv 1$ on $U_{p,n}$ but $\chi \not\equiv 1$ on $U_{p,n-1}$ (cf. §8, #5).

Assume again that $\chi:Q_p^\times \to C^\times$ is a character.

<u>6:</u> DEFINITION χ is <u>ramified of degree $n \geq 1$</u> if $\underline{\chi}|U_{p,n} \equiv 1$ and $\underline{\chi}|U_{p,n-1} \not\equiv 1$.

<u>7:</u> DEFINITION The <u>conductor</u> con χ of χ is $Z_p^\times$ if χ is unramified and $U_{p,n}$ if χ is ramified of degree n.

<u>8:</u> RAPPEL If G is a finite abelian group, then the number of unitary characters of G is card G.

<u>9:</u> LEMMA

$$[Z_p^\times:U_{p,1}] = p-1 \quad \text{(cf. §4, \#40)}$$

and

$$[U_{p,1}:U_{p,n}] = p^{n-1}.$$

If χ is ramified of degree n, then $\underline{\chi}$ can be viewed as a unitary character of $Z_p^\times/U_{p,n}$. But the quotient $Z_p^\times/U_{p,n}$ is a finite abelian group, thus has

$$\text{card } Z_p^\times/U_{p,n} = [Z_p^\times:U_{p,n}]$$

unitary characters. And

$$[Z_p^\times:U_{p,n}] = [Z_p^\times:U_{p,1}] \cdot [U_{p,1}:U_{p,n}]$$

$$= (p-1)p^{n-1},$$

this being the number of unitary characters of $Z_p^\times$ of degree $\leq$ n. Therefore the group $Z_p^\times$ has p-2 unitary characters of degree 1 and for $n \geq 2$, the group $Z_p^\times$ has

$$(p-1)p^{n-1} - (p-1)p^{n-2} = p^{n-2}(p-1)^2$$

unitary characters of degree n.

10: LEMMA Let $\chi \in \widehat{Q_p^\times}$ -- then

$$\chi(x) = |x|_p^{\sqrt{-1}t}\underline{\chi}(u(x)),$$

where t is real and

$$-(\pi/\log p) < t \leq \pi/\log p.$$

APPENDIX

Suppose that $p \neq 2$, let $\tau \in Q_p^\times - (Q_p^\times)^2$, and form the quadratic extension

$$Q_p(\tau) = \{x + y\sqrt{\tau} : x, y \in Q_p\}.$$

1: NOTATION Let $Q_{p,\tau}$ be the set of points of the form $x^2 - \tau y^2$ $(x \neq 0, y \neq 0)$.

2: LEMMA $Q_{p,\tau}$ is a subgroup of $Q_p^\times$ containing $(Q_p^\times)^2$.

3: LEMMA

$$[Q_p^\times : Q_{p,\tau}] = 2 \text{ and } [Q_{p,\tau} : (Q_p^\times)^2] = 2.$$

[Note:

$$[Q_p^\times : (Q_p^\times)^2] = 4 \quad (\text{cf. §4, \#53}).]$$

<u>4:</u> DEFINITION Given $x \in Q_p^\times$, let

$$\mathrm{sgn}_\tau(x) = \begin{cases} 1 \text{ if } x \in Q_{p,\tau} \\ -1 \text{ if } x \notin Q_{p,\tau}. \end{cases}$$

<u>5:</u> LEMMA sgn_τ is a unitary character of $\hat{Q}_p$.

§10. *TEST FUNCTIONS*

The Schwartz space $S(R^n)$ consists of those complex valued C^∞ functions which, together with all their derivatives, vanish at infinity faster than any power of $||\cdot||$.

1: DEFINITION. The elements f of $S(R^n)$ are the test functions on R^n.

2: EXAMPLE Take n = 1 -- then

$$f(x) = Cx^A \exp(-\pi x^2),$$

where A = 0 or 1, is a test function, said to be standard. Here

$$\int_R x^A \exp(-\pi x^2) e^{2\pi\sqrt{-1}\,tx} dx = (\sqrt{-1})^A t^A \exp(-\pi t^2),$$

thus F_R of a standard function is again standard (cf. §7, #51).

[Note: Henceforth, by definition, the Fourier transform of an $f \in L^1(R)$ will be the function

$$\hat{f}: R \to C$$

defined by the rule

$$\begin{aligned}\hat{f}(t) &= F_R f(t) \\ &= \int_R f(x) e^{2\pi\sqrt{-1}\,tx} dx.]\end{aligned}$$

3: EXAMPLE Take n = 2 and identify R^2 with C -- then

$$f(z) = Cz^A \bar{z}^B \exp(-2\pi|z|^2),$$

where $A,B \in Z_{\geq 0}$ & AB = 0, is a test function, said to be standard. Here

$$\int_C z^A \bar{z}^B \exp(-2\pi|z|^2)e^{2\pi\sqrt{-1}(wz+\bar{w}\bar{z})}|dz\wedge d\bar{z}|$$

$$= (\sqrt{-1})^{A+B} w^B \bar{w}^A \exp(-2\pi|w|^2),$$

thus F_C of a standard function is again standard (cf. §7, #53).

[Note: Henceforth, by definition, the Fourier transform of an $f \in L^1(C)$ will be the function

$$\hat{f}: C \to C$$

defined by the rule

$$\hat{f}(w) = F_C f(w)$$

$$= \int_C f(z)e^{2\pi\sqrt{-1}(wz+\bar{w}\bar{z})}|dz\wedge d\bar{z}|.]$$

<u>4:</u> DEFINITION Let G be a totally disconnected locally compact group -- then a function $f:G \to C$ is said to be <u>locally constant</u> if for any $x \in G$, there is an open subset U_x of G containing x such that f is constant on U_x.

<u>5:</u> LEMMA A locally constant function f is continuous.

PROOF Fix $x \in G$ and suppose that $\{x_i\}$ is a net converging to x -- then x_i is eventually in U_x, hence there $f(x_i) = f(x)$.

<u>6:</u> DEFINITION The <u>Bruhat space</u> $\mathcal{B}(G)$ consists of those complex valued locally constant functions whose support is compact.

[Note: $\mathcal{B}(G)$ carries a "canonical topology" but I shall pass in silence as regards to its precise formulation.]

7: DEFINITION The elements f of $\mathcal{B}(G)$ are the test functions on G.

8: LEMMA Given a test function f, there exists an open-compact subgroup K of G, an integer $n \geq 0$, elements $x_1,\ldots,x_n$ in G and elements $c_1,\ldots,c_n$ in C such that the union $\bigcup_{k=1}^{n} Kx_kK$ is disjoint and

$$f = \sum_{k=1}^{n} c_k\chi_{Kx_kK},$$

χ_{Kx_kK} the characteristic function of Kx_kK.

PROOF Since f is locally constant, for every $z \in C$ the preimage $f^{-1}(z)$ is an open subset of G. Therefore $X = \{x:f(x) \neq 0\}$ is the support of f. This said, given $x \in X$, define a map $\phi_x:G \times G \to C$ by $\phi_x(x_1,x_2) = f(x_1xx_2)$, thus $\phi_x(e,e) = f(x)$ and ϕ_x is continuous if C has the discrete topology. Consequently, one can find an open-compact subgroup K_x of G such that ϕ_x is constant on $K_x \times K_x$. Put $U_x = K_xxK_x$ — then U_x is open-compact and f is constant on U_x. But X is covered by the U_x, hence, being compact, is covered by finitely many of them. Bearing in mind that distinct double cosets are disjoint, consider now the intersection K of the finitely many K_x that occur.

Specialize and let $G = Q_p$.

9: EXAMPLE If $K \subset Q_p$ is open-compact, then its characteristic function χ_K is a test function on Q_p.

10: LEMMA Every $f \in \mathcal{B}(Q_p)$ is a finite linear combination of functions of the form

$$\chi_{x+p^n Z_p} \quad (x \in Q_p,\ n \in Z).$$

[This is an instance of #8 or argue directly (cf. §4, #33).]

11: DEFINITION Given $f \in L^1(Q_p)$, its Fourier transform is the function

$$\hat{f}: Q_p \to C$$

defined by the rule

$$\hat{f}(t) = \int_{Q_p} f(x)\chi_{p,t}(x)dx$$

$$= \int_{Q_p} f(x)\chi_p(tx)dx.$$

12: LEMMA $\forall\ f \in L^1(Q_p)$,

$$\hat{\bar{f}}(t) = \overline{\hat{f}(-t)}.$$

PROOF

$$\hat{\bar{f}}(t) = \int_{Q_p} \overline{f(x)}\chi_p(tx)dx$$

$$= \int_{Q_p} \overline{f(x)\chi_p(-tx)}dx$$

$$= \int_{Q_p} \overline{f(x)\chi_p((-t)x)}dx$$

$$= \overline{\int_{Q_p} f(x)\chi_p((-t)x)dx}$$

$$= \overline{\hat{f}(-t)}.$$

13: SUBLEMMA

$$\int_{p^n Z_p} \chi_p(x)\,dx = \begin{cases} p^{-n} & (n \geq 0) \\ 0 & (n < 0). \end{cases}$$

[Recall that

$$\mu_{Q_p}(p^n Z_p) = p^{-n}$$

and apply §7, #46 and §8, #12.]

14: LEMMA Take $f = \chi_{p^n Z_p}$ -- then

$$\hat{\chi}_{p^n Z_p} = p^{-n}\chi_{p^{-n} Z_p}.$$

PROOF

$$\hat{\chi}_{p^n Z_p}(t) = \int_{Q_p} \chi_{p^n Z_p}(x)\chi_{p,t}(x)\,dx$$

$$= \int_{Q_p} \chi_{p^n Z_p}(x)\chi_p(tx)\,dx$$

$$= |t|_p^{-1} \int_{Q_p} \chi_{p^n Z_p}(t^{-1}x)\chi_p(x)\,dx$$

$$= |t|_p^{-1} \int_{p^{n+v(t)} Z_p} \chi_p(x)\,dx.$$

The last integral equals

$$p^{-n-v(t)}$$

if $n+v(t) \geq 0$ and equals 0 if $n+v(t) < 0$ (cf. #13). But

$$t \in p^{-n}Z_p \iff v(t) \geq -n \iff n+v(t) \geq 0.$$

Since

$$|t|_p^{-1} \, p^{v(t)} = 1,$$

it therefore follows that

$$\hat{\chi}_{p^nZ_p} = p^{-n}\chi_{p^{-n}Z_p}.$$

In particular:

$$\hat{\chi}_{Z_p} = \chi_{Z_p}.$$

<u>15:</u> THEOREM Take $f = \chi_{x+p^nZ_p}$ -- then

$$\hat{\chi}_{x+p^nZ_p}(t) = \begin{cases} \chi_p(tx)p^{-n} & (|t|_p \leq p^n) \\ 0 & (|t|_p > p^n). \end{cases}$$

PROOF

$$\begin{aligned}\hat{\chi}_{x+p^nZ_p}(t) &= \int_{Q_p} \chi_{x+p^nZ_p}(y)\chi_{p,t}(y)dy \\ &= \int_{Q_p} \chi_{x+p^nZ_p}(y)\chi_p(ty)dy \\ &= \int_{x+p^nZ_p} \chi_p(ty)dy \\ &= \int_{p^nZ_p} \chi_p(t(x+y))dy\end{aligned}$$

$$= \int_{p^n Z_p} \chi_p(tx+ty)\,dy$$

$$= \int_{p^n Z_p} \chi_p(tx)\chi_p(ty)\,dy$$

$$= \chi_p(tx)\int_{p^n Z_p} \chi_p(ty)\,dy$$

$$= \chi_p(tx)\int_{Q_p} \chi_{p^n Z_p}(y)\chi_p(ty)\,dy$$

$$= \chi_p(tx)\int_{Q_p} \chi_{p^n Z_p}(y)\chi_{p,t}(y)\,dy$$

$$= \chi_p(tx)\hat{\chi}_{p^n Z_p}(t)$$

$$= \chi_p(tx)p^{-n}\chi_{p^{-n} Z_p}(t).$$

<u>16:</u> APPLICATION Taking into account #10,

$$f \in \mathcal{B}(Q_p) \Rightarrow \hat{f} \in \mathcal{B}(Q_p).$$

<u>17:</u> THEOREM $\forall\, f \in \mathrm{INV}(Q_p)$,

$$\hat{\hat{f}}(x) = f(-x) \quad (x \in Q_p).$$

PROOF It suffices to check this for a single function, so take $f = \chi_{Z_p}$ — then, as noted above,

$$\hat{\chi}_{Z_p} = \chi_{Z_p},$$

thus $\forall$ x,

$$\hat{\hat{\chi}}_{Z_p}(x) = \chi_{Z_p}(x) = \chi_{Z_p}(-x).$$

18: N.B. It is clear that

$$\mathcal{B}(Q_p) \subset \text{INV}(Q_p).$$

19: SCHOLIUM The arrow $f \to \hat{f}$ is a linear bijection of $\mathcal{B}(Q_p)$ onto itself. [Injectivity is manifest. As for surjectivity, the arrow $f \to \check{f}$, where

$$\check{f}(x) = f(-x),$$

maps $\mathcal{B}(Q_p)$ into itself. And

$$f = \check{\check{f}} = (\check{f})^{\vee} = (\check{f}\,)^{\wedge\wedge} = ((\check{f}\,)^{\wedge})^{\wedge}.]$$

20: REMARK As is well-known, the same conclusion obtains if Q_p is replaced by R or C.

Pass now from Q_p to $Q_p^\times$.

21: LEMMA Let $f \in \mathcal{B}(Q_p^\times)$ -- then $\exists\ n \in N$:

$$\begin{cases} |x|_p < p^{-n} \Rightarrow f(x) = 0 \\ |x|_p > p^n \Rightarrow f(x) = 0. \end{cases}$$

Therefore an element f of $\mathcal{B}(Q_p^\times)$ can be viewed as an element of $\mathcal{B}(Q_p)$ with the property that $f(0) = 0$.

22: DEFINITION Given $f \in L^1(Q_p^\times, d^\times x)$, its Mellin transform $\tilde{f}$ is the Fourier transform of f per $Q_p^\times$:

$$\tilde{f}(\chi) = \int_{Q_p^\times} f(x)\chi(x)d^\times x.$$

[Note: By definition,

$$d^\times x = \frac{p}{p-1}\frac{dx}{|x|_p} \quad \text{(cf. §6, \#26)},$$

so

$$\text{vol}_{d^\times x}(Z_p^\times) = \text{vol}_{dx}(Z_p) = 1.]$$

23: EXAMPLE Take $f = \chi_{Z_p^\times}$ -- then

$$\tilde{\chi}_{Z_p^\times}(\chi) = \int_{Q_p^\times} \chi_{Z_p^\times}(x)\chi(x)d^\times x$$

$$= \int_{Z_p^\times} \chi(x)d^\times x.$$

Decompose χ as in §9, #10, hence

$$\int_{Z_p^\times} \chi(x)d^\times x = \int_{Z_p^\times} |x|_p^{\sqrt{-1}\, t} \underline{\chi}(p^{-v(x)}x)d^\times x$$

$$= \int_{Z_p^\times} \underline{\chi}(x)d^\times x$$

$$= \begin{cases} 0 & (\underline{\chi} \not\equiv 1) \\ 1 & (\underline{\chi} \equiv 1). \end{cases}$$

According to §9, #2, a unitary character $\chi \in \widehat{(Q_p^\times)}$ is unramified if its restriction $\underline{\chi}$ to $Z_p^\times$ is trivial. Therefore the upshot is that the Mellin transform of $\chi_{Z_p^\times}$ is the characteristic function of the set of unramified elements of $\widehat{(Q_p^\times)}$.

APPENDIX

Let K be a finite extension of Q_p -- then

$$K^\times \approx Z \times R^\times$$

and the generalities developed in §9 go through with but minor changes when Q_p is replaced by K.

In particular: $\forall\ \chi \in \hat{K}^\times$, there is a splitting

$$\chi(a) = |a|_K^{\sqrt{-1}\ t} \underline{\chi}(\pi^{-v(a)} a),$$

where t is real and

$$-(\pi/\log q) < t \leq \pi/\log q.$$

[Note: χ is unramified if it is trivial on $R^\times$.]

1. N.B. The "π" in the first instance is a prime element (cf. §5, #10) and $|\pi|_K = \frac{1}{q}$. On the other hand, the "π" in the second instance is 3.14... .

The extension of the theory from $\mathcal{B}(Q_p)$ to $\mathcal{B}(K)$ is straightforward, the point of departure being the observation that

$$\int_{\pi^n R} \chi_{K,p}(a)\,da = \mu_K(R) \begin{cases} q^{-n} & (n = -d, -d+1, \ldots) \\ 0 & (n = -d-1, -d-2, \ldots). \end{cases}$$

2: CONVENTION Normalize the Haar measure on K by stipulating that $\int_R da = q^{-d/2}$.

3: DEFINITION Given $f \in L^1(K)$, its Fourier transform is the function

$$\hat{f}: K \to C$$

defined by the rule

$$\hat{f}(b) = \int_K f(a)\chi_{K,p,b}(a)da$$

$$= \int_K f(a)\chi_{K,p}(ab)da.$$

4: THEOREM $\forall f \in \text{INV}(K)$,

$$\hat{\hat{f}}(a) = f(-a) \quad (a \in K).$$

PROOF It suffices to check this for a single function, so take $f = \chi_R$, in which case the work has already been done in the Appendix to §8. To review:

- $$\hat{\chi}_R(b) = \int_K \chi_R(a)\chi_{K,p}(ab)da$$

$$= \int_R \chi_{K,p}(ab)da$$

$$= q^{-d/2}\chi_{\Delta_K}(b).$$

- $$\int_K q^{-d/2}\chi_{\Delta_K}(b)\chi_{K,p}(ab)db$$

$$= q^{-d/2}\int_{\Delta_K}\chi_{K,p}(ab)db$$

$$= \chi_R(a) \quad \text{(loc. cit., \#13)}$$

$$= \chi_R(-a).$$

5: N.B. It is clear that

$$\mathcal{B}(K) \subset \mathrm{INV}(K).$$

6: SCHOLIUM The arrow $f \to \hat{f}$ is a linear bijection of $\mathcal{B}(K)$ onto itself.

7: CONVENTION Put

$$d^{\times}a = \frac{q}{q-1}\,\frac{da}{|a|_K}.$$

Then $d^{\times}a$ is a Haar measure on $K^{\times}$ and

$$\mathrm{vol}_{d^{\times}a}(R^{\times}) = \mathrm{vol}_{da}(R) = q^{-d/2}.$$

8: DEFINITION Given $f \in L^1(K^{\times}, d^{\times}a)$, its Mellin transform $\tilde{f}$ is the Fourier transform of f per $K^{\times}$:

$$\tilde{f}(\chi) = \int_{K^{\times}} f(a)\chi(a)\,d^{\times}a.$$

9: EXAMPLE Take $f = \chi_{R^{\times}}$ -- then

$$\tilde{\chi}_{R^{\times}}(\chi) = \begin{cases} 0 & (\underline{\chi} \not\equiv 1) \\ q^{-d/2} & (\chi \equiv 1). \end{cases}$$

§11. *LOCAL ZETA FUNCTIONS*: $R^\times$ *or* $C^\times$

We shall first consider $R^\times$, hence $\tilde{R}^\times \approx Z/2Z \times C$ and every character has the form

$$\chi(x) \equiv \chi_{\sigma,s}(x) = (\text{sgn } x)^\sigma |x|^s \quad (\sigma \in \{0,1\},\ s \in C) \quad (\text{cf. §7, \#11}).$$

1. DEFINITION Given $f \in S(R)$ and a character $\chi : R^\times \to C^\times$, the local zeta function attached to the pair (f,χ) is

$$Z(f,\chi) = \int_{R^\times} f(x)\chi(x)d^\times x,$$

where $d^\times x = \frac{dx}{|x|}$.

[Note: The parameters σ and s are implicit:

$$Z(f,\chi) \equiv Z(f,\chi_{\sigma,s}).]$$

2: LEMMA The integral defining $Z(f,\chi)$ is absolutely convergent for $\text{Re}(s) > 0$.

PROOF Since f is Schwartz, there are no issues at infinity. As for what happens at the origin, let $I =]-1,1[-\{0\}$ and fix $C > 0$ such that $|f(x)| \leq C$ $(x \in I)$ -- then

$$|Z(f,\chi)| \leq \int_{R-\{0\}} |f(x)|\ |x|^{\text{Re}(s)-1} dx$$

$$\leq \left(\int_{R-I} + \int_I\right) |f(x)|\ |x|^{\text{Re}(s)-1} dx$$

$$\leq M + C \int_I |x|^{\text{Re}(s)-1} dx,$$

a finite quantity.

<u>3:</u> LEMMA $Z(f,\chi)$ is a holomorphic function of s in the strip $\text{Re}(s) > 0$.

[Formally,

$$\frac{d}{ds} Z(f,\chi) = \int_{R^\times} f(x)(\text{sgn } x)^\sigma (\log |x|)|x|^s d^\times x,$$

and while correct, "differentiation under the integral sign" does require a formal proof... .]

