

Local and Global Analysis

Garth Warner
Department of Mathematics
University of Washington

ACKNOWLEDGEMENTS

Many thanks to Judith Clare Salzer for typing the manuscript on an IBM Selectric.

Recently David Clark converted the typewritten manuscript to AMS-TeX. This was a monumental task and in so doing he made a number of constructive and useful suggestions which serve to enhance the exposition. His careful scrutiny of the manuscript has been invaluable.

DEDICATION

This article is dedicated to the memory of Paul Sally.

CONTENTS

- §1. ABSOLUTE VALUES
- §2. TOPOLOGICAL FIELDS
- §3. COMPLETIONS
- §4. p -ADIC STRUCTURE THEORY
- §5. LOCAL FIELDS
- §6. HAAR MEASURE
- §7. HARMONIC ANALYSIS
- §8. ADDITIVE p -ADIC CHARACTER THEORY
- §9. MULTIPLICATIVE p -ADIC CHARACTER THEORY
- §10. TEST FUNCTIONS
- §11. LOCAL ZETA FUNCTIONS: \mathbb{R}^\times OR \mathbb{C}^\times
- §12. LOCAL ZETA FUNCTIONS: \mathbb{Q}_p^\times
- §13. RESTRICTED PRODUCTS
- §14. ADELES AND IDELES

- §15. GLOBAL ANALYSIS
- §16. FUNCTIONAL EQUATIONS
- §17. GLOBAL ZETA FUNCTIONS
- §18. LOCAL ZETA FUNCTIONS (BIS)
- §19. L-FUNCTIONS
- §20. FINITE CLASS FIELD THEORY
- §21. LOCAL CLASS FIELD THEORY
- §22. WEIL GROUPS: THE ARCHIMEDEAN CASE
- §23. WEIL GROUPS: THE NON-ARCHIMEDEAN CASE
- §24. THE WEIL-DELIGNE GROUP

APPENDIX A: TOPICS IN TOPOLOGY

APPENDIX B: TOPICS IN ALGEBRA

APPENDIX C: TOPICS IN GALOIS THEORY

REFERENCES

PREFACE

The objective of this article 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.

§1. ABSOLUTE VALUES

1: DEFINITION Let \mathbb{F} be a field –then an absolute value (a.k.a. a valuation of order 1) is a function

$$|\cdot| : \mathbb{F} \rightarrow \mathbb{R}_{\geq 0}$$

satisfying the following conditions.

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

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

AV-3 $\exists M > 0:$

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

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

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

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

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

$$|1| = 1.$$

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

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

$$\implies |a| = 1.$$

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 $n \mid r$, 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 \mathbb{F}_q is trivial.

[In fact, \mathbb{F}_q^\times is cyclic of order $q - 1$.]

9: DEFINITION Two absolute values $|\cdot|_1$, and $|\cdot|_2$ on a field \mathbb{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 $|\cdot|$ satisfies the triangle inequality if

$$|a + b| \leq |a| + |b|.$$

13: LEMMA Suppose given a function $|\cdot| : \mathbb{F} \rightarrow \mathbb{R}_{\geq 0}$ satisfying AV-1 and AV-2, –then AV-3 holds with $M \leq 2$ iff the triangle inequality obtains.

PROOF Obviously, if

$$|a + b| \leq |a| + |b|,$$

then

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

In the other direction, by induction on m ,

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

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

$$\begin{aligned} \left| \sum_{k=1}^n a_k \right| &\leq M \sup \left(\left| \sum_{k=1}^{2^{m-1}} a_k \right|, \left| \sum_{k=2^{m-1}+1}^{2^m} a_k \right| \right) \\ &\leq 2 \sup \left(\left| \sum_{k=1}^{2^{m-1}} a_k \right|, \left| \sum_{k=2^{m-1}+1}^{2^{m-1}+2^{m-1}} a_k \right| \right) \\ &\leq 2 \sup \left(2^{m-1} \sup_{k \leq 2^{m-1}} |a_k|, 2^{m-1} \sup_{k > 2^{m-1}} |a_k| \right) \\ &\leq 2 \cdot 2^{m-1} \sup_{1 \leq k \leq n} |a_k| \\ &\leq 2 \cdot n \cdot \sup_{1 \leq k \leq n} |a_k|. \end{aligned}$$

I.e.

$$\begin{aligned} \left| \sum_{k=1}^n a_k \right| &\leq 2n \sup_{1 \leq k \leq n} |a_k| \\ &\leq 2n \sum_{k=1}^n |a_k|. \end{aligned}$$

In particular,

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

Finally,

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

\Rightarrow

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

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

15: DEFINITION A place of \mathbb{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 $|\cdot|$ 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 $|\cdot|$ is non-archimedean and let $|b| < |a|$ –then

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

PROOF

$$\begin{aligned} |a| &= |(a + b) - b| \leq \sup(|a + b|, |b|) \\ &= |a + b| \end{aligned}$$

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

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

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

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

where $p \nmid m$, $p \nmid n$, and then define the p -adic absolute value $|\cdot|_p$ 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

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

\implies

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

As for AV-3, $|\cdot|_p$ satisfies the ultrametric inequality. To establish this, assume without loss

of generality that $k \leq \ell$ and write

$$\begin{aligned} x + y &= p^k \left(\frac{m}{n} + p^{\ell-k} \frac{u}{v} \right) \\ &= p^k \frac{mv + p^{\ell-k} nu}{nv}. \end{aligned}$$

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

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

is coprime to p (otherwise,

$$\begin{aligned} mv &= p^r N - p^{\ell-k} nu \quad (r \geq 1) \\ &= p(p^{r-1} N - p^{\ell-k-1} nu) \end{aligned}$$

$$\implies p | mv)$$

\implies

$$\begin{aligned} |x + y|_p &= p^{-k} \\ &= |x|_p \\ &= \sup(|x|_p, |y|_p), \end{aligned}$$

since

$$\begin{aligned} \ell - k > 0 &\implies p^{-\ell} < p^{-k} \\ &\implies |y|_p < |x|_p. \end{aligned}$$

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

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

\implies

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

\implies

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

And

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

\implies

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

20: REMARK It can be shown that every nontrivial absolute value on \mathbb{Q} is equivalent to a $|\cdot|_p$ for some p or to $|\cdot|_\infty$.

21: LEMMA $\forall x \in \mathbb{Q}^\times$,

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

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

PROOF Write

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

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

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

\implies

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

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

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

$$|p_1|_{p_1} = p_1^{-1} \implies |p_1^n|_{p_1} = p_1^{-n} \rightarrow 0.$$

Meanwhile,

$$\begin{aligned} |p_1|_{p_2} &= |p_2^0 p_1|_{p_2} = p_2^{-0} = 1 \\ \implies |p_1^n|_{p_2} &\equiv 1. \end{aligned}$$

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

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

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

§2. TOPOLOGICAL FIELDS

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

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

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

PROOF The nontrivial point is to show that given $V \in \mathcal{B}_a$ (\mathcal{B}_a = the set of open balls centered at 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 $W \subset V$:

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

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

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

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

PROOF This is because $|\cdot|$ is equivalent to an absolute value satisfying the triangle

inequality (cf. §1, #14), the underlying metric being

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

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

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

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

is in force.

6: 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

$$\begin{aligned} d(a, p) &\leq \sup(d(a, b), d(b, p)) \\ &< r \end{aligned}$$

\Rightarrow

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

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

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

PROOF E.g:

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

\implies

$$\begin{aligned} |b - a'| &= |(b - a) + (a - a')| \\ &\leq \sup(|b - a|, |a - a'|) \\ &< r \end{aligned}$$

\implies

$$N_r(a) \subset N_r(a').$$

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

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

PROOF Without loss of generality write $a_1 = \sup_{1 \leq k \leq n} |a_k|$. Then

$$\begin{aligned} |a_1| &= |0 - a_1| \\ &= |a_1 + a_2 + \cdots + a_n - a_1| \\ &= |a_2 + \cdots + a_n| \\ &\leq \sup_{2 \leq k \leq n} |a_k| \\ &= |a_j| \quad (\exists j : 2 \leq j \leq n) \end{aligned}$$

$$\begin{aligned} &\leq \sup_{1 \leq k \leq n} |a_k| \\ &= |a_1|. \end{aligned}$$

§3. COMPLETIONS

Let $|\cdot|$ be an absolute value on a field \mathbb{F} which satisfies the triangle inequality – then per $|\cdot|$, \mathbb{F} might or might not be complete. (Recall, a metric space is complete iff every Cauchy sequence converges.)

1: EXAMPLE Take $\mathbb{F} = \mathbb{R}$ or \mathbb{Q} and let $|\cdot| = |\cdot|_\infty$ – then \mathbb{R} is complete but \mathbb{Q} is not.

2: EXAMPLE Take $\mathbb{F} = \mathbb{Q}$ and let $|\cdot| = |\cdot|_p$ – then \mathbb{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

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

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 \mathbb{Q} , thus

$$\begin{aligned} |x_n^2 + 1|_5 \leq 5^{-n} &\implies |x^2 + 1|_5 = 0 \\ &\implies x^2 + 1 = 0 \dots \end{aligned}$$

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

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

5: RAPPEL Every metric space X has a completion \overline{X} . Moreover, there is an isometry $\phi : X \rightarrow \overline{X}$ such that $\phi(X)$ is dense in \overline{X} and \overline{X} is unique up to isometric isomorphism. (Recall, an isometry is a distance preserving mapping. An isometry is injective, indeed, is a homeomorphism onto its image.)