<u>4:</u> NOTATION Put

$$\check{\chi} = \chi^{-1}|.|.$$

The integral defining $Z(f,\check{\chi})$ is absolutely convergent if $\text{Re}(1-s) > 0$, i.e., if $1 - \text{Re}(s) > 0$ or still, if $\text{Re}(s) < 1$.

<u>5:</u> LEMMA Let $f,g \in \mathcal{S}(R)$ and suppose that $0 < \text{Re}(s) < 1$ -- then

$$Z(f,\chi)Z(\hat{g},\check{\chi}) = Z(\hat{f},\check{\chi})Z(g,\chi).$$

PROOF Write

$$Z(f,\chi)Z(\hat{g},\check{\chi})$$

$$= \iint_{R^\times \times R^\times} f(x)\hat{g}(y)\chi(xy^{-1})|y|d^\times x\, d^\times y$$

and make the substitution $t = yx^{-1}$ to get

$$Z(f,\chi)Z(\hat{g},\check{\chi})$$

$$= \int_{R^\times} (\int_{R^\times} f(x)\hat{g}(tx)|x|d^\times x)\chi(t^{-1})|t|d^\times t.$$

The claim now is that the inner integral is symmetric in f and g (which then implies that

$$Z(f,\chi)Z(\hat{g},\check{\chi}) = Z(g,\chi)Z(\hat{f},\check{\chi}),$$

the desired equality). To see that this is so, observe first that

$$|x|du\cdot d^{\times}x = |u|dx\cdot d^{\times}u.$$

Since $R^{\times}$ and R differ by a single element, it therefore follows that

$$\int_{R^{\times}} f(x)\hat{g}(tx)|x|d^{\times}x$$

$$= \int_{R^{\times}} f(x)|x|(\int_R g(u)e^{2\pi\sqrt{-1}\,txu}du)d^{\times}x$$

$$= \int\int_{R\times R^{\times}} f(x)g(u)|x|e^{2\pi\sqrt{-1}\,txu}dud^{\times}x$$

$$= \int_{R^{\times}} g(u)|u|(\int_R f(x)e^{2\pi\sqrt{-1}\,txu}dx)d^{\times}u$$

$$= \int_{R^{\times}} g(u)\hat{f}(tu)|u|d^{\times}u.$$

Fix $\phi \in S(R)$ and put

$$\rho(\chi) = \frac{Z(\phi,\chi)}{Z(\hat{\phi},\check{\chi})}.$$

Then $\rho(\chi)$ is independent of the choice of ϕ and $\forall\ f \in S(R)$, the functional equation

$$Z(f,\chi) = \rho(\chi)Z(\hat{f},\check{\chi})$$

obtains.

6: LEMMA $\rho(\chi)$ is a meromorphic function of s (cf. infra).

7: APPLICATION $\forall\, f \in S(R)$, $Z(f,\chi)$ admits a meromorphic continuation to the whole s-plane.

8: NOTATION Set

$$\Gamma_R(s) = \pi^{-s/2}\Gamma(s/2).$$

9: DEFINITION Write

$$L(\chi) = \begin{cases} \Gamma_R(s) & (\sigma = 0) \\ \Gamma_R(s+1) & (\sigma = 1). \end{cases}$$

Proceeding to the computation of $\rho(\chi)$, distinguish two cases.

- $\sigma = 0$ Take $\phi_0(x)$ to be $e^{-\pi x^2}$ — then

$$\begin{aligned} Z(\phi_0,\chi) &= \int_{R^\times} e^{-\pi x^2} |x|^s d^\times x \\ &= 2 \int_0^\infty e^{-\pi x^2} x^{s-1} dx \\ &= \pi^{-s/2}\Gamma(s/2) = \Gamma_R(s) = L(\chi). \end{aligned}$$

Next $\hat{\phi}_0 = \phi_0$ (cf. §10, #2) so by the above argument,

$$Z(\hat{\phi}_0,\check{\chi}) = L(\check{\chi}),$$

from which

$$\rho(\chi) = \frac{L(\chi)}{L(\check{\chi})}$$

$$= \frac{\pi^{-s/2}\Gamma(\frac{s}{2})}{\pi^{-(1-s)/2}\Gamma(\frac{1-s}{2})}$$

$$= 2^{1-s}\pi^{-s} \cos(\frac{\pi s}{2})\Gamma(s).$$

• $\underline{\sigma = 1}$ Take $\phi_1(x)$ to be $xe^{-\pi x^2}$ -- then

$$Z(\phi_1,\chi) = \int_{R^\times} xe^{-\pi x^2} \frac{x}{|x|} |x|^s d^\times x$$

$$= \int_{R^\times} e^{-\pi x^2} |x|^{s+1} d^\times x$$

$$= 2 \int_0^\infty e^{-\pi x^2} x^s dx$$

$$= \pi^{-(s+1)/2} \Gamma(\frac{s+1}{2})$$

$$= \Gamma_R(s+1) = L(\chi).$$

Next

$$\hat{\phi}_1(t) = \sqrt{-1}\, t \exp(-\pi t^2) \qquad \text{(cf. §10, \#2).}$$

Therefore

$$Z(\hat{\phi}_1,\check{\chi}) = \sqrt{-1} \int_{R^\times} xe^{-\pi x^2} \cdot \frac{x}{|x|} \cdot |x|^{1-s} d^\times x$$

$$= \sqrt{-1} \int_{R^\times} e^{-\pi x^2} |x|^{2-s} d^\times x$$

$$= \sqrt{-1}\, 2 \int_0^\infty e^{-\pi x^2} x^{1-s} dx$$

$$= \sqrt{-1}\ \pi^{-(2-s)/2}\Gamma(\tfrac{2-s}{2})$$

$$= \sqrt{-1}\ \Gamma_R(2-s) = \sqrt{-1}\ L(\check{\chi}).$$

Accordingly

$$\rho(\chi) = -\sqrt{-1}\ \frac{L(\chi)}{L(\check{\chi})}$$

$$= -\sqrt{-1}\ \frac{\pi^{-(s+1)/2}\Gamma(\frac{s+1}{2})}{\pi^{(s-2)/2}\ \Gamma(\frac{2-s}{2})}$$

$$= -\sqrt{-1}\ 2^{1-s}\pi^{-s}\ \sin(\tfrac{\pi s}{2})\Gamma(s).$$

<u>10:</u> FACT

$$\left[\begin{array}{l} \dfrac{\zeta(1-s)}{\zeta(s)} = 2^{1-s}\pi^{-s}\ \cos(\tfrac{\pi s}{2})\Gamma(s) \\[2ex] \dfrac{\zeta(s)}{\zeta(1-s)} = 2^{s}\pi^{s-1}\ \sin(\tfrac{\pi s}{2})\Gamma(1-s). \end{array}\right.$$

To recapitulate: $\rho(\chi)$ is a meromorphic function of s and

$$\rho(\chi) = \varepsilon(\chi)\ \frac{L(\chi)}{L(\check{\chi})},$$

where

$$\left[\begin{array}{ll} \varepsilon(\chi) = 1 & (\sigma = 0) \\ \varepsilon(\chi) = -\sqrt{-1} & (\sigma = 1). \end{array}\right.$$

Having dealt with $R^{\times}$, let us now turn to $C^{\times}$, hence $\tilde{C}^{\times} \approx Z \times C$ and every character has the form

$$\chi(x) \equiv \chi_{n,s}(x) = \exp(\sqrt{-1}\ n \arg x)|x|^{s} \quad (n \in Z,\ s \in C) \quad (\text{cf. §7, \#12}).$$

Here, however, it will be best to make a couple of adjustments.

1. Replace x by z.

2. Replace $|.|$ by $|.|_C$, the normalized absolute value, so

$$|z|_C = |z\bar{z}| = |z|^2 \quad (\text{cf. §6, \#15}).$$

<u>11.</u> DEFINITION Given $f \in S(C)$ $(= S(R^2))$ and a character $\chi: C^{\times} \to C^{\times}$, the <u>local zeta function</u> attached to the pair (f,χ) is

$$Z(f,\chi) = \int_{C^{\times}} f(z)\chi(z)d^{\times}z,$$

where $d^{\times}z = \dfrac{|dz \wedge d\bar{z}|}{|z|_C}$.

[Note: The parameters n and s are implicit:

$$Z(f,\chi) \equiv Z(f,\chi_{n,s}).]$$

<u>12:</u> NOTATION Put

$$\check{\chi} = \chi^{-1}|.|_C.$$

The analogs of #2 and #3 are immediate, as is the analog of #5 (just replace $R^{\times}$ by $C^{\times}$ and $|.|$ by $|.|_C$), the crux then being the analog of #6.

<u>13:</u> NOTATION Set

$$\Gamma_C(s) = (2\pi)^{1-s}\Gamma(s).$$

14: DEFINITION Write

$$L(\chi) = \Gamma_{\mathbb{C}}(s + \frac{|n|}{2}).$$

To determine $\rho(\chi)$ via a judicious choice of ϕ per the relation

$$\rho(\chi) = \frac{Z(\phi,\chi)}{Z(\hat{\phi},\check{\chi})},$$

let

$$\begin{cases} \phi_n(z) = \bar{z}^n e^{-2\pi|z|^2} & (n \geq 0) \\ \phi_n(z) = z^{-n} e^{-2\pi|z|^2} & (n < 0). \end{cases}$$

Then

$$\hat{\phi}_n = (\sqrt{-1})^{|n|}\phi_{-n} \qquad \text{(cf. §10, \#3).}$$

15: N.B. In terms of polar coordinates $z = re^{\sqrt{-1}\,\theta}$,

- $\phi_n(z) = r^{|n|}\exp(-\,2\pi r^2 - \sqrt{-1}\,n\theta)$
- $d^{\times}z = \frac{2rdrd\theta}{r^2} = \frac{2}{r}\,drd\theta$
- $\chi(z) = e^{\sqrt{-1}\,n\theta}|z|_{\mathbb{C}}^{s} = e^{\sqrt{-1}\,n\theta}r^{2s}.$

Therefore

$$Z(\phi_n,\chi)$$

$$= \int_0^{2\pi} \int_0^{\infty} r^{|n|} \exp(-2\pi r^2 - \sqrt{-1}\, n\theta) e^{\sqrt{-1}\, n\theta} r^{2s} \frac{2}{r}\, dr d\theta$$

$$= \int_0^{2\pi} \int_0^{\infty} r^{2(s-1)+|n|} \exp(-2\pi r^2)\, 2r dr d\theta$$

$$= 2\pi \int_0^{\infty} t^{(s-1)+|n|/2} \exp(-2\pi t) dt$$

$$= (2\pi)^{1-s-|n|/2}\Gamma(s + \frac{|n|}{2})$$

$$= \Gamma_C(s + \frac{|n|}{2}) = L(\chi)$$

and

$$Z(\hat{\phi}_n, \check{\chi}) = Z((\sqrt{-1})^{|n|}\phi_{-n}, \check{\chi})$$

$$= (\sqrt{-1})^{|n|} (2\pi)^{1-(1-s)-|n|/2}\Gamma(1-s + \frac{|n|}{2})$$

$$= (\sqrt{-1})^{|n|} (2\pi)^{s-|n|/2}\Gamma(1-s + \frac{|n|}{2})$$

$$= (\sqrt{-1})^{|n|}\Gamma_C(1-s + \frac{|n|}{2}) = (\sqrt{-1})^{|n|} L(\check{\chi}).$$

Consequently

$$\rho(\chi) = \frac{Z(\phi_n, \chi)}{Z(\hat{\phi}_n, \check{\chi})}$$

$$= (\sqrt{-1})^{-|n|} \frac{L(\chi)}{L(\check{\chi})}$$

$$= \varepsilon(\chi) \frac{L(\chi)}{L(\check{\chi})},$$

where

$$\varepsilon(\chi) = (\sqrt{-1})^{-|n|}.$$

And

$$\frac{L(\chi)}{L(\check{\chi})} = (2\pi)^{1-2s} \frac{\Gamma(s + \frac{|n|}{2})}{\Gamma(1-s + \frac{|n|}{2})} \, .$$

§12. *LOCAL ZETA FUNCTIONS*: $Q_p^\times$

The theory set forth below is in the same spirit as that of §11 but matters are technically more complicated due to the presence of ramification.

1: DEFINITION Given $f \in \mathcal{B}(Q_p)$ and a character $\chi: Q_p^\times \to C^\times$, the local zeta function attached to the pair (f,χ) is

$$Z(f,\chi) = \int_{Q_p^\times} f(x)\chi(x)d^\times x,$$

where $d^\times x = \frac{p}{p-1}\frac{dx}{|x|_p}$ (cf. §6, #26).

[Note: There are two parameters associated with χ, viz. s and $\underline{\chi}$ (cf. §9).]

2: LEMMA The integral defining $Z(f,\chi)$ is absolutely convergent for $\mathrm{Re}(s) > 0$.

PROOF It suffices to check absolute convergence for $f = \chi_{p^n Z_p}$ (cf. §10, #10) and then we might just as well take $n = 0$:

$$|Z(f,\chi)| \leq \int_{Q_p^\times} |f(x)|\ |x|_p^{\mathrm{Re}(s)} d^\times x$$

$$= \int_{Q_p^\times} \chi_{Z_p}(x)\,|x|_p^{\mathrm{Re}(s)} d^\times x$$

$$= \int_{Z_p - \{0\}} |x|_p^{\mathrm{Re}(s)} d^\times x$$

$$= \frac{1}{1-p^{-\mathrm{Re}(s)}} \quad \text{(cf. §6, #27)}.$$

<u>3:</u> LEMMA $Z(f,\chi)$ is a holomorphic function of s in the strip $\text{Re}(s) > 0$.

<u>4:</u> NOTATION Put

$$\check{\chi} = \chi^{-1}|\cdot|_p.$$

The integral defining $Z(f,\check{\chi})$ is absolutely convergent if $\text{Re}(1-s) > 0$, i.e., if $1 - \text{Re}(s) > 0$ or still, if $\text{Re}(s) < 1$.

<u>5:</u> LEMMA Let $f,g \in \mathcal{B}(Q_p)$ and suppose that $0 < \text{Re}(s) < 1$ — then

$$Z(f,\chi)Z(\hat{g},\check{\chi}) = Z(\hat{f},\check{\chi})Z(g,\chi).$$

[Simply follow verbatim the argument employed in §11, #5.]

Fix $\phi \in \mathcal{B}(Q_p)$ and put

$$\rho(\chi) = \frac{Z(\phi,\chi)}{Z(\hat{\phi},\check{\chi})}.$$

Then $\rho(\chi)$ is independent of the choice of ϕ and $\forall\ f \in \mathcal{B}(Q_p)$, the <u>functional equation</u>

$$Z(f,\chi) = \rho(\chi)Z(\hat{f},\check{\chi})$$

obtains.

<u>6:</u> LEMMA $\rho(\chi)$ is a meromorphic function of s (cf. infra).

<u>7:</u> APPLICATION $\forall\ f \in \mathcal{B}(Q_p)$, $Z(f,\chi)$ admits a meromorphic continuation to the whole s-plane.

<u>8:</u> DEFINITION Write

$$L(\chi) = \begin{cases} (1 - \chi(p))^{-1} & (\chi \text{ unramified}) \\ 1 & (\chi \text{ ramified}). \end{cases}$$

There remains the computation of $\rho(\chi)$, the simplest situation being when χ is unramified, say $\chi = |\cdot|_p^s$, in which case we take $\phi_0(x) = \chi_p(x)\chi_{Z_p}(x)$:

$$\begin{aligned}
Z(\phi_0,\chi) &= \int_{Q_p^\times} \phi_0(x)\chi(x)d^\times x \\
&= \int_{Q_p^\times} \chi_p(x)\chi_{Z_p}(x)\,|x|_p^s\, d^\times x \\
&= \int_{Z_p-\{0\}} \chi_p(x)\,|x|_p^s\, d^\times x \\
&= \int_{Z_p-\{0\}} |x|_p^s\, d^\times x \\
&= \frac{1}{1-p^{-s}} \quad \text{(cf. §6, \#27)} \\
&= \frac{1}{1-|p|_p^s} \\
&= \frac{1}{1-\chi(p)} = L(\chi).
\end{aligned}$$

To finish the determination, it is necessary to explicate the Fourier transform $\hat{\phi}_0$ of ϕ_0 (cf. §10, #11):

$$\begin{aligned}
\hat{\phi}_0(t) &= \int_{Q_p} \phi_0(x)\chi_p(tx)dx \\
&= \int_{Q_p} \chi_p(x)\chi_{Z_p}(x)\chi_p(tx)dx \\
&= \int_{Z_p} \chi_p(x)\chi_p(tx)dx
\end{aligned}$$

$$= \int_{Z_p} \chi_p((1+t)x)dx$$

$$= \chi_{Z_p}(t).$$

Therefore

$$Z(\hat{\phi}_0,\check{\chi}) = \int_{Q_p^\times} \hat{\phi}_0(x)\check{\chi}(x)d^\times x$$

$$= \int_{Q_p^\times} \chi_{Z_p}(x)|x|_p^{1-s}\, d^\times x$$

$$= \int_{Z_p-\{0\}} |x|_p^{1-s}\, d^\times x$$

$$= \frac{1}{1-p^{-(1-s)}} \quad \text{(cf. §6, \#27)}$$

$$= \frac{1}{1-|p|_p^{1-s}}$$

$$= \frac{1}{1-\check{\chi}(p)} = L(\check{\chi}).$$

And finally

$$\rho(\chi) = \frac{Z(\phi_0,\chi)}{Z(\hat{\phi},\check{\chi})} = \frac{L(\chi)}{L(\check{\chi})}$$

or still,

$$\rho(\chi) = \frac{1-p^{-(1-s)}}{1-p^{-s}}.$$

<u>9:</u> REMARK The function

$$\frac{1-p^{-(1-s)}}{1-p^{-s}}$$

has a simple pole at $s = 0$ with residue

$$\frac{p-1}{p} \log p$$

and there are no other singularities.

Suppose now that χ is ramified of degree $n \geq 1$: $\chi = |\cdot|_p^s \underline{\chi}$ (cf. §9, #6) and take $\phi_n(x) = \chi_p(x)\chi_{p^{-n}Z_p}(x)$:

$$Z(\phi_n, \chi) = \int_{Q_p^\times} \phi_n(x)\chi(x)d^\times x$$

$$= \int_{Q_p^\times} \chi_p(x)\chi_{p^{-n}Z_p}(x)|x|_p^s \underline{\chi}(x)d^\times x$$

$$= \int_{p^{-n}Z_p-\{0\}} \chi_p(x)|x|_p^s \underline{\chi}(x)d^\times x$$

$$= \sum_{k=-n}^{\infty} \int_{Z_p^\times} \chi_p(p^k u)|p^k u|_p^s \underline{\chi}(u)d^\times u$$

$$= \sum_{k=-n}^{\infty} p^{-ks} \int_{Z_p^\times} \chi_p(p^k u)\underline{\chi}(u)d^\times u.$$

<u>10:</u> LEMMA If $|v|_p \neq p^n$, then

$$\int_{Z_p^\times} \chi_p(vu)\underline{\chi}(u)d^\times u = 0.$$

Since $|p^k|_p = p^{-k}$, $Z(\phi_n, \chi)$ reduces to

$$p^{ns} \int_{Z_p^\times} \chi_p(p^{-n}u)\underline{\chi}(u)d^\times u.$$

Let $E = \{e_i : i \in I\}$ be a system of coset representatives for $Z_p^\times/U_{p,n}$ -- then by assumption, $\underline{\chi}$ is constant on the cosets mod $U_{p,n}$, hence

$$\int_{Z_p^\times} \chi_p(p^{-n}u)\underline{\chi}(u)d^\times u$$

$$= \sum_{i=1}^{r} \underline{\chi}(e_i) \int_{e_i U_{p,n}} \chi_p(p^{-n}u)d^\times u.$$

But

$$u \in e_i U_{p,n} \Rightarrow p^{-n}u \in p^{-n}e_i + Z_p$$

$\Rightarrow$

$$\chi_p(p^{-n}u) = \chi_p(p^{-n}e_i + x) \quad (x \in Z_p)$$

$$= \chi_p(p^{-n}e_i).$$

Therefore

$$\int_{Z_p^\times} \chi_p(p^{-n}u)\underline{\chi}(u)d^\times u$$

$$= \sum_{i=1}^{r} \underline{\chi}(e_i)\chi_p(p^{-n}e_i) \int_{e_i U_{p,n}} d^\times u$$

$$= \tau(\chi) \int_{U_{p,n}} d^\times u$$

if

$$\tau(\chi) = \sum_{i=1}^{r} \underline{\chi}(e_i)\chi_p(p^{-n}e_i).$$

And

$$\int_{U_{p,n}} d^{\times}u = \int_{1+p^n Z_p} d^{\times}u$$

$$= \frac{p}{p-1} \int_{1+p^n Z_p} \frac{du}{|u|_p}$$

$$= \frac{p}{p-1} \int_{1+p^n Z_p} du$$

$$= \frac{p}{p-1} \int_{p^n Z_p} du$$

$$= \frac{p}{p-1} p^{-n} = \frac{p^{1-n}}{p-1} .$$

So in the end

$$Z(\phi_n, \chi) = \tau(\chi) \frac{p^{1+n(s-1)}}{p-1} .$$

Next

$$\hat{\phi}_n(t) = \int_{Q_p} \phi_n(x) \chi_p(tx) dx$$

$$= \int_{Q_p} \chi_p(x) \chi_{p^{-n}Z_p}(x) \chi_p(tx) dx$$

$$= \int_{p^{-n}Z_p} \chi_p(x) \chi_p(tx) dx$$

$$= \int_{p^{-n}Z_p} \chi_p((1+t)x) dx$$

$$= \mathrm{vol}_{dx}(p^{-n}Z_p) \chi_{p^n Z_p - 1}(t)$$

$$= p^n \chi_{p^n Z_p - 1}(t) .$$

Therefore

$$Z(\hat{\phi}_n,\check{\chi}) = \int_{Q_p^\times} \hat{\phi}_n(x)\check{\chi}(x)d^\times x$$

$$= \int_{Q_p^\times} p^n\chi_{p^nZ_p-1}(x)\chi^{-1}(x)\,|x|_p d^\times x$$

$$= p^n \int_{p^nZ_p-1} \overline{\chi(x)}\,|x|_p^{1-s} d^\times x$$

$$= p^n \int_{p^nZ_p-1} \overline{\chi(x)} d^\times x$$

$$= p^n \int_{1+p^nZ_p} \overline{\chi(-x)} d^\times x$$

$$= p^n\overline{\chi(-1)} \int_{1+p^nZ_p} \overline{\chi(x)} d^\times x$$

$$= p^n\chi(-1) \int_{U_{p,n}} d^\times x$$

$$= p^n\chi(-1)\,\frac{p^{1-n}}{p-1}$$

$$= \frac{p}{p-1}\,\chi(-1).$$

[Note: $\chi(-1) = \pm 1$:

$$1 = (-1)(-1) \Rightarrow 1 = \chi(-1)\chi(-1) = \chi(-1)^2.]$$

Assembling the data then gives

$$\rho(\chi) = \frac{Z(\phi_n,\chi)}{Z(\hat{\phi}_n,\check{\chi})}$$

$$= \frac{\tau(\chi)\,\frac{p^{1+n(s-1)}}{p-1}}{\frac{p}{p-1}\,\chi(-1)}$$

$$= \tau(\chi)\,\frac{p^{1+n(s-1)}}{p-1}\,\frac{p-1}{p\chi(-1)}$$

$$= \tau(\chi)\chi(-1)p^{n(s-1)}$$

$$= \tau(\chi)\chi(-1)p^{n(s-1)}\,\frac{1}{1}$$

$$= \tau(\chi)\chi(-1)p^{n(s-1)}\,\frac{L(\chi)}{L(\check{\chi})}\,.$$

<u>11:</u> THEOREM

$$\rho(\chi) = \varepsilon(\chi)\,\frac{L(\chi)}{L(\check{\chi})}\,,$$

where

$$\varepsilon(\chi) = 1$$

if χ is unramified and

$$\varepsilon(\chi) = \rho(\chi)$$

if χ is ramified of degree $n \geq 1$.