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

$$\{x_n\} \sim \{y_n\} \Leftrightarrow d(x_n, y_n) \rightarrow 0,$$

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

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

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

Take $X = \mathbb{F}$ and

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

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

$$\begin{aligned} d(x_n + y_n, x_m + y_m) &= |x_n + y_n - x_m - y_m| \\ &= |(x_n - x_m) + (y_n - y_m)| \\ &\leq |x_n - x_m| + |y_n - y_m|. \end{aligned}$$

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

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

Proof: Choose $n \in \mathbb{N}$ such that

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

and

$$|(x_n + y_n) - (x'_n + y'_n)| \leq |x_n - x'_n| + |y_n - y'_n| < \frac{\epsilon}{3}.$$

Then

$$\begin{aligned} |\bar{z} - \bar{z}'| &\leq |\bar{z} - (x_n + y_n)| + |\bar{z}' - (x_n + y_n)| \\ &\leq |\bar{z} - (x_n + y_n)| + |\bar{z}' - (x'_n + y'_n)| + |(x'_n + y'_n) - (x_n + y_n)| < \epsilon \\ &\implies \bar{z} = \bar{z}'. \end{aligned}$$

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

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

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

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

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

PROOF Given $\begin{Bmatrix} \bar{x} \\ \bar{y} \end{Bmatrix} \in \overline{\mathbb{F}}$, choose $\begin{Bmatrix} x_n \\ y_n \end{Bmatrix} \in \mathbb{F}$ such that $\begin{cases} x_n \rightarrow \bar{x}_n \\ y_n \rightarrow \bar{y}_n \end{cases}$ in $\overline{\mathbb{F}}$:

$$\begin{aligned} |\bar{x} - \bar{y}| &\leq |\bar{x} - x_n + x_n - y_n + y_n - \bar{y}| \\ &\leq |\bar{x} - x_n| + |x_n - y_n| + |y_n - \bar{y}|. \\ &\quad \downarrow \qquad \qquad \qquad \downarrow \\ &\quad 0 \qquad \qquad \qquad 0 \end{aligned}$$

And

$$\begin{aligned}
|x_n - y_n| &\leq \sup(|x_n|, |y_n|) \\
&= \frac{1}{2}(|x_n| + |y_n|) + |x_n - y_n| \\
&\rightarrow \frac{1}{2}(|\bar{x}| + |\bar{y}|) + |\bar{x} - \bar{y}| \\
&= \sup(|\bar{x}|, |\bar{y}|).
\end{aligned}$$

9: LEMMA If $|\cdot|$ is non-archimedean per $|\cdot|$, then

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

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

• $|x| < |\bar{x}| :$

$$|\bar{x} - x| = |\bar{x} + (-x)| = |\bar{x}| \quad (\text{c.f. } \S 1, \#18) < |\bar{x}| \dots$$

• $|\bar{x}| < |x| :$

$$|\bar{x} - x| = |-x + \bar{x}| = |-x| \quad (\text{c.f. } \S 1, \#18) = |x| < |\bar{x}| \dots$$

10: EXAMPLE The image of \mathbb{Q}_p under $|\cdot|_p$ is the same as the image of \mathbb{Q} under $|\cdot|_p$, namely

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

Let \mathbb{K} be a field, \mathbb{L}/\mathbb{K} a finite field extension.

11: EXTENSION PRINCIPLE Let $|\cdot|_{\mathbb{K}}$ be a complete absolute value on \mathbb{K} –then there is one and only one extension $|\cdot|_{\mathbb{L}}$ of $|\cdot|_{\mathbb{K}}$ to \mathbb{L} and it is given by

$$|x|_{\mathbb{L}} = |N_{\mathbb{L}/\mathbb{K}}(x)|_{\mathbb{K}}^{1/n},$$

where $n = [\mathbb{L} : \mathbb{K}]$. In addition, \mathbb{L} is complete with respect to $|\cdot|_{\mathbb{L}}$.

[Note: $|\cdot|_{\mathbb{L}}$ is non-archimedean if $|\cdot|_{\mathbb{K}}$ is non-archimedean.]

12: SCHOLIUM There is a unique extension of $|\cdot|_{\mathbb{K}}$ to the algebraic closure \mathbb{K}^{cl} of \mathbb{K} .

[Note: It is not true in general that \mathbb{K}^{cl} is complete.]

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

$$|\cdot|_{\sigma}|_{\mathbb{K}} = |\cdot|_{\mathbb{K}},$$

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

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

\implies

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

APPENDIX

1: APPROXIMATION PRINCIPLE Let $|\cdot|_1, \dots, |\cdot|_N$ be pairwise inequivalent non-trivial absolute values on \mathbb{F} . Fix elements a_1, \dots, a_N in \mathbb{F} –then $\forall \epsilon > 0, \exists a_{\epsilon} \in \mathbb{F}$:

$$|a_{\epsilon} - a_k|_k < \epsilon \quad (k = 1, \dots, N).$$

Let $\overline{\mathbb{F}}_1, \dots, \overline{\mathbb{F}}_N$ be the associated completions and let

$$\Delta : \mathbb{F} \rightarrow \prod_{k=1}^N \overline{\mathbb{F}}_k$$

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

[Fix $\epsilon > 0$ and elements $\bar{a}_1, \dots, \bar{a}_N$ in $\overline{\mathbb{F}}_1, \dots, \overline{\mathbb{F}}_N$ respectively –then there exist elements $a_k \in \mathbb{F}$:

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

Choose $a_\epsilon \in \mathbb{F}$:

$$|a_\epsilon - \bar{a}_k| < \epsilon \quad (k = 1, \dots, N).$$

Then

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

2: N.B. The product $\prod_{k=1}^N \overline{\mathbb{F}}_k$ carries the product topology and the prescription

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

metrizes the product topology. Therefore

$$\begin{aligned} d((a_\epsilon, \dots, a_\epsilon), (\bar{a}_1, \dots, \bar{a}_N)) &= \sup_{1 \leq k \leq N} d_k(a_\epsilon, \bar{a}_k) \\ &= \sup_{1 \leq k \leq N} |a_\epsilon - \bar{a}_k|_k \\ &< 2\epsilon. \end{aligned}$$

§4. p-ADIC STRUCTURE THEORY

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

1: NOTATION Let

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

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

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

3: N.B. It follows from this that \mathbb{Q}_p is uncountable, so \mathbb{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:

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

where the $a_n \in \mathcal{A}$.

5: EXAMPLE

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

6: EXAMPLE Take $p = 3$ –then

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

\Rightarrow

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

7: LEMMA

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

PROOF

$$\begin{aligned} & 1 + (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \dots \\ &= p + (p-1)p + (p-1)p^2 + (p-1)p^3 + \dots \\ &= p^2 + (p-1)p^2 + (p-1)p^3 + \dots \\ &= p^3 + (p-1)p^3 + \dots \\ &= 0. \end{aligned}$$

8: APPLICATION

$$\begin{aligned} -N &= (-1) \cdot N \\ &= \left(\sum_{i=0}^{\infty} (p-1)p^i \right) (a_0 + a_1p + \dots + a_np^n) \\ &= \dots \end{aligned}$$

9: LEMMA A p -adic series

$$\sum_{n=0}^{\infty} x_n \quad (x_n \in \mathbb{Q}_p)$$

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

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

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

Let

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

Then

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

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

10: EXAMPLE The p -adic series

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

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

11: EXAMPLE The p -adic series

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

is convergent.

[Note that

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

where

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

12: EXAMPLE The p -adic series

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

is convergent (to -1).

13: LEMMA \mathbb{Q}_p is a topological field (cf. § 2, #5).

14: LEMMA \mathbb{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).

15: NOTATION

- $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$
- $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$
- $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}$

16: LEMMA \mathbb{Z}_p is a commutative ring with unit (the ring of p -adic integers,)
in fact \mathbb{Z}_p is an integral domain.

17: LEMMA $p\mathbb{Z}_p$ is an ideal in \mathbb{Z}_p , in fact $p\mathbb{Z}_p$ is a maximal ideal in \mathbb{Z}_p , in fact $p\mathbb{Z}_p$ is the unique maximal ideal in \mathbb{Z}_p , hence \mathbb{Z}_p is a local ring.

18: LEMMA \mathbb{Z}_p^\times is a group under multiplication, in fact \mathbb{Z}_p^\times is the set of p -adic units in \mathbb{Z}_p , i.e., the set of elements in \mathbb{Z}_p that have a multiplicative inverse in \mathbb{Z}_p .

Obviously,

$$\mathbb{Z}_p = \mathbb{Z}_p^\times \amalg (\mathbb{Z}_p - \mathbb{Z}_p^\times)$$

or still,

$$\mathbb{Z}_p = \mathbb{Z}_p^\times \amalg p\mathbb{Z}_p.$$

19: LEMMA

$$\mathbb{Z}_p = \bigcup_{0 \leq k \leq p-1} (k + p\mathbb{Z}_p).$$

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

$$x + p\mathbb{Z}_p = q + p\mathbb{Z}_p.$$

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

$$\begin{aligned} \left| k - \frac{a}{b} \right|_p < 1 &\implies k + p\mathbb{Z}_p = q + p\mathbb{Z}_p = x + p\mathbb{Z}_p \\ &\implies x \in k + p\mathbb{Z}_p. \end{aligned}$$

Consider a p -adic series

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

Then

$$\begin{aligned} \left| \sum_{n=0}^{\infty} a_n p^n \right|_p &\leq \sup_n |a_n p^n|_p \\ &\leq \sup_n |p^n|_p \\ &\leq 1, \end{aligned}$$

so it converges to an element x of \mathbb{Z}_p . Conversely:

20: THEOREM Every $x \in \mathbb{Z}_p$ admits a unique representation

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

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

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

where $a_n \in \mathcal{A}$ and $x_{N+1} \in \mathbb{Z}_p$. But

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

21: APPLICATION \mathbb{Z} is dense in \mathbb{Z}_p .

22: EXAMPLE Let $x \in \mathbb{Z}_p$ —then $\forall n \in \mathbb{N}$,

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

23: LEMMA

$$\mathbb{Z}_p^\times = \bigcup_{1 \leq k \leq p-1} (k + p\mathbb{Z}_p).$$

Consequently, if

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

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

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

24: THEOREM An element

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

in \mathbb{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 $a_0 b_0 \equiv 1 \pmod{p}$. Proceed from here by recursion and assume that b_1, \dots, b_M between 0 and $p-1$ have already been found subject to

$$x \left(\sum_{0 \leq m \leq M} b_m p^m \right) \equiv 1 \pmod{p^{M+1}}.$$

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

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

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

25: EXAMPLE $1-p$ is invertible in \mathbb{Z}_p but p is not invertible in \mathbb{Z}_p .