<u>12:</u> LEMMA Suppose that χ is ramified of degree $n \geq 1$ -- then

$$\varepsilon(\chi)\varepsilon(\check{\chi}) = \chi(-1).$$

PROOF $\forall\ f \in \mathcal{B}(Q_p)$,

$$Z(f,\chi) = \varepsilon(\chi) Z(\hat{f},\check{\chi})$$

$$= \varepsilon(\chi)\varepsilon(\check{\chi}) Z(\hat{\hat{f}},\check{\check{\chi}}).$$

But $\check{\check{\chi}} = \chi$, hence

$$Z(\hat{\hat{f}},\check{\check{\chi}}) = \int_{\mathbf{Q}_p^\times} \hat{\hat{f}}(x)\chi(x)d^\times x$$

$$= \int_{\mathbf{Q}_p^\times} f(-x)\chi(x)d^\times x$$

$$= \int_{\mathbf{Q}_p^\times} f(x)\chi(-x)d^\times x$$

$$= \chi(-1) \int_{\mathbf{Q}_p^\times} f(x)\chi(x)d^\times x$$

$$= \chi(-1) Z(f,\chi).$$

13: APPLICATION

$$\tau(\chi)\tau(\check{\chi}) = p^n \chi(-1).$$

[In fact,

$$\varepsilon(\chi)\varepsilon(\check{\chi})$$

$$= \tau(\chi)p^{n(s-1)}\chi(-1)\tau(\check{\chi})p^{n(1-s-1)}\check{\chi}(-1)$$

$$= \tau(\chi)\tau(\check{\chi})p^{-n} = \chi(-1)$$

=>

$$\tau(\chi)\tau(\check{\chi}) = p^n\chi(-1).]$$

14: LEMMA Suppose that χ is ramified of degree $n \geq 1$ -- then

$$\varepsilon(\bar{\chi}) = \chi(-1)\overline{\varepsilon(\chi)}.$$

PROOF $\forall\ f \in \mathcal{B}(Q_p)$,

$$\begin{aligned}
Z(\hat{\bar{f}},\chi) &= \int_{Q_p^\times} \hat{\bar{f}}(x)\chi(x)d^\times x \\
&= \int_{Q_p^\times} \overline{\hat{f}(-x)}\chi(x)d^\times x \quad \text{(cf. 10.12)} \\
&= \int_{Q_p^\times} \overline{\hat{f}(x)}\chi(-x)d^\times x \\
&= \chi(-1) \int_{Q_p^\times} \overline{\hat{f}(x)}\chi(x)d^\times x \\
&= \chi(-1)Z(\bar{\hat{f}},\chi).
\end{aligned}$$

But $\check{\bar{\chi}} = \bar{\check{\chi}}$, hence

$$\begin{aligned}
\overline{Z(f,\chi)} &= Z(\bar{f},\bar{\chi}) \\
&= \varepsilon(\bar{\chi})Z(\hat{\bar{f}},\check{\bar{\chi}}) \\
&= \varepsilon(\bar{\chi})Z(\hat{\bar{f}},\bar{\check{\chi}}) \\
&= \varepsilon(\bar{\chi})\chi(-1)Z(\bar{\hat{f}},\bar{\check{\chi}}) \\
&= \varepsilon(\bar{\chi})\chi(-1)\overline{Z(\hat{f},\check{\chi})}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\overline{Z(f,\chi)} &= \overline{\varepsilon(\chi)Z(\hat{f},\check{\chi})} \\
&= \overline{\varepsilon(\chi)}\,\overline{Z(\hat{f},\check{\chi})}.
\end{aligned}$$

Therefore

$$\varepsilon(\bar{\chi})\chi(-1) = \overline{\varepsilon(\chi)}$$

=>

$$\varepsilon(\bar{\chi}) = \chi(-1)\overline{\varepsilon(\chi)}.$$

15: APPLICATION

$$\tau(\bar{\chi}) = \chi(-1)\overline{\tau(\chi)}.$$

[In fact,

$$\varepsilon(\bar{\chi}) = \tau(\bar{\chi})p^{n(\bar{s}-1)}\bar{\chi}(-1)$$

$$= \chi(-1)\overline{\varepsilon(\chi)}$$

$$= \chi(-1)\overline{\tau(\chi)}p^{n(\bar{s}-1)}\overline{\chi(-1)}$$

$$= \chi(-1)\overline{\tau(\chi)}p^{n(\bar{s}-1)}\bar{\chi}(-1)$$

=>

$$\tau(\bar{\chi}) = \chi(-1)\overline{\tau(\chi)}.]$$

16: DEFINITION Let $\underline{\chi} \in \widehat{\mathbb{Z}_p^\times}$ be a nontrivial unitary character — then its root number $W(\underline{\chi})$ is prescribed by the relation

$$W(\underline{\chi}) = \varepsilon(|\cdot|_p^{1/2}\underline{\chi}).$$

[Note: If $\underline{\chi}$ is trivial, then $W(\underline{\chi}) = 1$.]

17: LEMMA

$$|W(\underline{\chi})| = 1.$$

PROOF Put $\chi = |.|_p^{1/2}\,\underline{\chi}$ — then

$$\varepsilon(\chi)\varepsilon(\check{\chi}) = \chi(-1) \qquad \text{(cf. \#12)}$$

=>

$$\begin{aligned}\varepsilon(\chi)^{-1} &= \varepsilon(\check{\chi})\chi(-1)^{-1} \\ &= \varepsilon(\check{\chi})\chi(-1) \\ &= \varepsilon(\bar{\chi})\chi(-1) \qquad (\check{\chi} = \bar{\chi}) \\ &= \chi(-1)\overline{\varepsilon(\chi)}\chi(-1) \qquad \text{(cf. \#14)} \\ &= \chi(-1)^2\overline{\varepsilon(\chi)} \\ &= \overline{\varepsilon(\chi)}\end{aligned}$$

=>

$$|\varepsilon(\chi)| = 1 \Rightarrow |W(\underline{\chi})| = 1.$$

<u>17:</u> APPLICATION

$$|\tau(|.|_p^{1/2}\,\chi)| = p^{n/2}.$$

[In fact,

$$1 = |W(\underline{\chi})| = |\tau(|.|_p^{1/2}\,\underline{\chi})p^{n(\frac{1}{2} - 1)}|.$$

<u>18:</u> EXERSIZE AD LIBITUM Show that the theory expounded above for Q_p can be carried over to any finite extension K of Q_p.

§13. *RESTRICTED PRODUCTS*

Recall:

1: FACT Suppose that X_i $(i \in I)$ is a nonempty Hausdorff space -- then the product $\prod_{i \in I} X_i$ is locally compact iff each X_i is locally compact and all but a finite number of the X_i are compact.

Let X_i $(i \in I)$ be a family of nonempty locally compact Hausdorff spaces and for each $i \in I$, let $K_i \subset X_i$ be an open-compact subspace.

2: DEFINITION The restricted product

$$\prod_{i \in I} (X_i : K_i)$$

consists of those $x = \{x_i\}$ in $\prod_{i \in I} X_i$ such that $x_i \in K_i$ for all but a finite number of $i \in I$.

3: N.B.

$$\prod_{i \in I} (X_i : K_i) = \bigcup_{S \subset I} \prod_{i \in S} X_i \times \prod_{i \notin S} K_i,$$

where $S \subset I$ is finite.

4: DEFINITION A restricted open rectangle is a subset of $\prod_{i \in I} (X_i : K_i)$ of the form

$$\prod_{i \in S} U_i \times \prod_{i \notin S} K_i,$$

where $S \subset I$ is finite and $U_i \subset X_i$ is open.

5: LEMMA The intersection of two restricted open rectangles is a restricted open rectangle.

Therefore the collection of restricted open rectangles is a basis for a topology on $\prod_{i\in I}(X_i:K_i)$, the restricted product topology.

6: LEMMA If I is finite, then

$$\prod_{i\in I} X_i = \prod_{i\in I} (X_i:K_i)$$

and the restricted product topology coincides with the product topology.

7: LEMMA If $I = I_1 \cup I_2$, with $I_1 \cap I_2 = \emptyset$, then

$$\prod_{i\in I}(X_i:K_i) \approx (\prod_{i\in I_1} (X_i:K_i)) \times (\prod_{i\in I_2} (X_i:K_i)),$$

the restricted product topology on the left being the product topology on the right.

8: LEMMA The inclusion $\prod_{i\in I} (X_i:K_i) \to \prod_{i\in I} X_i$ is continuous but the restricted product topology coincides with the relative topology only if $X_i = K_i$ for all but a finite number of $i \in I$.

9: LEMMA $\prod_{i\in I} (X_i:K_i)$ is a Hausdorff space.

PROOF Taking into account #8, this is because

1. A subspace of a Hausdorff space is Hausdorff;
2. Any finer topology on a Hausdorff space is Hausdorff.

10: LEMMA $\prod_{i\in I} (X_i:K_i)$ is a locally compact Hausdorff space.

PROOF Let $x \in \prod_{i \in I} (X_i:K_i)$ -- then there exists a finite set $S \subset I$ such that $x_i \in K_i$ if $i \notin S$. Next, for each $i \in S$, choose a compact neighborhood U_i of x_i. This done, consider

$$\prod_{i \in S} U_i \times \prod_{i \notin S} K_i,$$

a compact neighborhood of x.

From this point forward, it will be assumed that $X_i \equiv G_i$ is a locally compact abelian group and $K_i \subset G_i$ is an open-compact subgroup.

<u>11:</u> NOTATION

$$G = \prod_{i \in I} (G_i:K_i).$$

<u>12:</u> LEMMA G is a locally compact abelian group.

Given $i \in I$, there is a canonical arrow

$$\text{in}_i:G_i \to G,$$

namely

$$x \to (\ldots,1,1,x,1,1,\ldots).$$

<u>13:</u> LEMMA in_i is a closed embedding.

PROOF Take $S = \{i\}$ and pass to

$$G_i \times \prod_{j \neq i} K_j,$$

an open, hence closed subgroup of G. The image $\text{in}_i(G_i)$ is a closed subgroup of

$$G_i \times \prod_{j \neq i} K_j$$

in the product topology, hence in the restricted product topology.

Therefore G_i can be regarded as a closed subgroup of G.

14: LEMMA

1. Let $\chi \in \tilde{G}$ -- then $\chi_i = \chi \circ \text{in}_i = \chi|G_i \in \tilde{G}_i$ and $\chi|K_i \equiv 1$ for all but a finite number of $i \in I$, so for each $x \in G$,

$$\chi(x) = \chi(\{x_i\}) = \prod_{i \in I} \chi_i(x_i).$$

2. Given $i \in I$, let $\chi_i \in \tilde{G}_i$ and assume that $\chi_i|K_i \equiv 1$ for all but a finite number of $i \in I$ -- then the prescription

$$\chi(x) = \chi(\{x_i\}) = \prod_{i \in I} \chi_i(x_i)$$

defines a $\chi \in \tilde{G}$.

These observations also apply if $\tilde{G}$ is replaced by $\hat{G}$, in which case more can be said.

15: THEOREM As topological groups,

$$\hat{G} \approx \prod_{i \in I} (\hat{G}_i : K_i^{\perp}).$$

[Note: Recall that

$$K_i^{\perp} = \{\chi_i \in \hat{G}_i : \chi_i|K_i \equiv 1\} \quad \text{(cf. §7, \#32)}$$

and a tacit claim is that $K_i^{\perp}$ is an open-compact subgroup of $\hat{G}$. To see this, quote §7, #34 to get

$$\hat{K}_i \approx \hat{G}/K_i^\perp,\ K_i^\perp \approx \widehat{G/K_i}.$$

Then

- K_i compact => $\hat{K}_i$ discrete => $\hat{G}/K_i^\perp$ discrete => $K_i^\perp$ open
- K_i open => G/K_i discrete => $\widehat{G/K_i}$ compact => $K_i^\perp$ compact.]

Let μ_i be the Haar measure on G_i normalized by the condition

$$\mu_i(K_i) = 1.$$

<u>16:</u> LEMMA There is a unique Haar measure μ_G on G such that for every finite subset $S \subset I$, the restriction of μ_G to

$$G_S \equiv \prod_{i \in S} G_i \times \prod_{i \notin S} K_i$$

is the product measure.

Suppose that f_i is a continuous, integrable function on G_i such that $f_i | K_i = 1$ for all i outside some finite set and let f be the function on G defined by

$$f(x) = f(\{x_i\}) = \prod_i f_i(x_i).$$

Then f is continuous. Proof: The G_S are open and cover G and on each of them f is continuous.

<u>17:</u> LEMMA Let $S \subset I$ be a finite subset of I -- then

$$\int_{G_S} f(x)\,d\mu_{G_S}(x) = \prod_{i\in S} \int_{G_i} f_i(x_i)\,d\mu_{G_i}(x_i).$$

18: APPLICATION If

$$\sup_S \prod_{i\in S} \int_{G_i} |f_i(x_i)|\,d\mu_{G_i}(x_i) < \infty,$$

then f is integrable on G and

$$\int_G f(x)\,d\mu_G(x) = \prod_{i\in I} \int_{G_i} f_i(x_i)\,d\mu_{G_i}(x_i).$$

19: EXAMPLE Take $f_i = \chi_{K_i}$ (which is continuous, K_i being open-compact) -- then $\hat{f}_i = \chi_{K_i^\perp}$. Setting

$$f = \prod_{i\in I} f_i,$$

it thus follows that $\forall\ \chi \in \hat{G}$,

$$\hat{f}(\chi) = \prod_{i\in I} \hat{f}_i(\chi_i).$$

Working within the framework of §7, #45, let $\mu_{\hat{G}_i}$ be the Haar measure on $\hat{G}_i$ per Fourier inversion.

20: LEMMA

$$\mu_{\hat{G}_i}(K_i^\perp) = 1$$

PROOF Since $\chi_{K_i} \in \text{INV}(G_i)$, $\forall\ x_i \in G_i$,

$$\chi_{K_i}(x_i) = \int_{\hat{G}_i} \hat{\chi}_{K_i}(x_i)\overline{\chi_i(x_i)}\,d\mu_{\hat{G}_i}(\chi_i)$$

$$= \int_{K_i^\perp} \overline{\chi_i(x_i)}\, d\mu_{\hat{G}_i}(\chi_i).$$

Now set $x_i = 1$ to get

$$1 = \int_{K_i^\perp} d\mu_{\hat{G}_i}(\chi_i)$$

$$= \mu_{\hat{G}_i}(K_i^\perp).$$

Let $\mu_{\hat{G}}$ be the Haar measure on $\hat{G}$ constructed as in #16 (i.e., replace G by $\hat{G}$, bearing in mind #20).

21: LEMMA $\mu_{\hat{G}}$ is the Haar measure on $\hat{G}$ figuring in Fourier inversion per μ_G.

PROOF Take

$$f = \prod_{i \in I} f_i,$$

where $f_i = \chi_{K_i}$ (cf. #19) -- then

$$\int_{\hat{G}} \hat{f}(\chi)\overline{\chi(x)}\, d\mu_{\hat{G}}(\chi)$$

$$= \prod_{i \in I} \int_{\hat{G}_i} \hat{f}_i(\chi_i)\overline{\chi_i(x_i)}\, d\mu_{\hat{G}_i}(\chi_i)$$

$$= \prod_{i \in I} f_i(x_i) = f(\{x_i\}) = f(x).$$

§14. ADELES AND IDELES

1. DEFINITION The set of finite adeles is the restricted product

$$A_{fin} = \prod_p (Q_p : Z_p).$$

2: DEFINITION The set of adeles is the product

$$A = A_{fin} \times R.$$

3: LEMMA A is a locally compact abelian group (under addition).

4: N.B. A is a subring of $\prod_p Q_p \times R$.

The image of the diagonal map

$$Q \to \prod_p Q_p \times R$$

lies in A, so Q can be regarded as a subring of A.

5: LEMMA Q is a discrete subspace of A.

PROOF To establish the discreteness of $Q \subset A$, one need only exhibit a neighborhood U of 0 in A such that $Q \cap U = \{0\}$. To this end, consider

$$U = \prod_p Z_p \times]-\frac{1}{2}, \frac{1}{2}[.$$

If $x \in Q \cap U$, then $|x|_p \leq 1 \ \forall \ p$. But $\bigcap_p (Q \cap Z_p) = Z$, so $x \in Z$. And further, $|x|_\infty < \frac{1}{2}$, hence finally $x = 0$.

6: FACT Let G be a locally compact group and let $\Gamma \subset G$ be a discrete subgroup -- then Γ is closed in G and G/Γ is a locally compact Hausdorff space.

7: THEOREM The quotient A/Q is a compact Hausdorff space.

PROOF Since $Q \subset A$ is a discrete subgroup, Q must be closed in A and the quotient A/Q must be Hausdorff. As for the compactness, it suffices to show that the compact set $\prod_p Z_p \times [0,1]$ contains a set of representatives of A/Q because this implies that the projection

$$\prod_p Z_p \times [0,1] \to A/Q$$

is surjective, hence that A/Q is the continuous image of a compact set. So let $x \in A$ -- then there is a finite set S of primes such that $p \notin S \Rightarrow x_p \in Z_p$. For $p \in S$, write

$$x_p = f(x_p) + [x_p],$$

thus $[x_p] \in Z_p$ and if $q \neq p$ is another prime,

$$|f(x_p)|_q = \left|\sum_{n=v(x_p)}^{-1} a_n p^n\right|_q$$

$$\leq \sup\{|a_n p^n|_q\} \leq 1.$$

Agreeing to denote $f(x_p)$ by r_p, write

$$x = (x-r_p) + r_p.$$

Then r_p is a rational number and per $x-r_p$, S reduces to $S - \{p\}$. Proceed from here by iteration to get

$$x = y + r,$$

where $\forall\, p$, $y_p \in Z_p$, and $r \in Q$. At infinity,

$$x_\infty = y_\infty + r \quad (r_\infty = r)$$

and there is a unique $k \in Z$ such that

$$y_\infty = (y_\infty - k) + k$$

with $0 \le y_\infty - k < 1$. Accordingly,

$$y = y + r = (y-k) + k + r.$$

And

$$\forall\ p,\ (y-k)_p = y_p - k_p = y_p - k \in Z_p,$$

while

$$x_\infty = (y_\infty - k) + k + r.$$

It therefore follows that x can be written as the sum of an element in $\prod_p Z_p \times [0,1]$ and a rational number, the contention.