26: REMARK The arrow

$$\epsilon : \mathbb{Z}_p \rightarrow \mathbb{Z}/p\mathbb{Z}$$

that sends

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

to $a_0 \bmod p$ 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, \dots be an infinite sequence in \mathbb{Z}_p . Choose $a_0 \in \mathcal{A}$ such that $a_0 + p\mathbb{Z}_p$ contains infinitely many of the x_n . Write

$$\begin{aligned} a_0 + p\mathbb{Z}_p &= a_0 + p\left(\bigcup_{a \in \mathcal{A}} (a + p\mathbb{Z}_p)\right) \\ &= a_0 + \bigcup_{a \in \mathcal{A}} (ap + p^2\mathbb{Z}_p) \\ &= \bigcup_{a \in \mathcal{A}} (a_0 + ap + p^2\mathbb{Z}_p). \end{aligned}$$

Choose $a_1 \in \mathcal{A}$ such that $a_0 + a_1p + p^2\mathbb{Z}_p$ contains infinitely many of the x_n . Etc. The

construction thus produces a descending sequence of cosets of the form

$$A_j + p^j \mathbb{Z}_p,$$

each of which contains infinitely many of the x_n . But

$$\begin{aligned} A_j + p^j \mathbb{Z}_p &= \{x \in \mathbb{Z}_p : |x - A_j|_p \leq p^{-j}\} \\ &\equiv B_{p^{-j}}(A_j), \end{aligned}$$

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

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

Finally choose

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

Then

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

28: APPLICATION \mathbb{Q}_p is locally compact.

[Since \mathbb{Q}_p is Hausdorff, it is enough to prove that each $x \in \mathbb{Q}_p$ has a compact neighborhood. But \mathbb{Z}_p is a compact neighborhood of 0, so $x + \mathbb{Z}_p$ is a compact neighborhood of x.]

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

$$\mathbb{Q}_p = \bigcup_{n=0}^{\infty} p^{-n}\mathbb{Z}_p.$$

Accordingly, \mathbb{Q}_p is σ -compact (the $p^{-n}\mathbb{Z}_p$ being compact).

29: SCHOLIUM A subset of \mathbb{Q}_p is compact iff it is closed and bounded.

30: LEMMA Given $n, m \in \mathbb{Z}$,

$$p^n \mathbb{Z}_p \subset p^m \mathbb{Z}_p \Leftrightarrow m \leq n.$$

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

32: LEMMA For every $x_0 \in \mathbb{Q}_p$ and $r > 0$, there is an integer n such that

$$\begin{aligned} N_r(x_0) &= \{x \in \mathbb{Q}_p : |x - x_0|_p < r\} \\ &= N_{p^{-n}}(x_0) \\ &= \{x \in \mathbb{Q}_p : |x - x_0|_p < p^{-n}\} \\ &= x_0 + p^{n+1} \mathbb{Z}_p \end{aligned}$$

33: SCHOLIUM The basic open sets in \mathbb{Q}_p are the cosets of some power of $p\mathbb{Z}_p$.

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

34: LEMMA

$$p^n \mathbb{Z}_p^\times = p^n \mathbb{Z}_p - p^{n+1} \mathbb{Z}_p.$$

35: DEFINITION The $p^n \mathbb{Z}_p^\times$ are called shells.

36: N.B. There is a disjoint decomposition

$$\mathbb{Q}_p^\times = \bigcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p^\times,$$

where

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

[Note: For the record, \mathbb{Q}_p^\times is totally disconnected and, being open in \mathbb{Q}_p , is Hausdorff and locally compact. Moreover, \mathbb{Z}_p^\times is open-closed (indeed, open-compact).]

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

$$\mathbb{Q}_p^\times \approx \langle p \rangle \times \mathbb{Z}_p^\times$$

or still,

$$\mathbb{Q}_p^\times \approx \mathbb{Z} \times \mathbb{Z}_p^\times.$$

37: NOTATION For $n = 1, 2, \dots$, put

$$U_{p,n} = 1 + p^n \mathbb{Z}_p.$$

[Note:

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

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

$$\mathbb{Z}_p^\times \supset U_{p,1} \supset U_{p,2} \supset \dots$$

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

39: DEFINITION $U_{p,1} = 1 + p\mathbb{Z}_p$ is called the group of principal units of \mathbb{Z}_p .

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

A generator of \mathbb{F}_p^\times can be "lifted" to \mathbb{Z}_p^\times .

41: THEOREM There exists a $\zeta \in \mathbb{Z}_p^\times$ 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 $x \in \mathbb{Z}_p$ 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 $\zeta \in U_{p,1}$:

$$\zeta = 1 + pu \ (u \in \mathbb{Z}_p) \implies (1 + pu)^{p-1} = 1 \implies u = 0,$$

a contradiction.]

43: SCHOLIUM \mathbb{Z}_p^\times can be written as a disjoint union

$$\mathbb{Z}_p^\times = U_{p,1} \cup \zeta U_{p,1} \cup \zeta^2 U_{p,1} \cup \dots \cup \zeta^{p-2} U_{p,1}.$$

Therefore

$$\mathbb{Q}_p^\times \approx \mathbb{Z} \times \mathbb{Z}_p^\times \approx \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times U_{p,1}.$$

44: LEMMA Any root of unity in \mathbb{Q}_p lies in \mathbb{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 $x \in \mathbb{Z}_p^\times$.

The roots of unity in \mathbb{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 \mathbb{Z}_p^\times generated by ζ , then G_{p-1} consists of $(p-1)^{st}$ roots of unity, hence $G_{p-1} \subset T_p$.

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

46: APPLICATION If p_1, p_2 are distinct primes, then \mathbb{Q}_{p_1} is not field isomorphic to \mathbb{Q}_{p_2} .

47: REMARK \mathbb{Q}_p is not a field isomorphic to \mathbb{R} .

[\mathbb{Q}_p has algebraic extensions of arbitrarily large linear degree which is not the case of \mathbb{R} (cf. §5, #26).]

48: LEMMA Let $x \in \mathbb{Q}_p^\times$ —then $x \in \mathbb{Z}_p^\times$ iff x^{p-1} possesses n^{th} roots for infinitely many n .

PROOF If $x \in \mathbb{Z}_p^\times$ and if n is not a multiple of p , then one can use Hensel's lemma to infer the existence of a $y_n \in \mathbb{Z}_p$ 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.

49: APPLICATION Let $\phi : \mathbb{Q}_p \rightarrow \mathbb{Q}_p$ be a field automorphism —then ϕ preserves units.

[In fact, if $x \in \mathbb{Z}_p^\times$, then

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

50: THEOREM The only field automorphism ϕ of \mathbb{Q}_p is the identity.

PROOF Given $x \in \mathbb{Q}_p^\times$, 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

$$v(\phi(x)) = v(x) \quad (\phi(u(x)) \in \mathbb{Z}_p^\times).$$

Therefore ϕ is continuous. Since \mathbb{Q} is dense in \mathbb{Q}_p , it follows that $\phi = id_{\mathbb{Q}_p}$.

[Note:

$$\begin{aligned}
x_k \rightarrow 0 &\implies |x_k|_p \rightarrow 0 \\
&\implies p^{-v(x_k)} \rightarrow 0 \\
&\implies p^{-v(\phi(x_k))} \rightarrow 0 \\
&\implies |\phi(x_k)|_p \rightarrow 0 \\
&\implies \phi(x_k) \rightarrow 0.]
\end{aligned}$$

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

$$\mathbb{Q}_p^\times \approx \mathbb{Z} \times \mathbb{Z}_p^\times \approx \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times U_{p,1}.$$

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

52: APPLICATION If $p \neq 2$, then

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

but if $p = 2$, then

$$(\mathbb{Q}_p^\times)^2 \approx 2\mathbb{Z} \times U_{2,3}.$$

53: THEOREM If $p \neq 2$, then

$$[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2] = 4$$

but if $p = 2$, then

$$[\mathbb{Q}_2^\times : (\mathbb{Q}_2^\times)^2] = 8.$$

54: REMARK If $p \neq 2$, then

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

but if $p = 2$, then

$$\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

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

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

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

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

And

$$\begin{cases} 2k - 1 = p - 1 \implies 2k = p \implies p \text{ even } \dots \\ 2k - 1 = 2p - 2 \implies 2k - 1 = 2(p - 1) \implies 2k - 1 \text{ even } \dots \end{cases} .$$

- $p\zeta$ is not a square.

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

$$\begin{aligned} \zeta = p^{2n-1}u^2 &\implies 1 = |\zeta|_p = |p^{2n-1}|_p = p^{1-2n} \\ &\implies 1 - 2n = 0, \end{aligned}$$

an untenable relation.]

56: THEOREM If $p \neq 2$, then up to isomorphism, \mathbb{Q}_p has three quadratic extensions, viz.

$$\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{\zeta}), \mathbb{Q}_p(\sqrt{p\zeta})$$

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

57: REMARK Another choice for the three quadratic extensions of \mathbb{Q}_p when $p \neq 2$ is

$$\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{a}), \mathbb{Q}_p(\sqrt{pa}),$$

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

58: REMARK It can be shown that up to isomorphism, \mathbb{Q}_2 has seven quadratic extensions, viz.

$$\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 5}), \mathbb{Q}_2(\sqrt{\pm 10}).$$

59: EXAMPLE Take $p = 5$ — then $2 \notin (\mathbb{Q}_5^\times)^2$, $3 \notin (\mathbb{Q}_5^\times)^2$, but $6 \in (\mathbb{Q}_5^\times)^2$. And

$$\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\sqrt{3}).$$

[Working within \mathbb{Z}_5^\times , consider the equation $x^2 = 2$ and expand x as usual:

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

Then

$$a_0^2 \equiv 2 \pmod{5}.$$

But the possible values of a_0 are 0, 1, 2, 3, 4, thus the congruence is impossible, so $2 \notin (\mathbb{Q}_5^\times)^2$. Analogously, $3 \notin (\mathbb{Q}_5^\times)^2$. On the other hand, $6 \in (\mathbb{Q}_5^\times)^2$ (by direct verification or Hensel's lemma), hence $6 = \gamma^2$ ($\gamma \in \mathbb{Q}_5$). Finally, to see that

$$\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\sqrt{3}),$$

it need only be shown that $\sqrt{2} = a + b\sqrt{3}$ for certain $a, b \in \mathbb{Q}_5$. 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, $-1 \in (\mathbb{Q}_2^\times)^2$ iff $(p-1)/2$ is even, i.e. iff $p \equiv 1 \pmod{4}$. Accordingly, to start $\sqrt{-1}$ exists in $\mathbb{Q}_5, \mathbb{Q}_{13}, \dots$.

[Note: $\sqrt{-1}$ does not exist in \mathbb{Q}_2 .]

APPENDIX

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

1: THEOREM \mathbb{Q}_p^{cl} is not second category.

2: APPLICATION The metric space \mathbb{Q}_p^{cl} is not complete.

3: APPLICATION The Hausdorff space \mathbb{Q}_p^{cl} is not locally compact (cf. §5, #5).

4: NOTATION Put

$$\mathbb{C}_p = \overline{(\mathbb{Q}_p^{cl})},$$

the completion of \mathbb{Q}_p^{cl} per $|\cdot|_p$.

5: THEOREM \mathbb{C}_p is algebraically closed.

6: N.B. The metric space \mathbb{C}_p is separable but the Hausdorff space \mathbb{C}_p is not locally compact (cf. §5, #5).

§5. LOCAL FIELDS

Let \mathbb{K} be a field of characteristic 0 equipped with a non-archimedean absolute value $|\cdot|$.

1: NOTATION Let

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

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

3: NOTATION Let

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

4: LEMMA P is a maximal ideal.

Therefore the quotient R/P is a field, the residue field of \mathbb{K} .

5: THEOREM \mathbb{K} is locally compact iff the following conditions are satisfied.

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

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

7: EXAMPLE \mathbb{R} and \mathbb{C} are local fields.

8: EXAMPLE \mathbb{Q}_p is a local field.

Assume that \mathbb{K} is a non-archimedean local field.

9: LEMMA R is compact.

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

$$|\mathbb{K}^\times| = |\pi|^\mathbb{Z}, \quad \text{where } 0 < |\pi| < 1.$$

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

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

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

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 \mathbb{K} is a finite extension of \mathbb{Q}_p for some p .

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

There is also a converse.

14: THEOREM Let \mathbb{K} be a finite extension of \mathbb{Q}_p —then \mathbb{K} is a local field.

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

$$\mathbb{Z}_p/p\mathbb{Z}_p \rightarrow R/P$$

is injective and

$$[R/P : \mathbb{F}_p] \leq [\mathbb{K} : \mathbb{Q}_p] < \infty.$$

[Details: To begin with,

$$\mathbb{Q}_p \cap P = p\mathbb{Z}_p,$$

thus the inclusion $\mathbb{Z}_p \rightarrow R$ induces an injection

$$\mathbb{Z}_p/p\mathbb{Z}_p \rightarrow R/P.$$

Put now $n = [\mathbb{K} : \mathbb{Q}_p]$ and let $A_1, \dots, A_{n+1} \in R$ —then the claim is that the residue classes $\bar{A}_1, \dots, \bar{A}_{n+1} \in R/P$ are linearly dependent over $\mathbb{Z}_p/p\mathbb{Z}_p$. In any event, there are elements $x_1, \dots, x_{n+1} \in \mathbb{Q}_p$ 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 $x_i \in \mathbb{Z}_p$ and not every residue class $\bar{x}_i \in \mathbb{Z}_p/p\mathbb{Z}_p$ 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 \mathbb{Q}_p ($\exists p$).

Let \mathbb{K}/\mathbb{Q}_p be a finite extension of degree n —then the canonical absolute value on \mathbb{K} is given by

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

[Note: The normalized absolute value on \mathbb{K} is given by

$$|a|_{\mathbb{K}} = |a|_p^n.$$

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

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

17: DEFINITION The ramification index of \mathbb{K} over \mathbb{Q}_p is the positive integer

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

I.e.,

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

Therefore

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

[Consider \mathbb{Z} and $e\mathbb{Z}$ —then the generator 1 of \mathbb{Z} is related to the generator e of $e\mathbb{Z}$ 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

$$\begin{aligned} |p|_p &= |\pi'|_p^e \\ &= (|\pi|_p^{v(\pi)})^e \\ &= (|\pi|_p^e)^{v(\pi)} \\ &= |p|_p^{v(\pi)}, \end{aligned}$$

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

19: NOTATION

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

so

$$f = [R/P : \mathbb{F}_p],$$

the residual index of \mathbb{K} over \mathbb{Q}_p .

20: THEOREM Let \mathbb{K}/\mathbb{Q}_p be a finite extension of degree n —then

$$n = [\mathbb{K} : \mathbb{Q}_p] = ef.$$

21: APPLICATION

$$\begin{aligned} |\pi|_{\mathbb{K}} &= |\pi|_p^n \\ &= |p|_p^{n/e} \\ &= \left(\frac{1}{p}\right)^{n/e} \\ &= \left(\frac{1}{p}\right)^f \\ &= \frac{1}{p^f} \\ &= \frac{1}{q}. \end{aligned}$$

View p as an element of \mathbb{K} :

- $|p|_p = |N_{\mathbb{K}/\mathbb{Q}_p}(p)|_p^{1/n} = |p^n|_p^{1/n} = |p|_p$.
- $|p|_{\mathbb{K}} = |N_{\mathbb{K}/\mathbb{Q}_p}(p)|_p = |p^n|_p = \frac{1}{p^n} = \frac{1}{p^{ef}} = \left(\frac{1}{p^f}\right)^e = q^{-e}$.

22: DEFINITION A finite extension \mathbb{K}/\mathbb{Q}_p is

- unramified if $e = 1$
- ramified if $f = 1$.

Take the case $\mathbb{K} = \mathbb{Q}_p$ –then $e = 1$, hence \mathbb{K} is unramified, and $f = 1$, hence \mathbb{K} is ramified.

23: LEMMA If \mathbb{K}/\mathbb{Q}_p is is unramified, then p is a prime element.

24: THEOREM $\forall n = 1, 2, \dots$, there is up to isomorphism one unramified extension \mathbb{K}/\mathbb{Q}_p of degree n .

Let \mathbb{K}/\mathbb{Q}_p be a finite extension.

25: LEMMA The group M^\times of roots of unity of order prime to p in \mathbb{K} is cyclic of order

$$p^f - 1 \quad (= q - 1).$$

26: LEMMA The set $M = M^\times \cup \{0\}$ is a set of coset representatives for R/P . Therefore (cf. §4, #43)

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

27: NOTATION Let

$$\mathbb{K}_{ur} = \mathbb{Q}_p(M^\times).$$

28: LEMMA \mathbb{K}_{ur} is the maximal unramified extension of \mathbb{Q}_p in \mathbb{K} and

$$[\mathbb{K}_{ur} : \mathbb{Q}_p] = f.$$

29: REMARK The maximal unramified extension $(\mathbb{Q}_p^{\text{cl}})_{ur} \subset \mathbb{Q}_p^{\text{cl}}$ 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 $\tau \in \mathbb{Q}_p^\times - (\mathbb{Q}_p^\times)^2$, and form the quadratic extension

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

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

$$\begin{aligned} |x + y\sqrt{\tau}|_p &= \left| N_{\mathbb{Q}_p(\sqrt{\tau})/\mathbb{Q}_p}(x + y\sqrt{\tau}) \right|_p^{1/2} \\ &= |x^2 - \tau y^2|_p^{1/2}. \end{aligned}$$

31: CLASSIFICATION Consider the three possibilities

$$\mathbb{Q}_p(\sqrt{p}), \quad \mathbb{Q}_p(\sqrt{\tau}), \quad \mathbb{Q}_p(\sqrt{p\tau}),$$

thus here $ef = 2$.

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

[Note that

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

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

[Note that

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

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

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

[There is up to isomorphism one unramified extension \mathbb{K} of \mathbb{Q}_p of degree 2 (cf. #24)].

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

The preceding developments are absolute, i.e., based at \mathbb{Q}_p . It is also possible to relativize the theory. Thus let \mathbb{L}/\mathbb{K} , \mathbb{K}/\mathbb{Q}_p be finite extensions. Append subscripts to the various quantities involved:

$$\left\{ \begin{array}{l} R_{\mathbb{K}} \supset P_{\mathbb{K}}, \quad R_{\mathbb{K}}/P_{\mathbb{K}}, \quad e_{\mathbb{K}}, \quad f_{\mathbb{K}}, \quad M_{\mathbb{K}}^{\times} \\ R_{\mathbb{L}} \supset P_{\mathbb{L}}, \quad R_{\mathbb{L}}/P_{\mathbb{L}}, \quad e_{\mathbb{L}}, \quad f_{\mathbb{L}}, \quad M_{\mathbb{L}}^{\times} \end{array} \right. .$$

Introduce

$$\left\{ \begin{array}{l} e(\mathbb{L}/\mathbb{K}) = [|\mathbb{L}^{\times}| : |\mathbb{K}^{\times}|] \\ f(\mathbb{L}/\mathbb{K}) = [R_{\mathbb{L}}/P_{\mathbb{L}} : R_{\mathbb{K}}/P_{\mathbb{K}}] \end{array} \right. .$$

32: LEMMA

$$[\mathbb{L} : \mathbb{K}] = e(\mathbb{L}/\mathbb{K})f(\mathbb{L}/\mathbb{K}).$$

PROOF We have

$$\left\{ \begin{array}{l} [\mathbb{L} : \mathbb{Q}_p] = e_{\mathbb{L}}f_{\mathbb{L}} \\ [\mathbb{K} : \mathbb{Q}_p] = e_{\mathbb{K}}f_{\mathbb{K}} \end{array} \right. \quad (\text{ cf. \#20}).$$

Therefore

$$[\mathbb{L} : \mathbb{K}] = \frac{[\mathbb{L} : \mathbb{Q}_p]}{[\mathbb{K} : \mathbb{Q}_p]} = \frac{e_{\mathbb{L}}f_{\mathbb{L}}}{e_{\mathbb{K}}f_{\mathbb{K}}} = e(\mathbb{L}/\mathbb{K})f(\mathbb{L}/\mathbb{K}).$$

33: THEOREM Let \mathbb{L}/\mathbb{K} , \mathbb{K}/\mathbb{Q}_p be finite extensions –then there exists a unique maximal intermediate extension $\mathbb{K} \subset \mathbb{K}_{ur} \subset \mathbb{L}$ that is unramified over \mathbb{K} .