8: DEFINITION The topological group A/Q is called the adele class group.

9: DEFINITION Let G be a locally compact group and let $\Gamma \subset G$ be a discrete subgroup -- then a fundamental domain for G/Γ is a Borel measurable subset $D \subset G$ which is a system of representatives for G/Γ.

10: LEMMA The set

$$D = \prod_p Z_p \times [0,1[$$

is a fundamental domain for A/Q.

PROOF The claim is that every $x \in A$ can be written uniquely as $d + r$, where $d \in D$, $r \in Q$. The proof of #7 settles existence, thus the remaining issue is uniqueness: $d_1 + r_1 = d_2 + r_2 \Rightarrow d_1 = d_2$, $r_1 = r_2$. To see this, consider

$$\rho = d_1 - d_2 = r_2 - r_1 \in (D-D) \cap Q.$$

- $\forall\, p,\ \rho = \rho_p \in D_p - D_p = D_p = Z_p$

  $\Rightarrow \rho \in \bigcap_p (Q \cap Z_p) = Z.$

- $\rho = \rho_\infty \in D_\infty - D_\infty =]-1,1[.$

Therefore

$$\rho \in Z \cap]-1,1[\Rightarrow \rho = 0.$$

11: REMARK Q is dense in A_{fin}.

[The point is that Z is dense in $\prod_p Z_p$.]

12: DEFINITION The set of finite ideles is the restricted product

$$I_{fin} = \prod_p (Q_p^\times : Z_p^\times).$$

13: DEFINITION The set of ideles is the product

$$I = I_{fin} \times R^\times.$$

14: LEMMA I is a locally compact abelian group (under multiplication).

Algebraically, I can be identified with $A^\times$ but there is a topological issue since when endowed with the relative topology, $A^\times$ is not a topological group: Multiplication is continuous but inversion is not continuous.

15: LEMMA Equip $A \times A$ with the product topology and define

$$\phi : I \to A \times A$$

by

$$\phi(x) = (x, \frac{1}{x}).$$

Endow the image $\phi(I)$ with the relative topology -- then ϕ is a topological isomorphism of I onto $\phi(I)$.

The image of the diagonal map

$$Q^\times \to \prod_p Q_p \times R^\times$$

lies in I, so $Q^\times$ can be regarded as a subgroup of I.

16: LEMMA $Q^\times$ is a discrete subspace of I.

PROOF Q is a discrete subspace of A (cf. #5), hence $Q \times Q$ is a discrete subspace of $A \times A$, hence $\phi(Q^\times)$ is a discrete subspace of $\phi(I)$.

Consequently, $Q^\times$ is a closed subgroup of I and the quotient $I/Q^\times$ is a locally compact Hausdorff space but, as opposed to the adelic situation, it is not compact (see below).

17: DEFINITION The topological group $I/Q^\times$ is called the idele class group.

18: NOTATION Given $x \in I$, put

$$|x|_A = \prod_{p\le\infty} |x_p|_p.$$

Extend the definition of $|.|_A$ to all of A by setting $|x|_A = 0$ if $x \in A - A^\times$.

19: LEMMA $\forall\, x \in Q^\times$, $|x|_A = 1$ (cf. §1, #21).

20: LEMMA The homomorphism

$$|\cdot|_A : I \to R^{\times}_{>0}$$

is continuous and surjective.

PROOF Omitting the verification of continuity, fix $t \in R^{\times}_{>0}$ and let x be the idele specified by

$$x_p = 1 \ (p < \infty), \ x_\infty = t.$$

Then $|x|_A = t$.

21: SCHOLIUM The idele class group $I/Q^{\times}$ is not compact.

22: NOTATION Let

$$I^1 = \text{Ker } |\cdot|_A.$$

23: N.B. $x \in I^1 \Rightarrow x_\infty \in Q^{\times}$.

24: THEOREM The quotient $I^1/Q^{\times}$ is a compact Hausdorff space, in fact

$$I^1/Q^{\times} \approx \prod_p Z_p^{\times},$$

hence

$$\prod_p Z_p^{\times} \times \{1\}$$

is a fundamental domain for $I^1/Q^{\times}$.

PROOF The arrow

$$\prod_p Z_p^{\times} \to I^1/Q^{\times}$$

that sends x to $(x,1)Q^{\times}$ is an isomorphism of topological groups.

[In obvious notation, the inverse is the map

$$x = (x_{fin}, x_\infty) \to \frac{1}{x_\infty} x_{fin}.]$$

<u>25:</u> REMARK $\forall$ p, $Z_p^\times$ is totally disconnected. But a product of totally disconnected spaces is totally disconnected, thus $\prod_p Z_p^\times$ is totally disconnected, thus $I^1/Q^\times$ is totally disconnected.

<u>26:</u> <u>N.B.</u> $\prod_p Z_p^\times \times R_{>0}^\times$ is a fundamental domain for $I/Q^\times$.

[Note: If $r \in Q$ and if $|r|_p = 1 \ \forall \ p$, then $r = \pm 1$.]

<u>27:</u> LEMMA

$$I \approx I^1 \times R_{>0}^\times.$$

PROOF The arrow

$$I \to I^1 \times R_{>0}^\times$$

that sends x to $(\tilde{x}, |x|_A)$, where

$$(\tilde{x})_p = \begin{cases} x_p & (p < \infty) \\ \dfrac{x_\infty}{|x|_A} & (p = \infty), \end{cases}$$

is an isomorphism of topological groups.

<u>28:</u> LEMMA There is a disjoint decomposition

$$I_{fin} = \coprod_{q \in Q_{>0}^{\times}} q(\prod_p Z_p^{\times}).$$

PROOF The right hand side is obviously contained in the left hand side. To go the other way, fix an $x \in I_{fin}$ -- then $|x|_A \in Q_{>0}^{\times}$. Moreover, $|x|_A x \in I_{fin}$ and $\forall\ p$, $||x|_A x_p|_p = 1$ (for $x_p = p^k u$ $(u \in Z_p^{\times})$ => $|x|_A = p^{-k} r$ $(r \in Q^{\times}$, r coprime to p)), hence

$$|x|_A x \in \prod_p Z_p^{\times}.$$

Now write

$$x = |x|_A^{-1} (|x|_A x)$$

to conclude that

$$x \in q \prod_p Z_p^{\times} \quad (q = |x|_A^{-1}).$$

<u>29:</u> LEMMA There is a disjoint decomposition

$$I_{fin} \cap \prod_p Z_p = \coprod_{n \in N} n(\prod_p Z_p^{\times}).$$

Normalize the Haar measure $d^{\times}x$ on I_{fin} by assigning the open-compact subgroup $\prod_p Z_p^{\times}$ total volume 1.

<u>30:</u> EXAMPLE Suppose that $Re(s) > 1$ -- then

$$\int_{I_{fin} \cap \prod_p Z_p} |x|_A^s \, d^{\times}x$$

$$= \sum_{n\in N} \int_{n(\prod_p Z_p^\times)} |x|_A^s \, d^\times x$$

$$= \sum_{n\in N} \int_{\prod_p Z_p^\times} |nx|_A^s \, d^\times x$$

$$= \sum_{n\in N} n^{-s} \, \mathrm{vol}_{d^\times x} (\prod_p Z_p^\times)$$

$$= \sum_{n\in N} n^{-s} = \zeta(s).$$

[Note: Let $x \in \prod_p Z_p^\times$:

$$\Rightarrow \forall p, \ |x_p|_p = 1$$

$$\Rightarrow |nx|_A = \prod_p |nx_p|_p$$

$$= \prod_p |n|_p \, |x_p|_p$$

$$= \prod_p |n|_p$$

$$= \prod_p |n|_p \cdot n \cdot \frac{1}{n}$$

$$= 1 \cdot \frac{1}{n} = n^{-1}.]$$

The idelic absolute value $|.|_A$ can be interpreted measure theoretically.

31: NOTATION Write

$$dx_A = \prod_{p\leq\infty} dx_p$$

for the Haar measure μ_A on A (cf. §13, #16).

Consider a function of the form $f = \prod_{p\leq\infty} f_p$, where $\forall$ p, f_p is a continuous, integrable function on Q_p, and for all but a finite number of p, $f_p = \chi_{Z_p}$ -- then

$$\int_A f(x)dx_A = \prod_{p\leq\infty} \int_{Q_p} f_p(x_p)dx_p \qquad \text{(cf. §13, #18)},$$

it being understood that $Q_\infty = R$.

32: LEMMA Let $M \subset A$ be a Borel set with $0 < \mu_A(M) < \infty$ -- then $\forall$ $x \in I$,

$$\frac{\mu_A(xM)}{\mu_A(M)} = |x|_A.$$

PROOF Take $M = D = \prod_p Z_p \times [0,1[$ (cf. #10):

$$\begin{aligned}\mu_A(xM) &= \prod_p \mu_{Q_p}(x_pZ_p) \times \mu_R(x_\infty[0,1[)\\ &= \prod_p |x_p|_p\,\mu_{Q_p}(Z_p) \times |x_\infty|\mu_R([0,1[)\\ &= \prod_p |x_p|_p \times |x_\infty|_\infty\\ &= \prod_{p\leq\infty} |x_p|_p = |x|_A.\end{aligned}$$

[Note: Needless to say, multiplication by an idele x is an automorphism of A, thus transforms μ_A into a positive constant multiple of itself, the multiplier being $|x|_A$.]

§15. *GLOBAL ANALYSIS*

By definition,

$$A = A_{\text{fin}} \times R.$$

Therefore

$$\hat{A} \approx \hat{A}_{\text{fin}} \times \hat{R}.$$

And

$$A_{\text{fin}} = \prod_p (Q_p : Z_p)$$

$$\Rightarrow$$

$$\hat{A}_{\text{fin}} \approx \prod_p (\hat{Q}_p : Z_p^{\perp}) \qquad \text{(cf. §13, \#15).}$$

Put

$$\chi_Q = \prod_{p \le \infty} \chi_p,$$

where

$$\chi_\infty(x) = \exp(-2\pi\sqrt{-1}\,x) \quad (x \in R) \qquad \text{(cf. §8, \#27).}$$

Then

$$\chi_Q \in \hat{A}.$$

Given $t \in A$, define $\chi_{Q,t} \in \hat{A}$ by the rule

$$\chi_{Q,t}(x) = \chi_Q(tx).$$

Then the arrow

$$\Xi_Q : A \to \hat{A}$$

that sends t to $\chi_{Q,t}$ is an isomorphism of topological groups (cf. §8, #24).

Recall now that $\forall\ q \in Q$,

$$\chi_Q(q) = 1 \quad (\text{cf. §8, \#28}).$$

Accordingly, χ_Q passes to the quotient and defines a unitary character of the adele class group A/Q. So, $\forall\ q \in Q$, $\chi_{Q,q}$ is constant on the cosets of A/Q, thus it too determines an element of $\widehat{A/Q}$.

Equip Q with the discrete topology.

<u>1:</u> THEOREM The induced map

$$\begin{cases} \Xi_Q|Q:Q \to \widehat{A/Q} \\ \quad q \to \chi_{Q,q} \end{cases}$$

is an isomorphism of topological groups.

PROOF Form $Q^\perp \subset \hat{A}$, the closed subgroup of $\hat{A}$ consisting of those χ that are trivial on Q -- then $Q \subset Q^\perp$ and $\widehat{A/Q} \approx Q^\perp$. But A/Q is compact, thus its unitary dual $\widehat{A/Q}$ is discrete, thus $Q^\perp$ is discrete. The quotient $Q^\perp/Q \subset A/Q$ $(A \approx \hat{A})$ is therefore discrete and closed, hence discrete and compact, hence finite. But $Q^\perp/Q$ is a Q-vector space, so $Q^\perp/Q = \{0\}$ or still, $Q^\perp = Q$, which implies that $Q \approx \widehat{A/Q}$.

<u>2:</u> <u>N.B.</u> There are two points of detail that have been tacitly invoked in the foregoing derivation.

- $Q^\perp/Q$ in the quotient topology is discrete. Reason: Let S be an arbitrary nonempty subset of $Q^\perp/Q$, say $S = \{xQ:x \in U\}$, U a subset of $Q^\perp$ -- then U is automatically open ($Q^\perp$ being discrete), thus by the very definition of the quotient topology, S is an open subset of $Q^{\perp}/Q$.

- The quotient $Q^{\perp}/Q$ is closed in A/Q. Reason: $Q^{\perp}$ is a closed subgroup of A containing Q, so the following generality is applicable: If G is a topological group, if H is a subgroup of G, if F is a closed subgroup of G containing H, then $\pi(F)$ is closed in G/H ($\pi: G \to G/H$ the projection).

3: SCHOLIUM

$$Q \approx \widehat{A/Q} \Rightarrow \hat{Q} \approx \widehat{\widehat{A/Q}} \approx A/Q.$$

[Note: Bear in mind that Q carries the discrete topology.]

4: DISCUSSION Explicated, if $\chi \in \hat{Q}$, then there exists a $t \in A$ such that $\chi = \chi_{Q,t}$ and $\chi_{Q,t_1} = \chi_{Q,t_2}$ iff $t_1 - t_2 \in Q$.

5: DEFINITION The Bruhat space $\mathcal{B}(A_{fin})$ consists of all finite linear combinations of functions of the form

$$f = \prod_p f_p,$$

where $\forall$ p, $f_p \in \mathcal{B}(Q_p)$ and $f_p = \chi_{Z_p}$ for all but a finite number of p.

6: DEFINITION The Bruhat-Schwartz space $\mathcal{B}_{\infty}(A)$ consists of all finite linear combinations of functions of the form

$$f = \prod_p f_p \times f_{\infty},$$

where

$$\prod_p f_p \in \mathcal{B}(A_{fin}) \text{ and } f_{\infty} \in \mathcal{S}(R).$$

Given an $f \in \mathcal{B}_\infty(A)$, its Fourier transform is the function $\hat{f}:A \rightarrow C$ defined by the rule

$$\hat{f}(t) = \int_A f(x)\chi_{Q,t}(x)d\mu_A(x)$$

$$= \int_A f(x)\chi_Q(tx)d\mu_A(x).$$

7: LEMMA If

$$f = \prod_p f_p \times f_\infty$$

is a Bruhat-Schwartz function, then

$$\hat{f} = \prod_p \hat{f}_p \times \hat{f}_\infty.$$

8: REMARK $\hat{f}_p$ is computed per §10, #11 but $\hat{f}_\infty$ is computed per

$$\chi_\infty(x) = \exp(-\,2\pi\sqrt{-1}\,x),$$

meaning that the sign convention here is the opposite of that laid down in §10 (a harmless deviation).

9: APPLICATION

$$f \in \mathcal{B}_\infty(A) \Rightarrow \hat{f} \in \mathcal{B}_\infty(A) \qquad \text{(cf. §10, #16)}.$$

10: N.B. It is clear that

$$\mathcal{B}_\infty(A) \subset \text{INV}(A)$$

and $\forall\ f \in \mathcal{B}_\infty(A)$,

$$\hat{\hat{f}}(x) = f(-x) \qquad (x \in A).$$

<u>11:</u> LEMMA Given $f \in \mathcal{B}_\infty(A)$, the series

$$\sum_{r\in Q} f(x+r), \quad \sum_{q\in Q} \hat{f}(x+q)$$

are absolutely and uniformly convergent on compact subsets of A.

<u>12:</u> POISSON SUMMATION FORMULA Given $f \in \mathcal{B}_\infty(A)$,

$$\sum_{r\in Q} f(r) = \sum_{q\in Q} \hat{f}(q).$$

The proof is not difficult but there are some measure-theoretic issues to be dealt with first.

On general grounds,

$$\int_A = \int_{A/Q} \sum_Q \qquad \text{(cf. §6, \#11).}$$

Here the integral $\int_A$ is with respect to the Haar measure μ_A on A (cf. §14, #31). Taking μ_Q to be counting measure, this choice of data fixes the Haar measure $\mu_{A/Q}$ on A/Q.

[Note: The restriction of μ_A to the fundamental domain

$$D = \prod_p Z_p \times [0,1[$$

for A/Q (cf. §14, #10) determines $\mu_{A/Q}$ and

$$1 = \mu_A(D) = \mu_{A/Q}(A/Q).]$$

If $\phi: Q \to C$, then $\hat{\phi}: \hat{Q} \to C$, i.e., $\hat{\phi}: A/Q \to C$ or still,

$$\hat{\phi}(\chi) = \sum_{r\in Q} \phi(r)\chi(r).$$

Specialize and suppose that ϕ is the characteristic function of $\{0\}$, so $\forall\ \chi$,

$$\hat{\phi}(\chi) = \chi(0) = 1.$$

Therefore $\hat{\phi}$ is the constant function 1 on A/Q. Pass now to $\hat{\hat{\phi}}$, thus $\hat{\hat{\phi}}:\widehat{A/Q} \rightarrow C$ or still,

$$\hat{\hat{\phi}}(\chi_{Q,q}) = \int_{A/Q} \hat{\phi}(x)\chi_{Q,q}(x)d\mu_{A/Q}(x)$$

$$= \int_{A/Q} \chi_{Q,q}(x)d\mu_{A/Q}(x)$$

which is 1 if $q = 0$ and is 0 otherwise (cf. §7, #46 (A/Q is compact)), hence $\hat{\hat{\phi}} = \phi$. But $\phi(r) = \phi(-r)$, thereby leading to the conclusion that the Haar measure $\mu_{A/Q}$ on A/Q is the one singled out by Fourier inversion (cf. §7, #45).

Summary: Per Fourier inversion,

- μ_Q is paired with $\mu_{A/Q}$.
- $\mu_{A/Q}$ is paired with μ_Q.

Given $f \in \mathcal{B}_\infty(A)$, put

$$F(x) = \sum_{r \in Q} f(x+r).$$

Then F lives on A/Q, so $\hat{F}$ lives on $\widehat{A/Q} \approx Q$:

$$\hat{F}(q) = \int_{A/Q} F(x)\chi_{Q,q}(x)d\mu_{A/Q}(x)$$

$$= \int_{A/Q} F(x)\chi_Q(qx)d\mu_{A/Q}(x).$$

On the other hand,

$$\hat{f}(q) = \int_A f(x)\chi_{Q,q}(x)d\mu_A(x)$$

$$= \int_{A} f(x)\chi_Q(qx)d\mu_A(x)$$

$$= \int_{A/Q} (\sum_{r\in Q} f(x+r)\chi_Q(q(x+r)))d\mu_{A/Q}(x)$$

$$= \int_{A/Q} (\sum_{r\in Q} f(x+r)\chi_Q(qx+qr))d\mu_{A/Q}(x)$$

$$= \int_{A/Q} (\sum_{r\in Q} f(x+r)\chi_Q(qx)\chi_Q(qr)d\mu_{A/Q}(x)$$

$$= \int_{A/Q} (\sum_{r\in Q} f(x+r))\chi_Q(qx)d\mu_{A/Q}(x)$$

$$= \int_{A/Q} F(x)\chi_Q(qx)d\mu_{A/Q}(x)$$

$$= \hat{F}(q).$$

To finish the proof, per Fourier inversion, write

$$F(x) = \sum_{q\in Q} \hat{F}(q)\overline{\chi_Q(qx)}$$

and then put $x = 0$:

$$F(0) = \sum_{r\in Q} f(r) = \sum_{q\in Q} \hat{F}(q) = \sum_{q\in Q} \hat{f}(q).$$

<u>13:</u> THEOREM Let $x \in I$ -- then $\forall f \in \mathcal{B}_\infty(A)$,

$$\sum_{r\in Q} f(rx) = \frac{1}{|x|_A} \sum_{q\in Q} \hat{f}(qx^{-1}).$$

PROOF Work with $f_x \in \mathcal{B}_\infty(A)$ $(f_x(y) = f(xy))$:

$$\sum_{r\in Q} f_x(r) = \sum_{q\in Q} \hat{f}_x(q).$$

But

$$\begin{aligned}\hat{f}_x(q) &= \int_A f_x(y)\chi_{Q,q}(y)\,d\mu_A(y)\\ &= \int_A f_x(y)\chi_Q(qy)\,d\mu_A(y)\\ &= \int_A f(xy)\chi_Q(qxx^{-1}y)\,d\mu_A(y)\\ &= \frac{1}{|x|_A}\int_A f(y)\chi_Q(qx^{-1}y)\,d\mu_A(y)\\ &= \frac{1}{|x|_A}\hat{f}(qx^{-1}).\end{aligned}$$

§16. FUNCTIONAL EQUATIONS

Let

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\mathrm{Re}(s) > 1)$$

be the Riemann zeta function -- then $\zeta(s)$ can be meromorphically continued into the whole s-plane with a simple pole as $s = 1$ and satisfies there the functional equation

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

<u>1:</u> REMARK The product $\pi^{-s/2}\Gamma(s/2)$ was denoted by $\Gamma_R(s)$ in §11, #8.

There are many proofs of the functional equation satisfied by $\zeta(s)$. Of these, we shall single out two, one "classical", the other "modern".

To proceed in the classical vein, start with

$$\Gamma(s) = \int_0^\infty e^{-x}x^s \frac{dx}{x} \quad (\mathrm{Re}(s) > 1).$$

Then by change of variable,

$$\pi^{-s/2}\Gamma(s/2)n^{-s} = \int_0^\infty e^{-n^2\pi x} x^{s/2} \frac{dx}{x}.$$

So, upon summing from $n = 1$ to ∞:

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty \psi(x)x^{s/2} \frac{dx}{x},$$

where

$$\psi(x) = \sum_{n=1}^{\infty} e^{-n^2\pi x}.$$

Put now

$$\theta(x) = 1 + 2\psi(x) = \sum_{n\in Z} e^{-n^2\pi x}.$$

2: LEMMA

$$\theta(\tfrac{1}{x}) = \sqrt{x}\,\theta(x).$$

Therefore

$$\psi(\tfrac{1}{x}) = -\tfrac{1}{2} + \tfrac{1}{2}\,\theta(\tfrac{1}{x})$$

$$= -\tfrac{1}{2} + \tfrac{\sqrt{x}}{2}\,\theta(x)$$

$$= -\tfrac{1}{2} + \tfrac{\sqrt{x}}{2} + \sqrt{x}\,\psi(x).$$

One may then write

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty \psi(x)x^{s/2}\,\frac{dx}{x}$$

$$= \int_0^1 \psi(x)x^{s/2}\,\frac{dx}{x} + \int_1^\infty \psi(x)x^{s/2}\,\frac{dx}{x}$$

$$= \int_1^\infty \psi(\tfrac{1}{x})x^{-s/2}\,\frac{dx}{x} + \int_1^\infty \psi(x)x^{s/2}\,\frac{dx}{x}$$

$$= \int_1^\infty (-\tfrac{1}{2} + \tfrac{\sqrt{x}}{2} + \sqrt{x}\,\psi(x))x^{-s/2}\,\frac{dx}{x} + \int_1^\infty \psi(x)x^{s/2}\,\frac{dx}{x}$$

$$= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \psi(x)\,(x^{s/2} + x^{(1-s)/2})\,\frac{dx}{x}.$$

The last integral is convergent for all values of s and thus defines a holomorphic function. Moreover, the last expression is unchanged if s is replaced by 1 - s. I.e.:

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

The modern proof of this relation uses the adele-idele machinery. Thus let

$$\Phi(x) = e^{-\pi x_\infty^2} \prod_p \chi_{Z_p}(x_p)\ (x \in A).$$

Then if Re(s) > 1,

$$\int_I \Phi(x)|x|_A^s \, d^\times x$$

$$= \int_{R^\times} e^{-\pi t^2}|t|^s \frac{dt}{|t|} \cdot \prod_p \int_{Q_p^\times} \chi_{Z_p}(x_p)|x_p|_p^s \, d^\times x_p$$

$$= \pi^{-s/2}\Gamma(s/2) \cdot \prod_p \int_{Z_p - \{0\}} |x_p|_p^s \, d^\times x_p$$

$$= \pi^{-s/2}\Gamma(s/2) \cdot \prod_p \frac{1}{1-p^{-s}} \quad \text{(cf. §6, \#26)}$$

$$= \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

To derive the functional equation, we shall calculate the integral

$$\int_I \Phi(x)|x|_A^s \, d^\times x$$

in another way. To this end, put

$$D^\times = \prod_p Z_p^\times \times R_{>0}^\times,$$

a fundamental domain for $I/Q^\times$ (cf. §14, #26), so

$$I = \bigcup_{r \in Q^\times} rD^\times \quad \text{(disjoint union)}.$$

Therefore

$$\int_I \Phi(x)|x|_A^s \, d^\times x$$

$$= \sum_{r \in Q^\times} \int_{rD^\times} \Phi(x) |x|_A^s \, d^\times x$$

$$= \int_{D^\times} \sum_{r \in Q^\times} \Phi(rx) |rx|_A^s \, d^\times x$$

$$= \int_{\substack{D^\times \\ |x|_A \leq 1}} \sum_{r \in Q^\times} \Phi(rx) |x|_A^s \, d^\times x$$

$$+ \int_{\substack{D^\times \\ |x|_A \geq 1}} \sum_{r \in Q^\times} \Phi(rx) |x|_A^s \, d^\times x.$$

To proceed further, recall that $\hat{\Phi} = \Phi$ $(\Rightarrow \hat{\Phi}(0) = \Phi(0) = 1)$, hence (cf. §15, #13)

$$1 + \sum_{r \in Q^\times} \Phi(rx) = \frac{1}{|x|_A} + \frac{1}{|x|_A} \sum_{q \in Q^\times} \Phi(qx^{-1}).$$

Accordingly,

$$\int_{\substack{D^\times \\ |x|_A \leq 1}} \sum_{r \in Q^\times} \Phi(rx) |x|_A^s \, d^\times x$$

$$= \int_{\substack{D^\times \\ |x|_A \leq 1}} \Big(-1 + \frac{1}{|x|_A} + \frac{1}{|x|_A} \sum_{q \in Q^\times} \Phi(qx^{-1})\Big) |x|_A^s \, d^\times x$$

$$= \int_{\substack{D^\times \\ |x|_A \leq 1}} (|x|_A^{s-1} - |x|_A^s) d^\times x + \int_{\substack{D^\times \\ |x|_A \geq 1}} \sum_{q \in Q^\times} \Phi(qx) |x|_A^{1-s} \, d^\times x.$$

But

$$\int_{\substack{D^\times \\ |x|_A \leq 1}} (|x|_A^{s-1} - |x|_A^s) d^\times x$$

$$= \int_0^1 (t^{s-1} - t) \frac{dt}{t} = \frac{1}{s-1} - \frac{1}{s} .$$

So, upon assembling the data, we conclude that

$$\int_I \Phi(x) |x|_A^s d^\times x$$

$$= \frac{1}{s-1} - \frac{1}{s} + \int_{\substack{D^\times \\ |x|_A \geq 1}} \sum_{q \in Q^\times} \Phi(qx) (|x|_A^s + |x|_A^{1-s}) d^\times x.$$

Since the second expression is invariant under the transformation $s \rightarrow 1-s$, the functional equation for $\zeta(s)$ follows once again.

<u>3:</u> REMARK Consider

$$\int_{\substack{D^\times \\ |x|_A \geq 1}} \sum_{q \in Q^\times} \Phi(qx) \ldots .$$

Then from the definitions,

$$x \in D^\times \Rightarrow x_p \in Z_p^\times \ \& \ qx_p \in Z_p$$

$$\Rightarrow q \in Z.$$

Matters thus reduce to

$$2\int_1^\infty \sum_{n=1}^\infty e^{-n^2 \pi t^2} (t^s + t^{1-s}) \frac{dt}{t}$$

or still,

$$\int_1^\infty \psi(t) (t^{s/2} + t^{(1-s)/2}) \frac{dt}{t} ,$$

the classical expression.

§17. *GLOBAL ZETA FUNCTIONS*

Structurally, there is a short exact sequence

$$1 \to I^1/Q^\times \to I/Q^\times \to R^\times_{>0} \to 1 \quad \text{(cf. §14, \#27)}$$

and $I^1/Q^\times$ is compact (cf. §14, #24).

<u>1:</u> DEFINITION Given $f \in \mathcal{B}_\infty(A)$ and a unitary character $\omega: I/Q^\times \to T$, the <u>global zeta function</u> attached to the pair (f,ω) is

$$Z(f,\omega,s) = \int_I f(x)\omega(x)|x|_A^s \, d^\times x \quad (\mathrm{Re}(s) > 1).$$

<u>2:</u> EXAMPLE In the notation of §16, take

$$f(x) = \Phi(x) = e^{-\pi x_\infty^2} \prod_p \chi_{Z_p}(x_p) \quad (x \in A)$$

and let $\omega = 1$ -- then as shown there

$$Z(f,1,s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

<u>3:</u> LEMMA $Z(f,\omega,s)$ is a holomorphic function of s in the strip $\mathrm{Re}(s) > 1$.

<u>4:</u> THEOREM $Z(f,\omega,s)$ can be meromorphically continued into the whole s-plane and satisfies the functional equation

$$Z(f,\omega,s) = Z(\hat{f},\bar{\omega},1-s).$$

[Note:

$$f \in \mathcal{B}_\infty(A) \Rightarrow \hat{f} \in \mathcal{B}_\infty(A) \quad \text{(cf. §15, \#9).]}$$

The proof is a computation, albeit a lengthy one.

To begin with,

$$I \approx R_{>0}^{\times} \times I^1 \quad \text{(cf. §14, #27)}.$$

Therefore

$$Z(f,\omega,s) = \int_I f(x)\omega(x)|x|_A^s \, d^\times x$$

$$= \int_{R_{>0}^{\times}\times I^1} f(tx)\omega(tx)|tx|_A^s \frac{dt}{t} d^\times x$$

$$= \int_0^\infty \left(\int_{I^1} f(tx)\omega(tx)|tx|_A^s \, d^\times x\right) \frac{dt}{t}.$$

5: NOTATION Put

$$Z_t(f,\omega,s) = \int_{I^1} f(tx)\omega(tx)|tx|_A^s \, d^\times x.$$

6: LEMMA

$$Z_t(f,\omega,s) + f(0) \int_{I^1/Q^\times} \omega(tx)|tx|_A^s \, d^\times x$$

$$= Z_{t^{-1}}(\hat{f},\bar{\omega},1-s) + \hat{f}(0)\int_{I^1/Q^\times} \bar{\omega}(t^{-1}x)|t^{-1}x|_A^{1-s} \, d^\times x.$$

PROOF Write

$$\int_{I^1} f(tx)\omega(tx)|tx|_A^s \, d^\times x$$

$$= \int_{I^1/Q^\times} \left(\sum_{r\in Q^\times} f(rtx)\omega(rtx)|rtx|_A^s\right) d^\times x$$

$$= \int_{I^1/Q^\times} \left(\sum_{r\in Q^\times} f(rtx)\omega(tx)|tx|_A^s\right) d^\times x.$$

Then

$$Z_t(f,\omega,s) + f(0) \int_{I^1/Q^\times} \omega(tx)\,|tx|_A^s\, d^\times x$$

$$= \int_{I^1/Q^\times} \Big(\sum_{r\in Q} f(rtx)\Big)\omega(tx)\,|tx|_A^s\, d^\times x$$

$$= \int_{I^1/Q^\times} \Big(\frac{1}{|tx|_A} \sum_{q\in Q} \hat{f}(qt^{-1}x^{-1})\Big)\omega(tx)\,|tx|_A^s\, d^\times x \qquad \text{(cf. §15, \#13)}$$

$$= \int_{I^1/Q^\times} \Big(\sum_{q\in Q} \hat{f}(qt^{-1}x)\Big)\,|t^{-1}x|_A\, \omega(tx^{-1})\,|tx^{-1}|_A^s\, d^\times x \qquad (x \to x^{-1})$$

$$= \int_{I^1/Q^\times} \Big(\sum_{q\in Q} \hat{f}(qt^{-1}x)\Big)\omega^{-1}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x$$

$$= \int_{I^1/Q^\times} \Big(\sum_{q\in Q} \hat{f}(qt^{-1}x)\Big)\bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x$$

$$= \int_{I^1/Q^\times} \Big(\sum_{q\in Q^\times} \hat{f}(qt^{-1}x)\bar{\omega}(qt^{-1}x)\,|qt^{-1}x|_A^{1-s}\Big) d^\times x$$

$$+ \hat{f}(0) \int_{I^1/Q^\times} \bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x$$

$$= \int_{I^1} \hat{f}(t^{-1}x)\bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x$$

$$+ \hat{f}(0) \int_{I^1/Q^\times} \bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x$$

$$= Z_{t^{-1}}(\hat{f},\bar{\omega},1-s) + \hat{f}(0) \int_{I^1/Q^\times} \bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x.$$

Return to $Z(f,\omega,s)$ and break it up as follows:

$$Z(f,\omega,s) = \int_0^1 Z_t(f,\omega,s)\,\frac{dt}{t} + \int_1^\infty Z_t(f,\omega,s)\,\frac{dt}{t}\,.$$

7: LEMMA The integral

$$\int_1^\infty Z_t(f,\omega,s)\,\frac{dt}{t}$$

is a holomorphic function of s.

[It can be expressed as

$$\int_{\substack{I \\ |x|_A \geq 1}} f(x)\omega(x)\,|x|_A^s\,d^\times x.]$$

This leaves

$$\int_0^1 Z_t(f,\omega,s)\,\frac{dt}{t}\,,$$

which can thus be represented as

$$\int_0^1 (Z_{t^{-1}}(\hat{f},\bar{\omega},1-s)$$

$$- f(0) \int_{I^1/Q^\times} \omega(tx)\,|tx|_A^s\,d^\times x$$

$$+ \hat{f}(0) \int_{I^1/Q^\times} \bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\,d^\times x)\,\frac{dt}{t}\,.$$

To carry out the analysis, subject

$$\int_0^1 Z_{t^{-1}}(\hat{f},\bar{\omega},1-s)\,\frac{dt}{t}$$

to the change of variable $t \to t^{-1}$, thereby leading to

$$\int_1^\infty Z_t(\hat{f},\bar{\omega},1-s)\,\frac{dt}{t}\,,$$

a holomorphic function of s (cf. #7 supra).

It remains to discuss

$$R(f,\omega,s) = \int_0^1 (- f(0) \int_{I^1/Q^\times} \omega(tx)\,|tx|_A^s\, d^\times x$$

$$+ \hat{f}(0) \int_{I^1/Q^\times} \bar{\omega}(t^{-1}x)\,|t^{-1}x|_A^{1-s}\, d^\times x)\, \frac{dt}{t}$$

$$= \int_0^1 (- f(0)\omega(t)\,|t|^s \int_{I^1/Q^\times} \omega(x)d^\times x$$

$$+ \hat{f}(0)\bar{\omega}(t^{-1})\,|t^{-1}|^{1-s} \int_{I^1/Q^\times} \bar{\omega}(x)d^\times x)\, \frac{dt}{t},$$

there being two cases.

1. ω is nontrivial on I^1. Since $I^1/Q^\times$ is compact (cf. §14, #24), the integrals

$$\int_{I^1/Q^\times} \omega(x)d^\times x, \quad \int_{I^1/Q^\times} \bar{\omega}(x)d^\times x$$

must vanish (cf. §7, #46). Therefore $R(f,\omega,s) = 0$, hence

$$Z(f,\omega,s) = \int_1^\infty Z_t(f,\omega,s)\, \frac{dt}{t} + \int_1^\infty Z_t(\hat{f},\bar{\omega},1-s)\, \frac{dt}{t},$$

a holomorphic function of s.

2. ω is trivial on I^1. Let $\phi: R_{>0}^\times \to I/I^1$ be the isomorphism per §14, #27 -- then $\omega \circ \phi: R_{>0}^\times \to T$ is a unitary character of $R_{>0}^\times$, thus for some $w \in R$, $\omega \circ \phi = |.|^{-\sqrt{-1}\,w}$, so

$$\omega = |.|^{-\sqrt{-1}\,w} \circ \phi^{-1} \Rightarrow \omega(x) = |x|_A^{-\sqrt{-1}\,w}.$$

Therefore

$$R(f,\omega,s) = - f(0)\text{vol}(I^1/Q^\times) \int_0^1 t^{-\sqrt{-1}\,w + s-1}\, dt$$

$$+ \hat{f}(0)\mathrm{vol}(I^1/Q^\times) \int_0^1 t^{-\sqrt{-1}\,w + s-2}\,dt$$

$$= -\,f(0)\,\frac{\mathrm{vol}(I^1/Q^\times)}{-\sqrt{-1}\,w+s} + \hat{f}(0)\,\frac{\mathrm{vol}(I^1/Q^\times)}{-\sqrt{-1}\,w+s-1},$$

a meromorphic function that has a simple pole at

$$\begin{cases} s = \sqrt{-1}\,w \text{ with residue } & -\,f(0)\mathrm{vol}(I^1/Q^\times) \text{ if } f(0) \neq 0 \\ s = \sqrt{-1}\,w+1 \text{ with residue } & \hat{f}(0)\mathrm{vol}(I^1/Q^\times) \text{ if } \hat{f}(0) \neq 0. \end{cases}$$

8: N.B. To explicate $\mathrm{vol}(I^1/Q^\times)$, use the machinery of §16: In the notation of #2 above,

$$Z(f,1,s) = -\frac{1}{s} + \frac{1}{s-1} + \cdots$$

$$\Rightarrow \mathrm{vol}(I^1/Q^\times) = 1.$$

[Note: Here, $w = 0$ and $f(0) = 1$, $\hat{f}(0) = 1$.]

That $Z(f,\omega,s)$ can be meromorphically continued into the whole s-plane is now manifest. As for the functional equation, we have

$$Z(f,\omega,s) = \int_1^\infty Z_t(f,\omega,s)\,\frac{dt}{t}$$

$$+ \int_1^\infty Z_t(\hat{f},\bar{\omega},1-s)\,\frac{dt}{t}$$

$$+ R(f,\omega,s)$$

$$= \int_1^\infty \left(\int_{I^1} f(tx)\omega(tx)\,|tx|_A^s\,d^\times x\right)\frac{dt}{t}$$

$$+ \int_1^\infty \left(\int_{I^1} \hat{f}(tx)\bar{\omega}(tx)\,|tx|_A^{1-s}\,d^\times x\right)\frac{dt}{t}$$

$$+ R(f,\omega,s).$$

And we also have

$$Z(\hat{f},\bar{\omega},1-s) = \int_1^\infty Z_t(\hat{f},\bar{\omega},1-s)\,\frac{dt}{t}$$

$$+ \int_1^\infty Z_t(\hat{\hat{f}},\bar{\bar{\omega}},1-(1-s))\,\frac{dt}{t}$$

$$+ R(\hat{f},\bar{\omega},1-s)$$

$$= \int_1^\infty Z_t(\hat{f},\bar{\omega},1-s)\,\frac{dt}{t}$$

$$+ \int_1^\infty Z_t(\hat{\hat{f}},\omega,s)\,\frac{dt}{t}$$

$$+ R(\hat{f},\bar{\omega},1-s)$$

$$= \int_1^\infty \left(\int_{I^1} \hat{f}(tx)\bar{\omega}(tx)\,|tx|_A^{1-s}\,d^\times x\right)\frac{dt}{t}$$

$$+ \int_1^\infty \left(\int_{I^1} \hat{\hat{f}}(tx)\omega(tx)\,|tx|_A^{s}\,d^\times x\right)\frac{dt}{t}$$

$$+ R(\hat{f},\bar{\omega},1-s).$$

The first of these terms can be left as is (since it already figures in the formula for $Z(f,\omega,s)$). Recalling that

$$\hat{\hat{f}}(x) = f(-x) \quad (x \in A) \quad \text{(cf. §15, \#10)},$$

the second term becomes

$$\int_1^\infty \left(\int_{I^1} f(-tx)\omega(tx)\,|tx|_A^{s}\,d^\times x\right)\frac{dt}{t}$$

or still,

$$\int_1^\infty \left(\int_{I^1} f(tx)\omega(-tx)\,|-tx|_A^s\, d^\times x\right) \frac{dt}{t}$$

$$= \int_1^\infty \left(\int_{I^1} f(tx)\omega(-tx)\,|tx|_A^s\, d^\times x\right) \frac{dt}{t}\,.$$

But by hypothesis, ω is trivial on $Q^\times$, hence

$$\omega(-tx) = \omega((-1)tx) = \omega(-1)\omega(tx) = \omega(tx),$$

and we end up with

$$\int_1^\infty \left(\int_{I^1} f(tx)\omega(tx)\,|tx|_A^s\, d^\times x\right) \frac{dt}{t}$$

which likewise figures in the formula for $Z(f,\omega,s)$. Finally, if ω is trivial on I^1, then

$$R(\hat{f},\bar{\omega},1-s) = -\frac{\hat{f}(0)}{\sqrt{-1}\,w + 1-s} + \frac{\hat{\hat{f}}(0)}{\sqrt{-1}\,w + (1-s)-1}$$

$$= \frac{f(0)}{\sqrt{-1}\,w - s} - \frac{\hat{f}(0)}{\sqrt{-1}\,w + 1-s}$$

$$= -\frac{f(0)}{-\sqrt{-1}\,w + s} + \frac{\hat{f}(0)}{-\sqrt{-1}\,w + s-1}$$

$$= R(f,\omega,s).$$

On the other hand, if ω is nontrivial on I^1, then $\bar{\omega}$ is nontrivial on I^1 and

$$R(f,\omega,s) = 0,\ R(\hat{f},\bar{\omega},1-s) = 0.$$

§18. *LOCAL ZETA FUNCTIONS [BIS]*

To be in conformity with the global framework laid down in §17, we shall reformulate the local theory of §11 and §12.