[In fact,

$$\mathbb{K}_{ur} = \mathbb{K}(M_{\mathbb{L}}^{\times}) \subset \mathbb{L}.]$$

[Note: The extension $\mathbb{L}/\mathbb{K}_{ur}$ 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 $A \subset X$,

$$\mu(A) = \inf_{U \supset A} \mu(U), \quad \text{where } U \subset X \text{ is open.}$$

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

$$\mu(A) = \sup_{K \subset A} \mu(K), \quad \text{where } K \subset X \text{ is compact.}$$

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 for 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 $G = \mathbb{R}$ –then $\mu_{\mathbb{R}} = dx$ ($dx =$ Lebesgue measure) is a Haar measure ($\mu_{\mathbb{R}}([0, 1]) = \int_0^1 dx = 1$).

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

9: EXAMPLE Take $G = \mathbb{Z}$ –then $\mu_{\mathbb{Z}} =$ counting measure is a Haar measure.

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

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

[Note: The function

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

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

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

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

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

is $\equiv 1$, hence when integrated over \mathbb{R}/\mathbb{Z} gives the volume of \mathbb{R}/\mathbb{Z} . On the other hand,

$$\int_{\mathbb{R}} \chi = 1.]$$

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

$$\mu_{\mathbb{K}}(M_a(A)) = \text{mod}_{\mathbb{K}}(a)\mu_{\mathbb{K}}(A)$$

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

$$\int_{\mathbb{K}} f(a^{-1}x) d\mu_{\mathbb{K}}(x) = \text{mod}_{\mathbb{K}}(a) \int_{\mathbb{K}} f(x) d\mu_{\mathbb{K}}(x).$$

[Note: $\text{mod}_{\mathbb{K}}(a)$ is independent of the choice of $\mu_{\mathbb{K}}$.]

Extend $\text{mod}_{\mathbb{K}}$ to all of \mathbb{K} by setting $\text{mod}_{\mathbb{K}}(0)$ equal to 0.

12: LEMMA Let \mathbb{K}, \mathbb{L} be local fields, where \mathbb{L}/\mathbb{K} is a finite field extension —then $\forall x \in \mathbb{L}$,

$$\begin{aligned} \text{mod}_{\mathbb{L}}(x) &= \text{mod}_{\mathbb{K}}(N_{\mathbb{L}/\mathbb{K}}(x)) \\ &\equiv \text{mod}_{\mathbb{K}}(\det(M_x)) \end{aligned}$$

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

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

$$\text{mod}_{\mathbb{R}}(a) = |a|.$$

[$\forall f \in C_c(\mathbb{R})$,

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

14: EXAMPLE Take $\mathbb{K} = \mathbb{C}, \mathbb{L} = \mathbb{C}$ —then $\forall a \in \mathbb{C}$,

$$\begin{aligned} \text{mod}_{\mathbb{C}}(z) &= \text{mod}_{\mathbb{R}}(N_{\mathbb{C}/\mathbb{R}}(z)) \\ &= |z\bar{z}| \\ &= |z|^2. \end{aligned}$$

15: LEMMA

$$\text{mod}_{\mathbb{Q}_p} = |\cdot|_p$$

To prove this we need a preliminary.

16: LEMMA The arrow

$$\epsilon_k : \mathbb{Z}_p \rightarrow \mathbb{Z}/p^k\mathbb{Z}$$

that sends

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

to

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

is a homomorphism of rings. It is surjective with kernel $p^k\mathbb{Z}_p$, so $[\mathbb{Z}_p : p^k\mathbb{Z}_p] = p^k$ (cf. §4, #26), thus there is a disjoint decomposition of \mathbb{Z}_p :

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

Normalize the Haar measure on \mathbb{Q}_p by stipulating that

$$\mu_{\mathbb{Q}_p}(\mathbb{Z}_p) = 1.$$

[Note: In this connection, recall that \mathbb{Z}_p is an open-compact set.]

The claim now is that for every Borel set A ,

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

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 the disjoint union of cosets of the subgroups $p^k\mathbb{Z}_p$ (cf. §4,

#33), hence thanks to translation invariance, it suffices to deal with these alone:

$$\begin{aligned}\mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) &= \text{mod}_{\mathbb{Q}_p}(p^k)\mu_{\mathbb{Q}_p}(\mathbb{Z}_p) \\ &= \text{mod}_{\mathbb{Q}_p}(p^k) \\ &= |p^k|_p.\end{aligned}$$

1. $k \geq 0$:

$$\begin{aligned}1 &= \mu_{\mathbb{Q}_p}(\mathbb{Z}_p) \\ &= \mu_{\mathbb{Q}_p}\left(\bigcup_{j=1}^{p^k}(x_j + p^k\mathbb{Z}_p)\right) \\ &= p^k\mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) \\ \implies \mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) &= p^{-k} \\ &= |p^k|_p.\end{aligned}$$

2. $k < 0$:

$$\begin{aligned}1 &= \mu_{\mathbb{Q}_p}(\mathbb{Z}_p) \\ &= \mu_{\mathbb{Q}_p}(p^{-k}p^k\mathbb{Z}_p) \\ &= \text{mod}_{\mathbb{Q}_p}(p^{-k})\mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) \\ &= |p^{-k}|_p\mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) \\ \implies \mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) &= |p^{-k}|_p^{-1} \\ &= |p^k|_p.\end{aligned}$$

17: SCHOLIUM If \mathbb{K} is a finite field extension of \mathbb{Q}_p , then $\forall a \in \mathbb{K}$,

$$\text{mod}_{\mathbb{K}}(a) = |N_{\mathbb{K}/\mathbb{Q}_p}(a)|_p,$$

the normalized absolute value on \mathbb{K} mentioned in § 5:

$$\text{mod}_{\mathbb{K}}(a) = |a|_{\mathbb{K}} \quad (= |a|_p^n, \quad n = [\mathbb{K} : \mathbb{Q}_p]).$$

18: CONVENTION Integration w.r.t. $\mu_{\mathbb{Q}_p}$ will be denoted by dx :

$$\int_{\mathbb{Q}_p} f(x) d\mu_{\mathbb{Q}_p}(x) = \int_{\mathbb{Q}_p} f(x) dx.$$

[Note: Points are of Haar measure zero:

$$\{0\} = \bigcap_{k=1}^{\infty} p^k \mathbb{Z}_p$$

\implies

$$\begin{aligned} \mu_{\mathbb{Q}_p}(\{0\}) &= \lim_{k \rightarrow \infty} \mu_{\mathbb{Q}_p}(p^k \mathbb{Z}_p) \\ &= \lim_{k \rightarrow \infty} p^{-k} = 0. \end{aligned}$$

19: EXAMPLE

$$\mathbb{Z}_p^\times = \bigcup_{1 \leq k \leq p-1} (k + p\mathbb{Z}_p) \quad (\text{cf. } \S 4, \#23).$$

Therefore

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

20: EXAMPLE

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

21: EXAMPLE Write

$$\mathbb{Z}_p - \{0\} = \bigcup_{n \geq 0} p^n \mathbb{Z}_p^\times.$$

Then

$$\begin{aligned}
\int_{\mathbb{Z}_p - \{0\}} \log |x|_p dx &= \sum_{n=0}^{\infty} \int_{p^n \mathbb{Z}_p^\times} \log |x|_p dx \\
&= \sum_{n=0}^{\infty} \log p^{-n} \text{vol}_{dx}(p^n \mathbb{Z}_p^\times) \\
&= -\log p \sum_{n=0}^{\infty} n(p^{-n} - p^{-n-1}) \\
&= -\log p \left(\sum_{n=0}^{\infty} \frac{n}{p^n} - \frac{1}{p} \sum_{n=0}^{\infty} \frac{n}{p^n} \right) \\
&= -\left(1 - \frac{1}{p}\right) \log p \sum_{n=0}^{\infty} \frac{n}{p^n} \\
&= -\left(1 - \frac{1}{p}\right) \log p \frac{p}{(p-1)^2} \\
&= -\frac{\log p}{p-1}.
\end{aligned}$$

22: EXAMPLE

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

[Break \mathbb{Z}_p^\times up via the scheme

$$(\mathbb{Z}_p^\times : a_0 \neq 1) \cup (\mathbb{Z}_p^\times : a_0 = 1, a_1 \neq 0) \cup (\mathbb{Z}_p^\times : a_0 = 1, a_1 = 0, a_2 \neq 0) \cup \dots.]$$

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

\mathbb{Q}_p^\times .

PROOF $\forall y \in \mathbb{Q}_p^\times$,

$$\begin{aligned}
\int_{\mathbb{Q}_p^\times} f(y^{-1}x) \frac{dx}{|x|_p} &= |y|_p^{-1} \int_{\mathbb{Q}_p^\times} f(y^{-1}x) \frac{1}{|y^{-1}x|_p} dx \\
&= |y|_p^{-1} \text{mod}_{\mathbb{Q}_p}(y) \int_{\mathbb{Q}_p^\times} f(x) \frac{dx}{|x|_p}
\end{aligned}$$

$$\begin{aligned}
&= |y|_p^{-1} |y|_p \int_{\mathbb{Q}_p^\times} f(x) \frac{dx}{|x|_p} \\
&= \int_{\mathbb{Q}_p^\times} f(x) \frac{dx}{|x|_p}.
\end{aligned}$$

24: EXAMPLE

$$\begin{aligned}
\text{vol}_{\frac{dx}{|x|_p}}(p^n \mathbb{Z}_p^\times) &= \text{vol}_{\frac{dx}{|x|_p}}(\mathbb{Z}_p^\times) \\
&= \int_{\mathbb{Z}_p^\times} \frac{dx}{|x|_p} \\
&= \int_{\mathbb{Z}_p^\times} dx \\
&= \text{vol}_{dx}(\mathbb{Z}_p^\times) \\
&= \frac{p-1}{p}.
\end{aligned}$$

25: DEFINITION The normalized Haar measure on the multiplicative group \mathbb{Q}_p^\times is given by

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

Accordingly,

$$\text{vol}_{d^\times x}(\mathbb{Z}_p^\times) = 1,$$

this condition characterizing $d^\times x$.

26: EXAMPLE Let s be a complex variable with $\Re(s) > 1$. Write

$$\mathbb{Z}_p - \{0\} = \bigcup_{n \geq 0} p^n \mathbb{Z}_p^\times.$$

Then

$$\begin{aligned}
\int_{\mathbb{Z}_p - \{0\}} |x|_p^s d^\times x &= \sum_{n=0}^{\infty} p^{-ns} \int_{\mathbb{Z}_p^\times} d^\times x \\
&= \sum_{n=0}^{\infty} p^{-ns} \\
&= \frac{1}{1 - p^{-s}},
\end{aligned}$$

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

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

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

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

$$\begin{aligned} \text{vol}_{d^\times a}(R^\times) &= \int_{R^\times} \frac{q}{q-1} \frac{da}{|a|_{\mathbb{K}}} \\ &= \frac{q}{q-1} \int_{R^\times} da \\ &= \sum_{n=0}^{\infty} q^{-n} \int_{R^\times} da \\ &= \sum_{n=0}^{\infty} \int_{R^\times} q^{-n} da \\ &= \sum_{n=0}^{\infty} \int_{\pi^n R^\times} da \\ &= \int_{\bigcup_{n \geq 0} \pi^n R^\times} da \\ &= \int_R da \\ &= \text{vol}_{da}(R). \end{aligned}$$

§7. HARMONIC ANALYSIS

Let G be a locally compact abelian group.

1: DEFINITION A character of G is a continuous homomorphism $\chi : G \rightarrow \mathbb{C}^\times$.

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 $\chi : G \rightarrow \mathbb{T}$.

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 $\mathbb{R}_{>0}$ is the trivial subgroup $\{1\}$.

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

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

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

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

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

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

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 $G = \mathbb{R}$ 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 $t \in \mathbb{R}$ such that $\chi = \chi_t$, hence G can be identified with \hat{G} .

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

20: EXAMPLE Take $G = \mathbb{Z}/n\mathbb{Z}$ and given an integer $m = 0, 1, \dots, n-1$, let $\chi_m(k) = \exp\left(2\pi\sqrt{-1} \frac{km}{n}\right)$ –then $\chi_0, \chi_1, \dots, \chi_{n-1}$ are 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 $G = \mathbb{T}$ and given $n \in \mathbb{Z}$, 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 $\mathbb{T} \approx \mathbb{Z}$.

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

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

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 $G = \mathbb{R}^\times$ –then

$$G \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}_{>0}^\times \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{R},$$

thus \widehat{G} is topologically isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{R}$:

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

where

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

27: EXAMPLE Take $G = \mathbb{C}^\times$ –then

$$G \approx \mathbb{T} \times \mathbb{R}_{>0}^\times \approx \mathbb{T} \times \mathbb{R},$$

thus \widehat{G} is topologically isomorphic to $\mathbb{Z} \times \mathbb{R}$:

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

where

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

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

$$\text{ev}_G(x)(\chi) = \chi(x).$$

28: REMARK If G, H are locally compact abelian groups and if $\phi : G \rightarrow H$ is

a continuous homomorphism, then there is a commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\text{ev}_G} & \widehat{\widehat{G}} \\ \downarrow \phi & & \downarrow \widehat{\widehat{\phi}} \\ H & \xrightarrow{\text{ev}_H} & \widehat{\widehat{H}} \end{array} .$$

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 $\widehat{G} : G \approx \widehat{G}$ (but the isomorphism is not "functorial").

Let H be a closed subgroup of G .

32: NOTATION Put

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

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

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

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

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 subgroup of G –then G contains a subgroup isomorphic to G/H .

[In fact,

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

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

$$\widehat{}: \mathbf{LCA} \rightarrow \mathbf{LCA}$$

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 $\widehat{}$:

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

which is also a short exact sequence.

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

$$\widehat{f}: \widehat{G} \rightarrow \mathbb{C}$$

defined by the rule

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

38: EXAMPLE Take $G = \mathbb{R}$ –then $\widehat{\mathbb{R}} \approx \mathbb{R}$ and

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

39: EXAMPLE Take $G = \mathbb{R}^2$ –then $\widehat{\mathbb{R}^2} \approx \mathbb{R}^2$ and

$$\widehat{f}(\chi_{(t_1, t_2)}) \equiv \widehat{f}(t_1, t_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_1, x_2) e^{\sqrt{-1} \, (t_1 x_1 + t_2 x_2)} dx_1 dx_2.$$

40: EXAMPLE Take $G = \mathbb{T}$ –then $\widehat{\mathbb{T}} \approx \mathbb{Z}$ and

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

41: EXAMPLE Take $G = \mathbb{Z}$ –then $\widehat{\mathbb{Z}} \approx \mathbb{T}$ and

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

42: EXAMPLE Take $G = \mathbb{Z}/n\mathbb{Z}$ –then $\widehat{\mathbb{Z}/n\mathbb{Z}} \approx \mathbb{Z}/n\mathbb{Z}$ and

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

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

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

44: NOTATION $\text{INV}(G)$ is the set of continuous functions $f \in L^1(G)$ with the
property that $\widehat{f} \in L^1(\widehat{G})$.

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

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

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

46: 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

$$\begin{aligned} \int_G \chi(x) d\mu_G(x) &= \int_G \chi(x - x_0 + x_0) d\mu_G(x) \\ &= \chi(x_0) \int_G \chi(x - x_0) d\mu_G(x) \\ &= \chi(x_0) \int_G \chi(x) d\mu_G(x) \end{aligned}$$

\Rightarrow

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

Assuming still that G is compact ($\Rightarrow \widehat{G}$ is discrete), take $f \equiv 1$:

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

I.e.: \widehat{f} is the characteristic function of $\{0\}$, hence is integrable, thus $f \in \mathbf{INV}(G)$. Accord-

ingly, if $\mu_{\widehat{G}}$ is the Haar measure on \widehat{G} per Fourier inversion, then

$$\begin{aligned} 1 &= f(0) \\ &= \int_{\widehat{G}} \widehat{f}(\chi) d\mu_{\widehat{G}}(\chi) \\ &= \mu_{\widehat{G}}(\{0\}), \end{aligned}$$

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

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

47: EXAMPLE Let $G = \mathbb{T}$ —then $d\mu_G = \frac{d\theta}{2\pi}$, so for $f \in \mathbf{INV}(G)$,

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

where

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

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

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

Assuming still that G is discrete ($\implies \widehat{G}$ is compact), take $f(0) = 1, f(x) = 0$ ($x \neq 0$) :

$$\begin{aligned} \widehat{f}(\chi) &= \int_G f(x) \chi(x) d\mu_G(x) \\ &= f(0) \chi(0) \mu_G(\{0\}) \\ &= 1. \end{aligned}$$

I.e.: \widehat{f} is the constant function 1, hence is integrable, thus $f \in \mathbf{INV}(G)$. Accordingly, if

$\mu_{\widehat{G}}$ is the Haar measure on \widehat{G} per Fourier inversion, then

$$\begin{aligned}\mu_{\widehat{G}}(\widehat{G}) &= \int_{\widehat{G}} 1 d\mu_{\widehat{G}}(\chi) \\ &= \int_{\widehat{G}} \widehat{f}(\chi) d\mu_{\widehat{G}}(\chi) \\ &= \int_{\widehat{G}} \widehat{f}(\chi) \chi(0) d\mu_{\widehat{G}}(\chi) \\ &= f(0) \\ &= 1.\end{aligned}$$

49: EXAMPLE Take $G = \mathbb{Z}/n\mathbb{Z}$ and let μ_G be the counting measure (thus here $\mu_G(G) = n$) –then $\mu_{\widehat{G}}$ is the counting measure divided by n and for $f \in \mathbf{INV}(G)$,

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

where

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

50: EXAMPLE Take $G = \mathbb{R}$ and let $\mu_G = \alpha dx$ ($\alpha > 0$), hence $\mu_{\widehat{G}} = \beta dt$ ($\beta > 0$) and we claim that

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

To establish this, recall first that the formalism is

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

Let $f(x) = e^{-|x|}$ –then

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

so $f \in \mathbf{INV}(G)$, 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 being that the Haar measure of $[0, 1]$ is not 1 but rather $\frac{1}{\sqrt{2\pi}}$.