1: DEFINITION Given $f \in S(R)$ and a unitary character $\omega: R^\times \to T$, the local zeta function attached to the pair (f,ω) is

$$Z(f,\omega,s) = \int_{R^\times} f(x)\omega(x)|x|^s d^\times x \quad (\mathrm{Re}(s) > 0).$$

2: THEOREM There exists a meromorphic function $\rho(\omega,s)$ such that $\forall f$,

$$\rho(\omega,s) = \frac{Z(f,\omega,s)}{Z(\hat{f},\bar{\omega},1-s)}.$$

Decompose ω as a product:

$$\omega(x) = (\mathrm{sgn}\ x)^\sigma |x|^{-\sqrt{-1}\,w} \quad (\sigma \in \{0,1\},\ w \in R).$$

3: DEFINITION Write (cf. §11, #9)

$$L(\omega,s) = \begin{cases} \Gamma_R(s - \sqrt{-1}\,w) & (\sigma = 0) \\ \Gamma_R(s - \sqrt{-1}\,w + 1) & (\sigma = 1). \end{cases}$$

4: FACT

$$\begin{cases} \rho(\omega,s) = \dfrac{L(\omega,s)}{L(\omega,1-s)} & (\sigma = 0) \\ \rho(\omega,s) = -\sqrt{-1}\,\dfrac{L(\omega,s)}{L(\bar{\omega},1-s)} & (\sigma = 1). \end{cases}$$

5: REMARK The complex case can be discussed analogously but it will not be needed in the sequel.

6: DEFINITION Given $f \in \mathcal{B}(\mathbb{Q}_p)$ and a unitary character $\omega:\mathbb{Q}_p^\times \to \mathbb{T}$, the local zeta function attached to the pair (f,ω) is

$$Z(f,\omega,s) = \int_{\mathbb{Q}_p^\times} f(x)\omega(x)|x|_p^s \, d^\times x \qquad (\mathrm{Re}(s) > 0).$$

7: THEOREM There exists a meromorphic function $\rho(\omega,s)$ such that $\forall$ f,

$$\rho(\omega,s) = \frac{Z(f,\omega,s)}{Z(\hat{f},\bar{\omega},1-s)} .$$

Decompose ω as a product:

$$\omega(x) = \underline{\omega}(x)|x|_p^{-\sqrt{-1}\,w} \quad (\underline{\omega} \in \widehat{\mathbb{Z}_p^\times},\ w \in \mathbb{R}).$$

8: DEFINITION Write (cf. § 12, #8)

$$L(\omega,s) = \begin{cases} (1 - \omega(p)p^{-s})^{-1} & (\underline{\omega} = 1) \\ 1 & (\underline{\omega} \neq 1). \end{cases}$$

[Note: If $\underline{\omega} = 1$, then

$$\omega(p) = |p|_p^{-\sqrt{-1}\,w} = p^{\sqrt{-1}\,w}.]$$

9: FACT $(\underline{\omega} = 1)$

$$\rho(\omega,s) = \frac{L(\omega,s)}{L(\bar{\omega},1-s)} = \frac{1 - \bar{\omega}(p)p^{-(1-s)}}{1 - \omega(p)p^{-s}} .$$

10: FACT ($\underline{\omega} \neq 1$)

$$\rho(\omega,s) = \tau(\omega)\underline{\omega}(-1)p^{n(s + \sqrt{-1} - 1)},$$

where

$$\tau(\omega) = \sum_{i=1}^{r} \underline{\omega}(e_i)\chi_p(p^{-n}e_i)$$

and $\deg \omega = n \geq 1$.

APPENDIX

It can happen that

$$Z(f,\omega,s) \equiv 0.$$

To illustrate, suppose that $\omega(-1) = -1$ and $f(x) = f(-x)$. Working with $Q_p^\times$ (the story for $R^\times$ being the same), we have

$$\begin{aligned} Z(f,\omega,s) &= \int_{Q_p^\times} f(x)\omega(x)|x|_p^s\, d^\times x \\ &= \int_{Q_p^\times} f(-x)\omega(-x)|-x|_p^s\, d^\times x \\ &= \omega(-1) \int_{Q_p^\times} f(x)\omega(x)|x|_p^s\, d^\times x \\ &= \omega(-1)Z(f,\omega,s) \\ &= -Z(f,\omega,s). \end{aligned}$$

§19. *L-FUNCTIONS*

Let $\omega: I/Q^\times \to T$ be a unitary character.

<u>1:</u> LEMMA There is a unique unitary character $\underline{\omega}$ of $I/Q^\times$ of finite order and a unique real number w such that

$$\omega = \underline{\omega}|\cdot|_A^{-\sqrt{-1}\,w}.$$

[Note: To say that $\underline{\omega}$ is of finite order means that there exists a positive integer n such that $\underline{\omega}(x)^n = 1$ for all $x \in I$.]

<u>2:</u> <u>N.B.</u>

$$\omega = \prod_p \omega_p \times \omega_\infty,$$

where

$$\omega_p = \underline{\omega}_p|\cdot|_p^{-\sqrt{-1}\,w}$$

and

$$\omega_\infty = (\mathrm{sgn})^\sigma|\cdot|_\infty^{-\sqrt{-1}\,w}.$$

<u>3:</u> DEFINITION

$$L(\omega,s) = \prod_p L(\omega_p,s) \times L(\omega_\infty,s).$$

<u>4:</u> RAPPEL

$$L(\omega_p,s) = \begin{cases} (1-\omega_p(p)p^{-s})^{-1} & (\underline{\omega}_p = 1) \\ 1 & (\underline{\omega}_p \neq 1) \end{cases} \qquad \text{(cf. §18, \#8).}$$

[Note: The set S_ω of primes for which $\underline{\omega}_p \neq 1$ is finite.]

5: SUBLEMMA

$$|x| < 1 \Rightarrow \log(1-x) = -\sum_{k=1}^{\infty} \frac{x^k}{k}.$$

Therefore

$$|x| > 1 \Rightarrow \log \frac{1}{1-x^{-1}}$$

$$= \log 1 - \log(1-x^{-1})$$

$$= -\left(-\sum_{k=1}^{\infty} \frac{x^{-k}}{k}\right)$$

$$= \sum_{k=1}^{\infty} \frac{x^{-k}}{k}.$$

6: N.B.

$$\log f(z) = \log |f(z)| + \sqrt{-1} \arg f(z)$$

$\Rightarrow$

$$\operatorname{Re} \log f(z) = \log |f(z)|.$$

7: LEMMA The product

$$\prod_p L(\omega_p, s)$$

is absolutely convergent provided $\operatorname{Re}(s) > 1$.

PROOF Ignoring S_ω (a finite set), it is a question of estimating

$$\prod \frac{1}{|1 - \omega_p(p)p^{-s}|}.$$

So take its logarithm and consider

$$\Sigma \log\left(\frac{1}{|1 - \omega_p(p)p^{-s}|}\right)$$

$$= \Sigma \operatorname{Re} \log\left(\frac{1}{1 - \omega_p(p)p^{-s}}\right)$$

$$= \operatorname{Re} \Sigma \log\left(\frac{1}{1 - \omega_p(p)p^{-s}}\right)$$

$$= \operatorname{Re} \Sigma \sum_{k=1}^{\infty} \frac{\omega_p(p)^k p^{-ks}}{k} .$$

The claim then is that the series

$$\Sigma \sum_{k=1}^{\infty} \frac{\omega_p(p)^k p^{-ks}}{k}$$

is absolutely convergent. But

$$\Sigma \sum_{k=1}^{\infty} \left|\frac{\omega_p(p)^k p^{-ks}}{k}\right|$$

$$= \Sigma \sum_{k=1}^{\infty} \frac{p^{-k \operatorname{Re}(s)}}{k}$$

which is bounded by

$$\sum_{p} \sum_{k=1}^{\infty} \frac{p^{-k \operatorname{Re}(s)}}{k}$$

$$= \sum_{p} \sum_{k=1}^{\infty} \frac{p^{-k(1+\delta)}}{k} \qquad (\operatorname{Re}(s) = 1 + \delta)$$

$$\leq \sum_p \sum_{k=1}^{\infty} p^{-k(1+\delta)}$$

$$= \sum_p \frac{p^{-(1+\delta)}}{1 - p^{-(1+\delta)}}$$

$$= \sum_p \frac{1}{p^{(1+\delta)}(1 - p^{-(1+\delta)})}$$

$$= \sum_p \frac{1}{p^{(1+\delta)} - 1}$$

$$\leq 2 \sum_p \frac{1}{p^{1+\delta}} < \infty.$$

8: EXAMPLE Take $\omega = 1$ -- then

$$L(\omega,s) = \prod_p \frac{1}{1 - p^{-s}} \times \Gamma_R(s)$$

$$= \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

9: LEMMA $L(\omega,s)$ is a holomorphic function of s in the strip $\mathrm{Re}(s) > 1$.

10: LEMMA $L(\omega,s)$ admits a meromorphic continuation to the whole s-plane (see below).

Owing to §17, #4, $\forall\ f \in \mathcal{B}_\infty(A)$,

$$Z(f,\omega,s) = Z(\hat{f},\bar{\omega},1-s).$$

To exploit this, assume that

$$f = \prod_p f_p \times f_\infty,$$

where $\forall$ p, $f_p \in \mathcal{B}(Q_p)$ and $f_p = \chi_{Z_p}$ for all but a finite number of p, while $f_\infty \in \mathcal{S}(R)$ -- then

$$Z(f,\omega,s)$$

$$= \int_I f(x)\omega(x)|x|_A^s d^\times x$$

$$= \prod_p \int_{Q_p^\times} f_p(x_p)\omega_p(x_p)|x_p|_p^s d^\times x_p \times \int_{R^\times} f_\infty(x_\infty)\omega_\infty(x_\infty)|x_\infty|_\infty^s d^\times x_\infty$$

$$= \prod_p Z(f_p,\omega_p,s) \times Z(f_\infty,\omega_\infty,s)$$

and analogously for $Z(\hat{f},\bar{\omega},1-s)$.

Therefore

$$1 = \frac{Z(f,\omega,s)}{Z(\hat{f},\bar{\omega},1-s)}$$

$$= \prod_p \frac{Z(f_p,\omega_p,s)}{Z(\hat{f}_p,\bar{\omega}_p,1-s)} \times \frac{Z(f_\infty,\omega_\infty,s)}{Z(\hat{f}_\infty,\bar{\omega}_\infty,1-s)}$$

$$= \prod_p \rho(\omega_p,s) \times \rho(\omega_\infty,s)$$

$$= \prod_{p\notin S_\omega} \rho(\omega_p,s) \times \prod_{p\in S_\omega} \rho(\omega_p,s) \times \rho(\omega_\infty,s)$$

$$= \prod_{p \notin S_\omega} \frac{L(\omega_p,s)}{L(\bar{\omega}_p,1-s)} \times \prod_{p \in S_\omega} \rho(\omega_p,s) \times \frac{L(\omega_\infty,s)}{L(\bar{\omega}_\infty,1-s)}$$

$$= \prod_{p \in S_\omega} \rho(\omega_p,s) \times \prod_{p \notin S_\omega} \frac{L(\omega_p,s)}{L(\bar{\omega}_p,1-s)} \times \prod_{p \in S_\omega} \frac{L(\omega_p,s)}{L(\bar{\omega}_p,1-s)} \times \frac{L(\omega_\infty,s)}{L(\bar{\omega}_\infty,1-s)}$$

$$= \prod_{p \in S_\omega} \rho(\omega_p,s) \times \prod_{p} \frac{L(\omega_p,s)}{L(\bar{\omega}_p,1-s)} \times \frac{L(\omega_\infty,s)}{L(\bar{\omega}_\infty,1-s)}$$

$$= \prod_{p \in S_\omega} \rho(\omega_p,s) \times \frac{\prod_p L(\omega_p,s) \times L(\omega_\infty,s)}{\prod_p L(\bar{\omega}_p,1-s) \times L(\bar{\omega}_\infty,1-s)}$$

$$= \prod_{p \in S_\omega} \rho(\omega_p,s) \times \frac{L(\omega,s)}{L(\bar{\omega},1-s)}$$

$$= \prod_{p \in S_\omega} \varepsilon(\omega_p,s) \times \frac{L(\omega,s)}{L(\bar{\omega},1-s)} \qquad \text{(cf. §12, \#11)}$$

$$= \varepsilon(\omega,s) \times \frac{L(\omega,s)}{L(\bar{\omega},1-s)},$$

where

$$\varepsilon(\omega,s) = \prod_{p \in S_\omega} \varepsilon(\omega_p,s).$$

11: THEOREM

$$L(\bar{\omega},1-s) = \varepsilon(\omega,s)L(\omega,s).$$

12: EXAMPLE Take $\omega = 1$ (cf. #8) -- then $\varepsilon(\omega,s) = 1$ and

$$L(\bar{\omega},1-s) = L(\omega,s)$$

translates into

$$\pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) \qquad \text{(cf. §16)}.$$

Make the following explicit choice for

$$f = \prod_p f_p \times f_\infty.$$

- If $\underline{\omega}_p = 1$, let

$$f_p(x_p) = \chi_p(x_p)\chi_{Z_p}(x_p).$$

Then

$$Z(f_p,\omega_p,s) = L(\omega_p,s).$$

- If $\underline{\omega}_p \neq 1$ and $\deg \omega_p = n \geq 1$, let

$$f_p(x_p) = \chi_p(x_p)\chi_{p^{-n}Z_p}(x_p).$$

Then

$$Z(f_p,\omega_p,s) = \tau(\omega_p)\,\frac{p^{1+n(s+\sqrt{-1}\,w-1)}}{p-1}\,L(\omega_p,s).$$

At infinity, take

$$f_\infty(x_\infty) = e^{-\pi x_\infty^2}(\sigma = 0) \text{ or } f_\infty(x_\infty) = x_\infty e^{-\pi x_\infty^2}(\sigma = 1).$$

Then

$$Z(f_\infty,\omega_\infty,s) = L(\omega_\infty,s).$$

<u>13:</u> NOTATION Put

$$H(\omega,s) = \prod_{p\in S_\omega} \tau(\omega_p)\,\frac{p^{1+n(s+\sqrt{-1}\,w-1)}}{p-1}.$$

14: N.B. $H(\omega,s)$ is a never zero entire function of s.

15: LEMMA

$$Z(f,\omega,s) = H(\omega,s)L(\omega,s).$$

Since $Z(f,\omega,s)$ is a meromorphic function of s (cf. §17, #4), it therefore follows that $L(\omega,s)$ is a meromorphic function of s.

Working now within the setting of §17, we distinguish two cases per ω.

1. ω is nontrivial on I^1, hence $\underline{\omega} \neq 1$ and in this situation, $Z(f,\omega,s)$ is a holomorphic function of s, hence the same is true of $L(\omega,s)$.

2. ω is trivial on I^1 — then $\omega = |.|_A^{-\sqrt{-1}\,w}$ and there are simple poles at

$$\begin{cases} s = \sqrt{-1}\,w \text{ with residue } - f(0) \text{ if } f(0) \neq 0 \\ s = \sqrt{-1}\,w + 1 \text{ with residue } \hat{f}(0) \text{ if } \hat{f}(0) \neq 0. \end{cases}$$

But $\forall$ p, $\omega_p = |.|_p^{-\sqrt{-1}\,w}$ ($\Rightarrow \underline{\omega}_p = 1$), so $f_p(0) = 1$. And likewise $f_\infty(0) = 1$ $(\sigma = 0)$. Conclusion: $f(0) = 1$. As for the Fourier transforms, $\hat{f}_p = \chi_{Z_p} \Rightarrow \hat{f}_p(0) = 1$. Also $\hat{f}_\infty = f_\infty$ $(\sigma = 0) \Rightarrow \hat{f}_\infty(0) = 1$. Conclusion: $\hat{f}(0) = 1$. The respective residues are therefore -1 and 1.

16: THEOREM Suppose that $\omega_{1,p} = \omega_{2,p}$ for all but finitely many p and $\omega_{1,\infty} = \omega_{2,\infty}$ -- then $\omega_1 = \omega_2$.

PROOF Put $\omega = \omega_1\omega_2^{-1}$, thus $\omega_p = 1$ for all p outside a finite set S of primes, so

$$L(\omega,s) = \prod_p L(\omega_p,s) \times L(\omega_\infty,s)$$

$$= \prod_{p \in S} L(\omega_p, s) \prod_{p \notin S} L(1_p, s) \times L(1_\infty, s)$$

$$= L(1,s) \prod_{p \in S} \frac{L(\omega_p, s)}{L(1_p, s)}$$

$$= L(1,s) \prod_{p \in S} \frac{1 - p^{-s}}{1 - \alpha_p p^{-s}},$$

where $\alpha_p = \omega_p(p)$ if $\underline{\omega}_p = 1$ and $\alpha_p = 0$ if $\underline{\omega}_p \neq 1$, and each factor

$$\frac{1 - p^{-s}}{1 - \alpha_p p^{-s}}$$

is nonzero at $s = 0$ and $s = 1$. Therefore $L(\omega,s)$ has a simple pole at $s = 0$ and $s = 1$. Consider the decomposition

$$\omega = \underline{\omega} |\cdot|_A^{-\sqrt{-1}\, w} \qquad \text{(cf §19, \#1)}.$$

Then $\underline{\omega} = 1$ since otherwise $L(\omega,s)$ would be holomorphic, which it isn't. But then from the theory, $L(\omega,s)$ has simple poles at

$$\begin{cases} s = \sqrt{-1}\, w \text{ with residue } -1 \\ s = \sqrt{-1}\, w + 1 \text{ with residue } 1, \end{cases}$$

thereby forcing $w = 0$, which implies that $\omega = 1$, i.e., $\omega_1 = \omega_2$.

[Note: In the end, $\omega_p = 1 \ \forall\, p$, hence

$$\prod_{p \in S} \frac{1 - p^{-s}}{1 - \alpha_p p^{-s}} = \prod_{p \in S} \frac{1 - p^{-s}}{1 - p^{-s}} = 1,$$

as it has to be.]

§20. *FINITE CLASS FIELD THEORY*

Given a finite field F_q of characteristic p (thus q is an integral power of p), then in $F_p^{c\ell}$,

$$F_q = \{x : x^q = x\}.$$

1: LEMMA The multiplicative group

$$F_q^{\times} = \{x : x^{q-1} = 1\}$$

is cyclic of order q - 1.

2: NOTATION

$$F_{q^n} = \{x : x^{q^n} = x\} \quad (n \geq 1).$$

3: LEMMA F_{q^n} is a Galois extension of F_q of degree n.

4: LEMMA $\mathrm{Gal}(F_{q^n}/F_q)$ is a cyclic group of order n generated by the element $\sigma_{q,n}$, where

$$\sigma_{q,n}(x) = x^q \quad (x \in F_{q^n}).$$

5: LEMMA The F_{q^n} are finite abelian extensions of F_q and they comprise all the finite extensions of F_q, hence the algebraic closure $\bigcup_n F_{q^n}$ is F_q^{ab}.

6: THEOREM There is a 1-to-1 correspondence between the finite abelian extensions of F_q and the subgroups of Z of finite index which is given by

$$F_{q^n} \longleftrightarrow nZ \quad (n \geq 1).$$

Schematically:

$$F_q \subset F_{q^2} \subset F_{q^4}$$

$$\cap \quad \cap$$

$$F_{q^3} \subset F_{q^6}$$

$$\cap$$

$$F_{q^9}$$

$$\longleftrightarrow$$

$$Z \supset 2Z \supset 4Z$$

$$\cup \quad \cup$$

$$3Z \supset 6Z$$

$$\cup$$

$$9Z.$$

The "class field" aspect of all this is the existence of a canonical homomorphism

$$rec_q : Z \to Gal(F_q^{ab}/F_q).$$

<u>7:</u> NOTATION Define

$$\sigma_q \in Gal(F_q^{ab}/F_q)$$

by

$$\sigma_q(x) = x^q.$$

8: N.B. Under the arrow of restriction

$$\mathrm{Gal}(F_q^{ab}/F_q) \to \mathrm{Gal}(F_{q^n}/F_q),$$

σ_q is sent to $\sigma_{q,n}$.

9: DEFINITION

$$\mathrm{rec}_q(k) = \sigma_q^k \quad (k \in Z).$$

10: LEMMA The identification

$$Z/nZ \approx \mathrm{Gal}(F_{q^n}/F_q)$$

is the arrow $k \to \sigma_{q,n}^k$.

On general grounds,

$$\mathrm{Gal}(F_q^{ab}/F_q) = \varprojlim \mathrm{Gal}(F_{q^n}/F_q).$$

[Note: The open subgroups of $\mathrm{Gal}(F_q^{ab}/F_q)$ are the $\mathrm{Gal}(F_q^{ab}/F_{q^n})$ and

$$\mathrm{Gal}(F_q^{ab}/F_q)/\mathrm{Gal}(F_q^{ab}/F_{q^n}) \approx \mathrm{Gal}(F_{q^n}/F_q).]$$

Therefore

$$\mathrm{Gal}(F_q^{ab}/F_q) \approx \varprojlim Z/nZ,$$

another realization of the RHS being $\prod_p Z_p$ which if invoked leads to

$$\sigma_q \longleftrightarrow (1,1,1,\ldots).$$

11: N.B. The composition

$$Z \xrightarrow{rec_q} Gal(F_q^{ab}/F_q) \approx \lim_{\leftarrow} Z/nZ$$

coincides with the canonical map

$$k \to (k \bmod n)_n.$$

12: REMARK Give Z the discrete topology -- then

$$rec_q: Z \to Gal(F_q^{ab}/F_q)$$

is continuous and injective but it is not a homeomorphism ($Gal(F_q^{ab}/F_q)$ is compact).

[Note: The image $rec_q(Z)$ is the cyclic subgroup $<\sigma_q>$ generated by σ_q. And:

- $<\sigma_q> \neq Gal(F_q^{ab}/F_q)$
- $\overline{<\sigma_q>} = Gal(F_q^{ab}/F_q)$.]