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

$$\mathcal{F}_{\mathbb{R}}f(t) = \int_{-\infty}^{\infty} f(x) e^{2\pi\sqrt{-1} tx} dx.$$

Therefore

$$\begin{aligned} \mathcal{F}_{\mathbb{R}}f(t) &= \sqrt{2\pi} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{2\pi\sqrt{-1} tx} dx \\ &= \sqrt{2\pi} \hat{f}(2\pi t). \end{aligned}$$

52: STANDARDIZATION ($G = \mathbb{R}$) Let $f \in \mathbf{INV}(\mathbb{R})$, —then

$$\mathcal{F}_{\mathbb{R}}\mathcal{F}_{\mathbb{R}}f(x) = f(-x).$$

[In fact,

$$\begin{aligned} \mathcal{F}_{\mathbb{R}}\mathcal{F}_{\mathbb{R}}f(x) &= \int_{-\infty}^{\infty} \mathcal{F}_{\mathbb{R}}f(t) e^{2\pi\sqrt{-1} tx} dx \\ &= \int_{-\infty}^{\infty} \sqrt{2\pi} \hat{f}(2\pi t) e^{2\pi\sqrt{-1} tx} dx \\ &= \sqrt{2\pi} \int_{-\infty}^{\infty} \hat{f}(u) e^{\sqrt{-1} ux} \frac{du}{2\pi} \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \widehat{f}(t) e^{\sqrt{-1} tx} dt \\
&= f(-x).]
\end{aligned}$$

Fourier inversion in the plane takes the form

$$\begin{cases} \widehat{f}(t_1, t_2) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_1, x_2) e^{\sqrt{-1} (t_1 x_1 + t_2 x_2)} dx_1 dx_2 \\ f(x_1, x_2) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \widehat{f}(t_1, t_2) e^{-\sqrt{-1} (t_1 x_1 + t_2 x_2)} dt_1 dt_2 \end{cases}.$$

One may then introduce

$$\begin{aligned}
\mathcal{F}_{\mathbb{R}^2} f(t_1, t_2) &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_1, x_2) e^{2\pi\sqrt{-1} (t_1 x_1 + t_2 x_2)} dx_1 dx_2 \\
&= 2\pi \widehat{f}(2\pi t_1, 2\pi t_2)
\end{aligned}$$

and proceeding as above we find that

$$\mathcal{F}_{\mathbb{R}^2} \mathcal{F}_{\mathbb{R}^2} f(x_1, x_2) = f(-x_1, -x_2).$$

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

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

Then

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

Therefore

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) e^{2\sqrt{-1} (ax - by)} dx dy = \widehat{f}(2a, -2b).$$

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

53: NOTATION Given $f \in L^1(\mathbb{R}^2)$, let

$$\begin{aligned}
 \mathcal{F}_{\mathbb{C}} f(w) &= \mathcal{F}_{\mathbb{C}} f(a, b) \\
 &= 2\mathcal{F}_{\mathbb{R}^2} f(2a, -2b) \\
 &= 4\pi \widehat{f}(4\pi a, -4\pi b) \\
 &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) e^{4\pi\sqrt{-1} (ax-by)} 2dxdy
 \end{aligned}$$

54: STANDARDIZATION ($G = \mathbb{C}$) Let $f \in \mathbf{INV}(\mathbb{C})$, -then

$$\mathcal{F}_{\mathbb{C}} \mathcal{F}_{\mathbb{C}} f(x, y) = f(-x, -y).$$

[In fact,

$$\begin{aligned}
 \mathcal{F}_{\mathbb{C}} \mathcal{F}_{\mathbb{C}} f(x, y) &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \mathcal{F}_{\mathbb{C}} f(a, b) e^{4\pi\sqrt{-1} (ax-by)} 2dad b \\
 &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} 4\pi \widehat{f}(4\pi a, -4\pi b) e^{4\pi\sqrt{-1} (ax-by)} 2dad b \\
 &= \frac{4\pi}{(4\pi)^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \widehat{f}(u, -v) e^{\sqrt{-1} (ux-vy)} 2dudv \\
 &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \widehat{f}(u, -v) e^{\sqrt{-1} (ux-vy)} dudv \\
 &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \widehat{f}(u, -v) e^{-\sqrt{-1} (-ux+vy)} dudv \\
 &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \widehat{f}(u, v) e^{-\sqrt{-1} (-ux-vy)} dudv \\
 &= f(-x, -y).]
 \end{aligned}$$

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 $L^2(\widehat{G})$, hence can be extended uniquely to an isometric isomorphism $L^2(G) \rightarrow L^2(\widehat{G})$.

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

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

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

§8. ADDITIVE p-ADIC CHARACTER THEORY

1: FACT Every proper closed subgroup of \mathbb{T} is finite.

Suppose that G is compact abelian and totally disconnected.

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

PROOF $\ker \chi$ is closed and

$$\chi(G) \approx G/\ker \chi.$$

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

3: N.B. The torsion of \mathbb{R}/\mathbb{Z} is \mathbb{Q}/\mathbb{Z} , so χ factors through the inclusion

$$\mathbb{Q}/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z}, \quad \text{i.e., } \chi(G) \subset \mathbb{Q}/\mathbb{Z}.$$

The foregoing applies in particular to $G = \mathbb{Z}_p$.

4: LEMMA Every character of \mathbb{Q}_p is unitary.

PROOF This is because

$$\mathbb{Q}_p = \bigcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p,$$

where the $p^n \mathbb{Z}_p$ are compact, thus §7, #7 is applicable.

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

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

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

A typical $x \neq 0$ of \mathbb{Q}_p has the form

$$\begin{aligned} x &= \sum_{n=v(x)}^{\infty} a_n p^n \quad (a_n \in \mathcal{A}, v(x) \in \mathbb{Z}) \\ &= f(x) + [x]. \end{aligned}$$

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.

$$f(x) \in \mathbb{Z}\left[\frac{1}{p}\right] \subset \mathbb{Q},$$

where

$$\mathbb{Z}\left[\frac{1}{p}\right] = \left\{ \frac{n}{p^k} : n \in \mathbb{Z}, k \in \mathbb{Z} \right\},$$

while $[x] \in \mathbb{Z}_p$.

8: OBSERVATION

$$\begin{aligned} 0 &\leq f(x) \\ &= \sum_{1 \leq j \leq -v(x)} \frac{a_{-j}}{p^j} \end{aligned}$$

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

\implies

$$f(x) \in [0, 1[\cap \mathbb{Z}\left[\frac{1}{p}\right].$$

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

$$\left\{ \begin{array}{l} \mu_p \subset \mu_{p^2} \subset \cdots \subset \mu_{p^k} \subset \cdots \\ \mu_{p^\infty} = \bigcup_{k \geq 0} \mu_{p^k} \end{array} \right.,$$

where

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

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

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

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

$$\chi_p(x) = \exp(2\pi\sqrt{-1} f(x)) \quad (x \in \mathbb{Q}_p).$$

Then

$$\chi_p : \mathbb{Q}_p \rightarrow \mathbb{T}$$

and $\mathbb{Z}_p \subset \ker \chi_p$.

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

$y \in \mathbb{Z}_p :$

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

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

11: LEMMA χ_p is a unitary character

PROOF Given $x, y \in \mathbb{Q}_p$, write

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

But at the same time

$$f(x+y) - f(x) - f(y) \in \mathbb{Z}\left[\frac{1}{p}\right].$$

Thus

$$f(x+y) - f(x) - f(y) \in \mathbb{Z}\left[\frac{1}{p}\right] \cap \mathbb{Z}_p = \mathbb{Z}$$

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 $\chi_p : \mathbb{Q}_p \rightarrow \mathbb{T}$ is a homomorphism. As for continuity, it suffice to check this at 0, matters then being clear (since χ_p is trivial in a neighborhood of 0) (\mathbb{Z}_p is open and $0 \in \mathbb{Z}_p$).

12: LEMMA The kernel of χ_p is \mathbb{Z}_p .

[A priori, the kernel of χ_p consists of those $x \in \mathbb{Q}_p$ such that $f(x) \in \mathbb{Z}$. Therefore

$$\ker \chi_p = \mathbb{Z}_p.]$$

13: 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.]

14: SCHOLIUM χ_p implements an isomorphism

$$\mathbb{Q}_p/\mathbb{Z}_p \approx \mu_{p^\infty}.$$

15: REMARK

$$\begin{aligned} x \in p^{-k}\mathbb{Z}_p &\Leftrightarrow p^k x \in \mathbb{Z}_p \\ &\Leftrightarrow \chi_p(p^k x) = 1 \\ &\Leftrightarrow \chi_p(x)^{p^k} = 1 \\ &\Leftrightarrow \chi_p(x) \in \mu_{p^k}. \end{aligned}$$

16: RAPPEL Let p be a prime —then a group is p -primary if every element has order a power of p .

17: RAPPEL Every abelian torsion group G is a direct sum of its p -primary subgroups G_p .

[Note: The p -primary component of G_p is the p -Sylow subgroup of G .]

18: NOTATION $\mathbb{Z}(p^\infty)$ is the p -primary component of \mathbb{Q}/\mathbb{Z} .

Therefore

$$\mathbb{Q}/\mathbb{Z} \approx \bigoplus_p \mathbb{Z}(p^\infty).$$

19: LEMMA $\mathbb{Z}(p^\infty)$ is isomorphic to μ_{p^∞} .

[$\mathbb{Z}(p^\infty)$ is generated by the $1/p^n$ in \mathbb{Q}/\mathbb{Z} .]

Therefore

$$\mathbb{Q}/\mathbb{Z} \approx \bigoplus_p \mu_{p^\infty} \approx \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p.$$

[Note: Consequently,

$$\begin{aligned} \text{End}(\mathbb{Q}/\mathbb{Z}) &\approx \text{End}\left(\bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p\right) \\ &\approx \prod_p \text{End}(\mathbb{Q}_p/\mathbb{Z}_p) \\ &\approx \prod_p \mathbb{Z}_p. \end{aligned}$$

20: REMARK $\widehat{\mathbb{Z}}_p$ is isomorphic to μ_{p^∞} (c.f. #26 infra).