13: SCHOLIUM The finite abelian extensions of F_q correspond 1-to-1 with the open subgroups of $Gal(F_q^{ab}/F_q)$.

[Quote the appropriate facts from infinite Galois theory.]

14: SCHOLIUM The open subgroups of $Gal(F_q^{ab}/F_q)$ correspond 1-to-1 with the open subgroups of Z of finite index.]

[Given an open subgroup $U \subset Gal(F_q^{ab}/F_q)$, send it to $rec_q^{-1}(U) \subset Z$ (discrete topology). Explicated:

$$rec_q^{-1}(Gal(F_q^{ab}/F_{q^n})) = nZ.]$$

APPENDIX

The norm map

$$N_{F_{q^n}/F_q} : F_{q^n}^{\times} \to F_q^{\times}$$

is surjective.

[Let $x \in F_{q^n}^{\times}$:

$$N_{F_{q^n}/F_q}(x) = \prod_{i=0}^{n-1} (\sigma_{q,n})^i x$$

$$= \prod_{i=0}^{n-1} x^{q^i}$$

$$= x^{\sum_{i=0}^{n-1} q^i}$$

$$= x^{(q^n-1)/(q-1)}.$$

Specialize now and take for x a generator of $F_{q^n}^{\times}$, hence x is of order q^n-1, hence $N_{F_{q^n}/F_q}(x)$ is of order $q-1$, hence is a generator of F_q.]

§21. *LOCAL CLASS FIELD THEORY*

Let K be a local field -- then there exists a unique continuous homomorphism

$$\text{rec}_K : K^\times \to \text{Gal}(K^{ab}/K),$$

the so-called <u>reciprocity map</u>, that has the properties delineated in the results that follow.

<u>1:</u> CHART

finite field K	Z	$\text{Gal}(K^{ab}/K)$
local field K	$K^\times$	$\text{Gal}(K^{ab}/K)$.

<u>2:</u> CONVENTION An <u>abelian extension</u> is a Galois extension whose Galois group is abelian.

<u>3:</u> SCHOLIUM The finite abelian extensions L of K correspond 1-to-1 with the open subgroups of $\text{Gal}(K^{ab}/K)$:

$$L \longleftrightarrow \text{Gal}(K^{ab}/L).$$

[Note: $\text{Gal}(L/K)$ is a homomorphic image of $\text{Gal}(K^{ab}/K)$:

$$\text{Gal}(L/K) \approx \text{Gal}(K^{ab}/K)/\text{Gal}(K^{ab}/L).]$$

<u>4:</u> LEMMA Suppose that L is a finite extension of K -- then

$$N_{L/K} : L^\times \to K^\times$$

is continuous, sends open sets to open sets, and closed sets to closed sets.

5: LEMMA Suppose that L is a finite extension of K -- then

$$[K^\times:N_{L/K}(L^\times)] \leq [L:K].$$

6: LEMMA Suppose that L is a finite extension of K -- then

$$[K^\times:N_{L/K}(L^\times)] = [L:K]$$

iff L/K is abelian.

7: NOTATION Given a finite abelian extension L of K, denote the composition

$$K^\times \xrightarrow{\text{rec}_K} \text{Gal}(K^{ab}/K) \xrightarrow{\pi_{L/K}} \text{Gal}(L/K)$$

by (., L/K), the norm residue symbol.

8: THEOREM Suppose that L is a finite abelian extension of K -- then the kernel of (., L/K) is $N_{L/K}(L^\times)$, hence

$$K^\times/N_{L/K}(L^\times) \approx \text{Gal}(L/K).$$

9: EXAMPLE Take K = R, thus K^{ab} = C and

$$N_{C/R}(C^\times) = R^\times_{>0}.$$

Moreover,

$$\text{Gal}(C/R) = \{\text{id}_C,\sigma\},$$

where σ is the complex conjugation. Define now

$$\text{rec}_R:R^\times \to \text{Gal}(R^{ab}/R)$$

by stipulating that

$$\text{rec}_R(R^\times_{>0}) = \text{id}_C,\ \text{rec}_R(R^\times_{<0}) = \sigma.$$

<u>10:</u> EXAMPLE Take $K = C$ -- then $K^{ab} = C = K$ and matters in this situation are trivial.

<u>11:</u> THEOREM The arrow

$$L \to N_{L/K}(L^\times)$$

is a bijection between the finite abelian extensions of K and the open subgroups of finite index of $K^\times$.

<u>12:</u> THEOREM The arrow $U \to rec_K^{-1}(U)$ is a bijection between the open subgroups of $Gal(K^{ab}/K)$ and the open subgroups of finite index of $K^\times$.

From this point forward, it will be assumed that K is non-archimedean, hence is a finite extension of Q_p for some p (cf. §5, #13).

<u>13:</u> LEMMA rec_K is injective and its image is a proper, dense subgroup of $Gal(K^{ab}/K)$.

<u>14:</u> LEMMA

$$(R^\times, L/K) = Gal(L/K_{ur}),$$

where K_{ur} is the largest unramified extension of K contained in L (cf. §5, #33).

[Note: The image

$$(1 + P^i, L/K) = G^i \quad (i \geq 1),$$

the i^{th} <u>ramification group in the upper numbering</u> (conventionally, one puts

$$G^0 = Gal(L/K_{ur})$$

and refers to it as the inertia group).]

Working within K^{sep}, the extension K^{ur} generated by the finite unramified extensions of K is called the maximal unramified extension of K. This is a Galois extension and

$$\mathrm{Gal}(K^{ur}/K) \approx \mathrm{Gal}(F_q^{ab}/F_q),$$

where $F_q = R/P$ (cf. §5, #19).

15: REMARK The finite unramified extensions L of K correspond 1-to-1 with the finite extensions of $R/P = F_q$ and

$$\mathrm{Gal}(L/K) \approx \mathrm{Gal}(F_{q^n}/F_q) \qquad (n = [L:K]).$$

16: LEMMA K^{ur} is the field obtained by adjoining to K all roots of unity having order prime to p.

17: APPLICATION K^{ur} is a subfield of K^{ab}.

[Cyclotomic extensions are Galois and abelian.]

18: THEOREM There is a commutative diagram

$$\begin{array}{ccc} K^{\times} & \xrightarrow{\ \mathrm{rec}_K\ } & \mathrm{Gal}(K^{ab}/K) \\ {\scriptstyle v_K}\downarrow & & \downarrow \\ Z & \xrightarrow[\ \mathrm{rec}_q\ ]{} & \mathrm{Gal}(F_q^{ab}/F_q), \end{array}$$

the vertical arrow on the right being the composition

$$\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(K^{ab}/K)/\mathrm{Gal}(K^{ab}/K^{ur})$$

$$\approx \mathrm{Gal}(K^{ur}/K)$$

$$\approx \mathrm{Gal}(F_q^{ab}/F_q).$$

[Note: $\forall\ a \in K^{\times}$,

$$\mathrm{mod}_K(a) = q^{-\mathrm{ord}_K(a)}.]$$

19: N.B. The image of

$$\mathrm{rec}_K(\pi)\,|K^{ur} \in \mathrm{Gal}(K^{ur}/K)$$

in $\mathrm{Gal}(F_q^{ab}/F_q)$ is σ_q (cf. §20, #7).

[Note: If L is a finite unramified extension of K and if $\tilde{\sigma}_{q,n}$ is the generator of Gal(L/K) which is the lift of the generator $\sigma_{q,n}$ of $\mathrm{Gal}(F_{q^n}/F_q)$ ($n = [L:K]$), then

$$(\pi, L/K) = \tilde{\sigma}_{q,n}.]$$

20: FUNCTORIALITY Suppose that $L \supset K$ is a finite extension of K -- then the diagram

$$\begin{array}{ccc} L^{\times} & \xrightarrow{\ \mathrm{rec}_L\ } & \mathrm{Gal}(L^{ab}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ K^{\times} & \xrightarrow[\ \mathrm{rec}_K\ ]{} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

commutes.

21: DEFINITION Given a Hausdorff topological group G, let G* be its commutator subgroup, and put $G^{ab} = G/\overline{G^*}$ -- then $\overline{G^*}$ is a closed normal subgroup of G and G^{ab} is abelian, the topological abelianization of G.

22: EXAMPLE

$$\mathrm{Gal}(K^{sep}/K)^{ab} = \mathrm{Gal}(K^{ab}/K).$$

23: CONSTRUCTION Let G be a Hausdorff topological group and let H be a closed subgroup of finite index -- then the transfer homomorphism $\tau: G^{ab} \to H^{ab}$ is defined as follows: Choose a section $s: H\backslash G \to G$ and for $x \in G$, put

$$\tau(x\overline{G^*}) = \prod_{\alpha \in H\backslash G} h_{x,\alpha} \pmod{\overline{H^*}},$$

where $h_{x,\alpha} \in H$ is defined by

$$s(\alpha)x = h_{x,\alpha}\, s(\alpha x).$$

24: EXAMPLE Suppose that $L \supset K$ is a finite extension of K -- then $L^{sep} \approx K^{sep}$ and

$$\mathrm{Gal}(L^{sep}/L) \subset \mathrm{Gal}(K^{sep}/K)$$

is a closed subgroup of finite index (viz. [L:K]), hence there is a transfer homomorphism

$$\tau: \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L^{ab}/L).$$

25: THEOREM The diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\ rec_L\ } & \mathrm{Gal}(L^{ab}/L) \\ \uparrow & & \uparrow \tau \\ K^\times & \xrightarrow[\ rec_K\ ]{} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

commutes.

§22. *WEIL GROUPS: THE ARCHIMEDEAN CASE*

<u>1.</u> DEFINITION Put $W_C = C^\times$, call it the <u>Weil group</u> of C, and leave it at that.

<u>2:</u> DEFINITION Put

$$W_R = C^\times \cup JC^\times \quad \text{(disjoint union) (J a formal symbol)},$$

where $J^2 = -1$ and $JzJ^{-1} = \bar{z}$ (obvious topology on W_R). Accordingly, there is a nonsplit short exact sequence

$$1 \to C^\times \to W_R \to \text{Gal}(C/R) \to 1,$$

the image of J in Gal(C/R) being complex conjugation.

[Note: $H^2(\text{Gal}(C/R), C^\times)$ is cyclic of order 2, thus up to equivalence of extensions of Gal(C/R) by $C^\times$ per the canonical action of Gal(C/R) on $C^\times$, there are two possibilities:

1. A split extension

$$1 \to C^\times \to E \to \text{Gal}(C/R) \to 1.$$

2. A nonsplit extension

$$1 \to C^\times \to E \to \text{Gal}(C/R) \to 1.$$

The Weil group W is a representative of the second situation which is why we took $J^2 = -1$ (rather than $J^2 = +1$).]

<u>3:</u> LEMMA The commutator subgroup W_R^* of W_R consists of all elements of the form $JzJ^{-1}z^{-1} = \frac{\bar{z}}{z}$, i.e., $W_R^* = S$, thus is closed.

Let

$$\mathrm{pr}: W_R \to R^\times$$

be the map sending J to -1 and z to $|z|^2$.

<u>4:</u> LEMMA S is the kernel of pr and pr is surjective.

<u>5:</u> LEMMA The arrow

$$\mathrm{pr}^{ab}: W_R^{ab} \to R^\times$$

induced by pr is an isomorphism.

<u>6:</u> REMARK The inverse $R^\times \to W_R^{ab}$ of pr^{ab} is characterized by the conditions

$$\begin{cases} -1 \longrightarrow JW_R^* \\ x \longrightarrow \sqrt{x}\, W_R^* \quad (x > 0). \end{cases}$$

<u>7:</u> NOTATION Define

$$||.||: W_R \to R_{>0}^\times$$

by the prescription

$$||z|| = z\bar{z} \ (z \in C), \ ||J|| = 1.$$

<u>8:</u> <u>N.B.</u> $||.||$ drops to a continuous homomorphism $W_R^{ab} \to R_{>0}^\times$.

<u>9:</u> DEFINITION A <u>representation</u> of W_R is a continuous homomorphism $\rho: W_R \to GL(V)$, where V is a finite dimensional complex vector space.

<u>10:</u> EXAMPLE If $s \in C$, then the assignment $w \to ||w||^s$ is a 1-dimensional

representation of W_R, i.e., is a character.

11: N.B. If χ is a character of $R^\times$, then $\chi \circ pr$ is a character of W_R and all such have this form.

[For any $\rho \in \tilde{W}_R$,

$$\rho(\bar{z}) = \rho(JzJ^{-1}) = \rho(J)\rho(z)\rho(J)^{-1} = \rho(z).$$

Therefore

$$1 = \rho(-1) \quad (\text{cf. §7, \#12}).$$

But

$$\rho(-1) = \rho(J^2) = \rho(J)^2,$$

so $\rho(J) = \pm 1$. This said, the characters of $R^\times$ are described in §7, #11, thus the 1-dimensional representations of W_R are parameterized by a sign and a complex number s:

- $(+,s): \rho(z) = |z|^s$, $\rho(J) = +1$
- $(-,s): \rho(z) = |z|^s$, $\rho(J) = -1$.]

Let V be a finite dimensional complex vector space.

12: DEFINITION A linear transformation $T:V \rightarrow V$ is semisimple if every T-invariant subspace has a complementary T-invariant subspace.

13: FACT T is semisimple iff T is diagonalizable, i.e., in some basis T is represented by a diagonal matrix.

[Bear in mind that C is algebraically closed... .]

<u>14:</u> DEFINITION A representation $\rho:W_R \to GL(V)$ is <u>semisimple</u> if $\forall\, w \in W_R$, $\rho(w):V \to V$ is semisimple.

<u>15:</u> DEFINITION A representation $\rho:W_R \to GL(V)$ is <u>irreducible</u> if $V \neq 0$ and the only ρ-invariant subspaces are 0 and V.

The irreducible 1-dimensional representations of W_R are its characters (which, of course, are automatically semisimple).

<u>16:</u> LEMMA If $\rho:W_R \to GL(V)$ is a semisimple irreducible representation of W_R of dimension > 1, then dim V = 2.

PROOF There is a nonzero vector $v \in V$ and a character $\chi:C^\times \to C^\times$ such that $\forall\, z \in C^\times$,

$$\rho(z)v = \chi(z)v.$$

Since the span S of $v, \rho(J)v$ is a ρ-invariant subspace, the assumption of irreducibility implies that dim V = 2.

[To check the ρ-invariance of S, note that

$$\left[\begin{array}{l} \rho(z)\rho(J)v = \rho(zJ)v = \rho(J\bar{z})v = \rho(J)\rho(\bar{z})v = \rho(J)\chi(\bar{z})v \\ \rho(J)\rho(J)v = \rho(J^2)v = \rho(-1)v = \chi(-1)v.] \end{array}\right.$$

Given an integer k and a complex number s, define a character $\chi_{k,s}:C^\times \to C^\times$ by the prescription

$$\chi_{k,s}(z) = \left(\frac{z}{|z|}\right)^k (|z|^2)^s$$

and let $\rho_{k,s} = \operatorname{ind} \chi_{k,s}$ be the representation of W_R which it induces.

17: LEMMA $\rho_{k,s}$ is 2-dimensional.

18: LEMMA $\rho_{k,s}$ is semisimple.

19: LEMMA $\rho_{k,s}$ is irreducible iff $k \neq 0$.

20: DEFINITION Let

$$\begin{cases} \rho_1 : W_R \to GL(V_1) \\ \rho_2 : W_R \to GL(V_2) \end{cases}$$

be representations of W_R -- then (ρ_1, V_1) is equivalent to (ρ_2, V_2) if there exists an isomorphism $f: V_1 \to V_2$ such that $\forall\, w \in W_R$,

$$f \circ \rho_1(w) = \rho_2(w) \circ f.$$

21: LEMMA ρ_{k_1,s_1} is equivalent to ρ_{k_2,s_2} iff $k_1 = k_2$, $s_1 = s_2$ or $k_1 = -k_2$, $s_1 = s_2$.

22: THEOREM Every 2-dimensional semisimple irreducible representation of W_R is equivalent to a unique $\rho_{k,s}$ $(k > 0)$.

23: N.B. Therefore the equivalence classes of 2-dimensional semisimple irreducible representations of W_R are parameterized by the points of $N \times C$.

24: DEFINITION A representation $\rho: W_R \to GL(V)$ is completely reducible if V is the direct sum of a collection of irreducible ρ-invariant subspaces.

25: LEMMA Let $\rho: W_R \to GL(V)$ be a semisimple representation -- then ρ is completely reducible.

PROOF The characters of $C^\times$ are of the form $z \to z^\mu \bar{z}^\nu$ with $\mu, \nu \in C$, $\mu - \nu \in Z$ and V is the direct sum of subspaces $V_{\mu,\nu}$, where $\rho(z)|V_{\mu,\nu} = z^\mu \bar{z}^\nu \, id_{V_{\mu,\nu}}$. Claim:

$$\rho(J)V_{\mu,\nu} = V_{\nu,\mu}.$$

Proof: $\forall \ v \in V_{\mu,\nu}$,

$$\begin{aligned}
\rho(z)\rho(J)v &= \rho(J\bar{z}J^{-1})\rho(J)v \\
&= \rho(J)\rho(\bar{z})\rho(J^{-1})\rho(J)v \\
&= \rho(J)\rho(\bar{z})v \\
&= \rho(J)\bar{z}^\mu z^\nu v \\
&= \rho(J)z^\nu \bar{z}^\mu v \\
&= z^\nu \bar{z}^\mu \rho(J)v.
\end{aligned}$$

Proceeding:

- $\mu = \nu$ Choose a basis of eigenvectors for $\rho(J)$ on $V_{\mu,\mu}$ -- then the span of each eigenvector is a 1-dimensional ρ-invariant subspace.

- $\mu \neq \nu$ Choose a basis $v_1, \ldots, v_r$ for $V_{\mu,\nu}$ and put $v_i' = \rho(J)v_i$ $(1 \leq i \leq r)$ -- then $Cv_i \oplus Cv_i'$ is a 2-dimensional ρ-invariant subspace and the direct sum

$$\bigoplus_{i=1}^{r} (Cv_i \oplus Cv_i')$$

equals

$$V_{\mu,\nu} \oplus V_{\nu,\mu}.$$

<u>26:</u> REMARK Suppose that $\rho : W_R \rightarrow GL(V)$ is a representation -- then

$$J^2 = -1 \Rightarrow (-1)J \cdot J = 1$$

$$\Rightarrow (-1)J = J^{-1}$$

$\Rightarrow$

$$\rho(J)^{-1} = \rho(J^{-1})$$

$$= \rho((-1)J)$$

$$= \rho(-1)\rho(J).$$

On the other hand, if $J^2 = 1$ (the split extension situation (cf. #2)), then

$$id_V = \rho(1)$$

$$= \rho(J^2) = \rho(J)\rho(J)$$

$\Rightarrow$

$$\rho(J)^{-1} = \rho(J).$$

§23. *WEIL GROUPS: THE NON-ARCHIMEDEAN CASE*

Let K be a non-archimedean local field.

1: NOTATION Put

$$\begin{cases} G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K) \\ G_K^{ab} = \mathrm{Gal}(K^{ab}/K). \end{cases}$$

2: N.B. Every character of G_K factors through $\overline{G_K^*}$, hence gives rise to a character of G_K^{ab}.

To study the characters of G_K^{ab}, precompose with the reciprocity map $\mathrm{rec}_K : K^\times \to G_K^{ab}$, thus

$$\chi_K : \begin{cases} (G_K^{ab})^{\sim} \to (K^\times)^{\sim} \\ \chi \to \chi \circ \mathrm{rec}_K. \end{cases}$$

3: LEMMA χ_K is a homomorphism.

4: LEMMA χ_K is injective.

PROOF Suppose that

$$\chi_K(\chi) = \chi \circ \mathrm{rec}_K$$

is trivial -- then $\chi | \mathrm{Im}\ \mathrm{rec}_K = 1$. But $\mathrm{Im}\ \mathrm{rec}_K$ is dense in G_K^{ab} (cf. §21, #13), so by continuity, $\chi \equiv 1$.

5: LEMMA χ_K is not surjective.

PROOF G_K^{ab} is compact abelian and totally disconnected. Therefore $(G_K^{ab})^{\sim} = (G_K^{ab})^{\wedge}$ and every χ is unitary and of finite order (cf. §7, #7 and §8, #2), thus the $\chi_K(\chi)$ are unitary and of finite order. But there are characters of $K^{\times}$ for which this is not the case.

6: N.B. The failure of χ_K to be surjective will be remedied below (cf. #19).

The kernel of the arrow

$$\mathrm{Gal}(K^{sep}/K) \rightarrow \mathrm{Gal}(K^{ur}/K)$$

of restriction is $\mathrm{Gal}(K^{sep}/K^{ur})$ and there is an exact sequence

$$1 \rightarrow \mathrm{Gal}(K^{sep}/K^{ur}) \rightarrow \mathrm{Gal}(K^{sep}/K) \rightarrow \mathrm{Gal}(K^{ur}/K) \rightarrow 1.$$

Identify

$$\mathrm{Gal}(K^{ur}/K)$$

with

$$\mathrm{Gal}(F_q^{ab}/F_q)$$

and put

$$W(F_q^{ab}/F_q) = \langle\sigma_q\rangle \quad \text{(discrete topology)}.$$

7: DEFINITION The Weil group $W(K^{sep}/K)$ is the inverse image of $W(F_q^{ab}/F_q)$ in $\mathrm{Gal}(K^{sep}/K)$, i.e., the elements in $\mathrm{Gal}(K^{sep}/K)$ which induce an integral power of σ_q.

<u>8:</u> NOTATION Abbreviate $W(K^{sep}/K)$ to W_K, hence $W_K \subset G_K$.

Setting

$$I_K = Gal(K^{sep}/K^{ur}) \quad \text{(the } \underline{\text{inertia group}}\text{)},$$

there is an exact sequence

$$1 \to I_K \to W_K \to W(F_q^{ab}/F_q) \to 1.$$

$$\updownarrow \approx$$

$$Z$$

[Note: Fix an element $\tilde{\sigma}_q \in W_K$ which maps to σ_q -- then structurally, W_K is the disjoint union

$$\underset{n \in Z}{\cup} (\tilde{\sigma}_q)^n I_K.]$$

Topologize W_K by taking for a neighborhood basis at the identity the

$$Gal(K^{sep}/L) \cap I_K,$$

where L is a finite Galois extension of K.

<u>9:</u> REMARK I_K has the relative topology per the inclusion $I_K \to G_K$ and any splitting $Z \to W_K$ induces an isomorphism $W_K \approx I_K \times Z$ of topological groups, where Z has the discrete topology.

<u>10:</u> LEMMA W_K is a totally disconnected locally compact group.

[Note: W_K is not compact... .]

<u>11:</u> LEMMA The inclusion $W_K \to G_K$ is continuous and has a dense image.

12: LEMMA I_K is open in W_K.

13: LEMMA I_K is a maximal compact subgroup of W_K.

Suppose that $L \supset K$ is a finite extension of K -- then $G_L \subset G_K$ is the subgroup of G_K fixing L, hence

$$W_L \subset G_L \subset G_K.$$

14: LEMMA

$$W_L = G_L \cap W_K \subset W_K$$

is open and of finite index in W_K, it being normal in W_K iff L/K is Galois.

15: THEOREM The arrow

$$L \rightarrow W_L$$

is a bijection between the finite extensions of K and the open subgroups of finite index of W_K.

[By contrast, the arrow

$$L \rightarrow \mathrm{Gal}(K^{sep}/L)$$

is a bijection between the finite extensions of K and the open subgroups of G_K.]

16: LEMMA

$$\overline{W_K^*} = \overline{G_K^*}\ .$$

17: APPLICATION The homomorphism $W_K^{ab} \rightarrow G_K^{ab}$ is 1-to-1.

<u>18:</u> THEOREM The image of $\text{rec}_K: K^\times \to G_K^{ab}$ is W_K^{ab} and the induced map $K^\times \to W_K^{ab}$ is an isomorphism of topological groups (cf. §21, #13).

The characters of W_K "are" the characters of W_K^{ab}, so we have:

<u>19:</u> SCHOLIUM There is a bijective correspondence between the characters of W_K and the characters of $K^\times$ or still, there is a bijective correspondence between the 1-dimensional representations of W_K and the 1-dimensional representations of $GL_1(K)$.

Suppose that $L \supset K$ is a finite Galois extension of K -- then $G_L \subset G_K$ and

$$G_K/G_L \approx \text{Gal}(L/K)$$

is finite of cardinality $[L:K]$. Since W_K is dense in G_K, it follows that the image of the arrow

$$\begin{cases} W_K \to G_K/G_L \\ w \to wG_L \end{cases}$$

is all of G_K/G_L, its kernel being those $w \in W_K$ such that $w \in G_L$, i.e., its kernel is $G_L \cap W_K$ or still, is W_L.

<u>20:</u> LEMMA

$$W_K/W_L \approx G_K/G_L \approx \text{Gal}(L/K).$$

<u>21:</u> LEMMA $\overline{W_L^*}$ is a normal subgroup of W_K.

[Bearing in mind that W_L is a normal subgroup of W_K, if $\alpha, \beta \in W_L^*$ and if $\gamma \in W_K$, then

$$\gamma\alpha\beta\alpha^{-1}\beta^{-1}\gamma^{-1} = (\gamma\alpha\gamma^{-1})(\gamma\beta\gamma^{-1})(\gamma\alpha^{-1}\gamma^{-1})(\gamma\beta^{-1}\gamma^{-1}).]$$

There is an exact sequence

$$1 \to W_L/W_L^* \to W_K/W_L^* \to (W_K/W_L^*)/(W_L/W_L^*) \to 1$$

or still, there is an exact sequence

$$1 \to W_L/W_L^* \to W_K/W_L^* \to W_K/W_L \to 1.$$

<u>22:</u> NOTATION Put

$$W(L,K) = W_K/W_L^*.$$

<u>23:</u> SCHOLIUM There is an exact sequence

$$1 \to W_L^{ab} \to W(L,K) \to W_K/W_L \to 1$$

and a diagram

$$\begin{array}{ccccc} & W_L^{ab} & \longrightarrow & W(L,K) & \longrightarrow & W_K/W_L & \\ & \uparrow \scriptstyle{rec_L} & & & & \downarrow \scriptstyle{\approx} & \\ 1 \longrightarrow & L^\times & & & & \mathrm{Gal}(L/K) & \to 1. \end{array}$$

<u>24:</u> NOTATION Given $w \in W_K$, let $||w||$ denote the effect on w of passing

from W_K to $R_{>0}^{\times}$ via the arrows

$$W_K \longrightarrow W_K^{ab} \xrightarrow{rec_K^{-1}} K^{\times} \xrightarrow{mod_K} R_{>0}^{\times}.$$

25: LEMMA $||.||:W_K \to R_{>0}^{\times}$ is a continuous homomorphism and its kernel is I_K.

[Under the arrow

$$W_K \to W_K^{ab},$$

I_K drops to

$$\mathrm{Gal}(K^{ab}/K^{ur}) \subset W_K^{ab}.$$

Consider now the arrow

$$rec_K : K^{\times} \to W_K^{ab}.$$

Then $R^{\times}$ is sent to $\mathrm{Gal}(K^{ab}/K^{ur})$ and a prime element $\pi \in R$ is sent to an element $\tilde{\sigma}_q$ in W_K^{ab} whose image in $W(F_q^{ab}/F_q)$ is σ_q. And

$$W_K^{ab} = \bigcup_{n \in Z} (\tilde{\sigma}_q)^n \, \mathrm{Gal}(K^{ab}/K^{ur}).]$$

26: DEFINITION A <u>representation</u> of W_K is a continuous homomorphism $\rho:W_K \to GL(V)$, where V is a finite dimensional complex vector space.

27: LEMMA A homomorphism $\rho:W_K \to GL(V)$ is continuous per the usual topology on GL(V) iff it is continuous per the discrete topology on GL(V).

[GL(V) has no small subgroups.]

<u>28:</u> SCHOLIUM The kernel of every representation of W_K is trivial on an open subgroup J of I_K. Conversely, if $\rho:W_K \to GL(V)$ is a homomorphism which is trivial on an open subgroup J of I_K, then the inverse image of any subset of GL(V) is a union of cosets of J, hence is open, hence ρ is continuous, so by definition is a representation of W_K.

<u>29:</u> EXAMPLE Suppose that $L \supset K$ is a finite Galois extension of K -- then

$$\begin{aligned} W_L \cap I_K &= G_L \cap W_K \cap I_K \\ &= G_L \cap I_K \end{aligned}$$

is an open subgroup of I_K. But

$$W_K/W_L \approx \mathrm{Gal}(L/K) \quad \text{(cf. \#20)}.$$

Therefore every homomorphism $\mathrm{Gal}(L/K) \to GL(V)$ lifts to a homomorphism $W_K \to GL(V)$ which is trivial on an open subgroup of I_K, hence is a representation of W_K.

<u>30:</u> <u>N.B.</u> Representations of W_K arising in this manner are said to be of <u>Galois type</u>.

<u>31:</u> LEMMA A representation of W_K is of Galois type iff it has finite image.

<u>32:</u> EXAMPLE $||\cdot||$ is a character of W_K but as a representation, is not of Galois type.

<u>33:</u> LEMMA Let $\rho:W_K \to GL(V)$ be a representation -- then the image $\rho(I_K)$ is finite.

PROOF Suppose that J is an open subgroup of I_K on which ρ is trivial. Since I_K is compact and J is open, the quotient I_K/J is finite, thus $\rho(I_K) = \rho(I_K/J)$ is finite.

34: DEFINITION A representation $\rho:W_K \to GL(V)$ is irreducible if $V \neq 0$ and the only ρ-invariant subspaces are 0 and V.

35: THEOREM Given an irreducible representation ρ of W_K, there exists an irreducible representation $\tilde{\rho}$ of W_K and a complex parameter s such that $\rho \approx \tilde{\rho} \otimes ||.||^s$.

36: LEMMA Let $\rho:W_K \to GL(V)$ be a representation -- then V is the sum of its irreducible ρ-invariant subspaces iff every ρ-invariant subspace has a ρ-invariant complement.

37: DEFINITION Let $\rho:W_K \to GL(V)$ be a representation -- then ρ is semisimple if it satisfies either condition of the preceding lemma.

38: N.B. Irreducible representations are semisimple.

39: THEOREM Let $\rho:W_K \to GL(V)$ be a representation -- then the following conditions are equivalent.

1. ρ is semisimple.
2. $\rho(\tilde{\sigma}_q)$ is semisimple.
3. $\rho(w)$ is semisimple $\forall\, w \in W_K$.

§24. *THE WEIL-DELIGNE GROUP*

1: DEFINITION The Weil-Deligne group WD_K is the semidirect product $C \times| W_K$, the multiplication rule being

$$(z_1,w_1)(z_2,w_2) = (z_1 + ||w_1||z_2,w_1w_2).$$

[Note: The identity in WD_K is $(0,e)$ and the inverse of (z,w) is $(-||w||^{-1}z,w^{-1})$:

$$(z,w)(-||w||^{-1}z,w^{-1})$$

$$= (z + ||w||(-||w||^{-1}z),ww^{-1})$$

$$= (z - z,e) = (0,e).]$$

2: N.B. The topology on WD_K is the product topology.

3: DEFINITION A Deligne representation of W_K is a triple (ρ,V,N), where $\rho:W_K \to GL(V)$ is a representation of W_K and $N:V \to V$ is a nilpotent endomorphism of V subject to the relation

$$\rho(w)N\rho(w)^{-1} = ||w||N \quad (w \in W_K).$$

[Note: $N = 0$ is admissible so every representation of W_K is a Deligne representation.]

4: EXAMPLE Take $V = C^n$, hence $GL(V) = GL_n(C)$. Let $e_0,e_1,\ldots,e_{n-1}$ be the usual basis of V. Define ρ by the rule

$$\rho(w)e_i = ||w||^i e_i \quad (w \in W_K,\ 0 \le i \le n-1)$$

and define N by the rule

$$Ne_i = e_{i+1} \quad (0 \le i \le n-2),\ Ne_{n-1} = 0.$$

Then the triple (ρ, V, N) is a Deligne representation of W_K, the <u>n-dimensional special representation</u>, denoted sp(n).

<u>5:</u> DEFINITION A <u>representation</u> of WD_K is a continuous homomorphism $\rho':WD_K \to GL(V)$ whose restriction to $\mathbb{C}$ is complex analytic, where V is a finite dimensional complex vector space.

<u>6:</u> LEMMA Every Deligne representation (ρ, V, N) of W_K gives rise to a representation $\rho':WD_K \to GL(V)$ of WD_K.

PROOF Put

$$\rho'(z,w) = \exp(zN)\rho(w).$$

Then

$$\rho'(z_1,w_1)\rho'(z_2,w_2)$$

$$= \exp(z_1N)\rho(w_1)\exp(z_2N)\rho(w_2)$$

$$= \exp(z_1N)\rho(w_1)\exp(z_2N)\rho(w_1^{-1})\rho(w_1)\rho(w_2)$$

$$= \exp(z_1N)\exp(z_2||w_1||N)\rho(w_1w_2)$$

$$= \exp(z_1N + z_2||w_1||N)\rho(w_1w_2)$$

$$= \exp((z_1 + ||w_1||z_2)N)\rho(w_1w_2)$$

$$= \rho'(z_1 + ||w_1||z_2, w_1w_2)$$

$$= \rho'((z_1,w_1)(z_2,w_2)).$$

[Note: The continuity of ρ' is manifest as is the complex analyticity of its restriction to C.]

One can also go the other way but this is more involved.

<u>7:</u> RAPPEL If $T:V \to V$ is unipotent, then

$$\log T = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} (T - I)^n$$

is nilpotent.

<u>8:</u> SUBLEMMA Let $\rho':WD_K \to GL(V)$ be a representation of WD_K -- then $\forall\, z \neq 0$, $\rho'(z,e)$ is unipotent.

<u>9:</u> SUBLEMMA Let $\rho':WD_K \to GL(V)$ be a representation of WD_K -- then $\forall\, z \neq 0$,

$$\log \rho'(z,e)$$

is nilpotent and

$$(\log \rho'(z,e))/z \quad (z \neq 0)$$

is independent of z.

<u>10:</u> LEMMA Every representation $\rho':WD_K \to GL(V)$ of WD_K gives rise to a Deligne representation (ρ,V,N) of W_K.

PROOF Put

$$\rho = \rho'|\{0\} \times W_K,\ N = \log \rho'(1,e).$$

Then $\forall\ w \in W_{K'}$,

$$\rho(w)N\rho(w)^{-1} = \rho(w)\log\ \rho'(1,e)\rho(w)^{-1}$$

$$= \rho(w)\ \left(\sum_{n\geq 1} \frac{(-1)^{n+1}}{n}\ (\rho'(1,e) - I)^n\right)\rho(w)^{-1}$$

$$= \sum_{n\geq 1} \frac{(-1)^{n+1}}{n}\ (\rho(w)\rho'(1,e)\rho(w)^{-1} - I)^n.$$

And

$$\rho(w)\rho'(1,e)\rho(w)^{-1}$$

$$= \rho'(0,w)\rho'(1,e)\rho'(0,w^{-1})$$

$$= \rho'((0,w)(1,e)(0,w^{-1}))$$

$$= \rho'((||w||,w)(0,w^{-1}))$$

$$= \rho'(||w||,e).$$

Therefore

$$\rho(w)N\rho(w)^{-1}$$

$$= \sum_{n\geq 1} \frac{(-1)^{n+1}}{n}\ (\rho'(||w||,e) - I)^n$$

$$= \log\ \rho'(||w||,e)$$

$$= ||w||(\log\ \rho'(||w||,e))/||w||$$

$$= ||w||\ \log\ \rho'(1,e)$$

$$= ||w||\ N.$$

<u>11:</u> OPERATIONS

- <u>Direct Sum</u>: Let (ρ_1, V_1, N_1), (ρ_2, V_2, N_2) be Deligne representations -- then their direct sum is the triple

$$(\rho_1 \oplus \rho_2, V_1 \oplus V_2, N_1 \oplus N_2).$$

- <u>Tensor Product</u>: Let (ρ_1, V_1, N_1), (ρ_2, V_2, N_2) be Deligne representations -- then their tensor product is the triple

$$(\rho_1 \otimes \rho_2, V_1 \otimes V_2, N_1 \otimes I_2 + I_1 \otimes N_2).$$

- <u>Contragredient</u>: Let (ρ, V, N) be a Deligne representation -- then its contragredient is the triple

$$(\rho^\vee, V^\vee, -N^\vee).$$

[Note: $V^\vee$ is the dual of V and $N^\vee$ is the transpose of N (thus $\forall f \in V^\vee$, $N^\vee(f) = f \circ N$).]

<u>12:</u> REMARK The definitions of $\oplus$, $\otimes$, $\vee$ when transcribed to the "prime picture" are the usual representation-theoretic formalities applied to the group WD_K.

<u>13:</u> <u>N.B.</u> Let

$$\left[\begin{array}{l} (\rho_1, N_1, V_1) \\ (\rho_2, N_2, V_2) \end{array}\right.$$

be Deligne representations of W_K -- then a morphism

$$(\rho_1, N_1, V_1) \rightarrow (\rho_2, N_2, V_2)$$

is a linear map $T:V_1 \to V_2$ such that

$$T\rho_1(w) = \rho_2(w)T \quad (w \in W_K)$$

and $TN_1 = N_2T$.

[Note: If T is a linear isomorphism, then the Deligne representations

$$\begin{bmatrix} (\rho_1,N_1,V_1) \\ (\rho_2,N_2,V_2) \end{bmatrix}$$

are said to be <u>isomorphic</u>.]

<u>14:</u> DEFINITION Suppose that (ρ,V,N) is a Deligne representation of W_K -- then a subspace $V_0 \subset V$ is an <u>invariant subspace</u> if it is invariant under ρ and N.

<u>15:</u> LEMMA The kernel of N is an invariant subspace.

PROOF If $Nv = 0$, then $\forall\ w \in W_K$,

$$N\rho(w)v = ||w^{-1}||\rho(w)Nv = 0.$$

<u>16:</u> DEFINITION A Deligne representation (ρ,V,N) of W_K is <u>indecomposable</u> if V cannot be written as a direct sum of proper invariant subspaces.

<u>17:</u> EXAMPLE Consider sp(n) -- then it is indecomposable.

[If $C^n = S \oplus T$ was a nontrivial decomposition into proper invariant subspaces, then both $\begin{bmatrix} S \cap \text{Ker } N \\ T \cap \text{Ker } N \end{bmatrix}$ would be nontrivial.]

<u>18:</u> DEFINITION A Deligne representation (ρ,V,N) of W_K is <u>semisimple</u> if ρ is semisimple (cf. §23, #37).

<u>19:</u> EXAMPLE Consider sp(n) -- then it is semisimple.

<u>20:</u> LEMMA Let π be an irreducible representation of W_K -- then $sp(n) \otimes \pi$ is semisimple and indecomposable.

[Note: Recall that π is identified with $(\pi,0)$.]

<u>21:</u> THEOREM Every semisimple indecomposable Deligne representation of W_K is equivalent to a Deligne representation of the form $sp(n) \otimes \pi$, where π is an irreducible representation of W_K and n is a positive integer.

<u>22:</u> THEOREM Let (ρ,N,V) be a semisimple Deligne representation of W_K -- then there is a decomposition

$$(\rho,V,N) = \bigoplus_{i=1}^{s} sp(n_i) \otimes \pi_i,$$

where π_i is an irreducible representation of W_K and n_i is a positive integer. Furthermore, if

$$(\rho,V,N) = \bigoplus_{j=1}^{t} sp(n_j') \otimes \pi_j'$$

is another such decomposition, then $s = t$ and after a renumbering of the summands, $\pi_i \approx \pi_i'$ and $n_i = n_i'$.

APPENDIX

Instead of working with

$$WD_K = \mathbf{C} \rtimes W_K,$$

some authorities work with

$$SL(2,C) \times W_K,$$

the rationale for this being that the semisimple representations of the two groups are the "same".

Given $w \in W_K$, let

$$h_w = \begin{bmatrix} ||w||^{1/2} & 0 \\ 0 & ||w||^{-1/2} \end{bmatrix}$$

and identify $z \in C$ with

$$\begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}.$$

Then

$$h_w \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix} h_w^{-1} = \begin{bmatrix} 1 & ||w||z \\ 0 & 1 \end{bmatrix}.$$

But conjugation by h_w is an automorphism of $SL(2,C)$, thus one can form the semi-direct product $SL(2,C) \rtimes W_K$, the multiplication rule being

$$(X_1,w_1)(X_2,w_2) = (X_1 h_{w_1} X_2 h_{w_1}^{-1}, w_1 w_2).$$

LEMMA The arrow

$$(X,w) \to (Xh_w,w)$$

from

$$SL(2,C) \times| W_K \text{ to } SL(2,C) \times W_K$$

is an isomorphism of groups.

DEFINITION A <u>representation</u> of $SL(2,C) \times W_K$ is a continuous homomorphism $\rho: SL(2,C) \times W_K \to GL(V)$ (V a finite dimensional complex vector space) such that the restriction of ρ to $SL(2,C)$ is complex analytic.

<u>N.B.</u> ρ is semisimple iff its restriction to W_K is semisimple.

[The restriction of ρ to $SL(2,C)$ is necessarily semisimple.]

The finite dimensional irreducible representations of $SL(2,C)$ are parameterized by the positive integers:

$$n \longleftrightarrow \text{sym}(n), \ \dim \text{sym}(n) = n.$$

THEOREM The isomorphism classes of semisimple Deligne representations of W_K are in a 1-to-1 correspondence with the isomorphism classes of semisimple representations of $SL(2,C) \times W_K$.

To explicate matters, start with a semisimple indecomposable Deligne representation of W_K, say $sp(n) \otimes \pi$, and assign to it the external tensor product $\text{sym}(n) \boxtimes \pi$, hence in general

$$\bigoplus_{i=1}^{s} sp(n_i) \otimes \pi_i \to \bigoplus_{i=1}^{s} \text{sym}(n_i) \boxtimes \pi_i.$$