Given $t \in \mathbb{Q}_p$, 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 $\forall x \in \mathbb{Q}_p$,

$$\chi_{p,t}(x) = \chi_p(tx).$$

[Note: Trivially, $\chi_{p,0} \equiv 1$. And $\forall t \neq 0$,

$$\text{con } \chi_{p,t} = p^{-v(t)}\mathbb{Z}_p.$$

Proof:

$$\begin{aligned} x \in \text{con } \chi_{p,t} &\Leftrightarrow tx \in \mathbb{Z}_p \\ &\Leftrightarrow |tx|_p \leq 1 \\ &\Leftrightarrow |x|_p \leq \frac{1}{|t|_p} = p^{v(t)} \\ &\Leftrightarrow x \in p^{-v(t)}\mathbb{Z}_p. \end{aligned}$$

Next

$$\begin{aligned}
\chi_{p,t}(x+y) &= \chi_p(t(x+y)) \\
&= \chi_p(tx+ty) \\
&= \chi_p(tx)\chi_p(ty) \\
&= \chi_{p,t}(x)\chi_{p,t}(y).
\end{aligned}$$

Therefore $\chi_{p,t} \in \widehat{\mathbb{Q}_p}$.

Next

$$\begin{aligned}
\chi_{p,t+s}(x) &= \chi_p((t+s)x) \\
&= \chi_p(tx+sx) \\
&= \chi_p(tx)\chi_p(sx) \\
&= \chi_{p,t}(x)\chi_{p,s}(x).
\end{aligned}$$

Therefore the arrow

$$\begin{aligned}
\Xi_p : \mathbb{Q}_p &\rightarrow \widehat{\mathbb{Q}_p} \\
t &\mapsto \chi_{p,t}
\end{aligned}$$

is a homomorphism.

21: 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 $\forall x \in \mathbb{Q}_p$, $\chi_p(tx) = \chi_p(sx)$ or still, $\forall x \in \mathbb{Q}_p$, $\chi_p((t-s)x) = 1$. But $L_{t-s} : \mathbb{Q}_p \rightarrow \mathbb{Q}_p$ is an automorphism, hence χ_p is trivial, which it isn't.

22: LEMMA The set

$$\Xi_p(\mathbb{Q}_p) = \{\chi_{p,t} : t \in \mathbb{Q}_p\}$$

is dense in $\widehat{\mathbb{Q}_p}$.

PROOF Let H be the closure in $\widehat{\mathbb{Q}}_p$ of the $\chi_{p,t}$. Consider the quotient $\widehat{\mathbb{Q}}_p/H$. To get a contradiction, assume that $H \neq \widehat{\mathbb{Q}}_p$, thus that there is a nontrivial $\xi \in \widehat{\widehat{\mathbb{Q}}_p}$ which is trivial on H . By definition, H^\perp is computed in $\widehat{\widehat{\mathbb{Q}}_p}$, which by Pontryagin duality, is identified with \mathbb{Q}_p , so spelled out

$$H^\perp = \{x \in \mathbb{Q}_p : \text{ev}_{\mathbb{Q}_p}(x)|_H = 1\}.$$

Accordingly, for some x , $\xi = \text{ev}_{\mathbb{Q}_p}(x)$, hence $\forall t$,

$$\begin{aligned} \xi(\chi_{p,t}) &= \text{ev}_{\mathbb{Q}_p}(x)(\chi_{p,t}) \\ &= \chi_{p,t}(x) \\ &= \chi_p(tx) \\ &= 1, \end{aligned}$$

which is possible only if $x = 0$ and this implies that ξ is trivial.

23: LEMMA The arrows

$$\begin{cases} \mathbb{Q}_p \rightarrow \Xi_p(\mathbb{Q}_p) \\ \Xi_p(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p \end{cases}$$

are continuous.

Therefore $\Xi(\mathbb{Q}_p)$ is a locally compact subgroup of $\widehat{\mathbb{Q}}_p$. But a locally compact subgroup of a locally compact group is closed. Therefore $\Xi_p(\mathbb{Q}_p) = \widehat{\mathbb{Q}}_p$.

In summary:

24: THEOREM $\widehat{\mathbb{Q}}_p$ is topologically isomorphic to \mathbb{Q}_p via the arrow

$$\Xi_p : \mathbb{Q}_p \rightarrow \widehat{\mathbb{Q}}_p.$$

25: LEMMA Fix t —then $\chi_{p,t}|_{\mathbb{Z}_p} = 1$ iff $t \in \mathbb{Z}_p$.

PROOF Recall that the kernel of χ_p is \mathbb{Z}_p .

- $t \in \mathbb{Z}_p, x \in \mathbb{Z}_p \implies tx \in \mathbb{Z}_p \implies \chi_p(tx) = 1 \implies \chi_{p,t}|_{\mathbb{Z}_p} = 1.$
- $\chi_{p,t}|_{\mathbb{Z}_p} = 1 \implies \chi_{p,t}(1) = 1 \implies \chi_p(t) = 1 \implies t \in \mathbb{Z}_p.$

26: APPLICATION $\widehat{\mathbb{Z}}_p$ is isomorphic to μ_{p^∞} .

$[\widehat{\mathbb{Z}}_p$ can be computed as $\widehat{\mathbb{Q}}_p/\mathbb{Z}_p^\perp$. But \mathbb{Z}_p^\perp , when viewed as a subset of \mathbb{Q}_p , consists of those t such that $\chi_{p,t}|_{\mathbb{Z}_p} = 1$. Therefore

$$\widehat{\mathbb{Z}}_p \approx \widehat{\mathbb{Q}}_p/\mathbb{Z}_p \approx \mathbb{Q}_p/\mathbb{Z}_p \approx \mu_{p^\infty}.]$$

27: NOTATION Let

$$x_\infty(x) = \exp(-2\pi\sqrt{-1} x) \quad (x \in \mathbb{R}).$$

28: PRODUCT PRINCIPLE $\forall x \in \mathbb{Q},$

$$\prod_{p \leq \infty} \chi_p(x) = 1.$$

PROOF Take x positive –then there exist primes p_1, \dots, p_n such that x admits a representation

$$x = \frac{N_1}{p_1^{\alpha_1}} + \frac{N_2}{p_2^{\alpha_2}} + \dots + \frac{N_n}{p_n^{\alpha_n}} + M,$$

where the α_k are positive integers, the N_k are positive integers ($1 \leq N_k < p_k^{\alpha_k} - 1$), and $M \in \mathbb{Z}$. Appending a subscript to f , we have

$$f_{p_k}(x) = \frac{N_k}{p_k^{\alpha_k}}, \quad f_p(x) = 0 \quad (p \neq p_k, \ k = 1, 2, \dots, n).$$

Therefore

$$\prod_{p < \infty} \chi_p(x) = \prod_{1 \leq k \leq n} \chi_{p_k}(x)$$

$$\begin{aligned}
&= \prod_{1 \leq k \leq n} \exp(2\pi\sqrt{-1} f_{p_k}(x)) \\
&= \exp(2\pi\sqrt{-1} \sum_{k=1}^n f_{p_k}(x)) \\
&= \exp(2\pi\sqrt{-1} (x - M)) \\
&= \exp(2\pi\sqrt{-1} x)
\end{aligned}$$

\Rightarrow

$$\begin{aligned}
\prod_{p \leq \infty} \chi_p(x) &= \prod_{p < \infty} \chi_p(x) \chi_\infty(x) \\
&= \exp(2\pi\sqrt{-1} x) \exp(-2\pi\sqrt{-1} x) \\
&= 1.
\end{aligned}$$

APPENDIX

Let \mathbb{K} be a finite extension of \mathbb{Q}_p .

1: THEOREM The topological groups \mathbb{K} and $\widehat{\mathbb{K}}$ are topologically isomorphic.

[Put

$$\begin{aligned}
\chi_{\mathbb{K},p}(a) &= \exp(2\pi\sqrt{-1} f(\text{tr}_{\mathbb{K}/\mathbb{Q}_p}(a))) \\
&= \chi_p(\text{tr}_{\mathbb{K}/\mathbb{Q}_p}(a))
\end{aligned}$$

and given $b \in \mathbb{K}$, put

$$\chi_{\mathbb{K},p,b}(a) = \chi_{\mathbb{K},p}(ab).$$

Proceed from here as above.]

2: REMARK Every character of \mathbb{K} is unitary.

3: LEMMA

$$\begin{cases} a \in R & \implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(a) \in \mathbb{Z}_p \\ a \in P & \implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(a) \in p\mathbb{Z}_p \end{cases}.$$

4: DEFINITION The differential of \mathbb{K} is the set

$$\Delta_{\mathbb{K}} = \{b \in \mathbb{K} : \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(Rb) \subset \mathbb{Z}_p\}.$$

5: LEMMA $\Delta_{\mathbb{K}}$ is a proper R -submodule of \mathbb{K} containing R .

6: LEMMA There exists a unique nonnegative integer d –the differential exponent of \mathbb{K} –characterized by the condition that

$$\pi^{-d}R = \Delta_{\mathbb{K}}.$$

[This follows from the theory of "fractional ideals" (details omitted).]

[Note: $\chi_{\mathbb{K},p}$ is trivial on $\pi^{-d}R$ but is nontrivial on $\pi^{-d-1}R$.]

7: LEMMA Let e be the ramification index of \mathbb{K} over \mathbb{Q}_p (cf. §5, #17) – then

$$a \in P^{-e+1} \implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(a) \in \mathbb{Z}_p.$$

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

$$|u| = 1, |b| < 1 \implies |ub| < 1$$

$$\begin{aligned}
&\implies ub \in P \\
&\implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(ub) \in p\mathbb{Z}_p \\
&\implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(pa) \in p\mathbb{Z}_p \\
&\implies p\operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(a) \in p\mathbb{Z}_p \\
&\implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(a) \in \mathbb{Z}_p.
\end{aligned}$$

8: APPLICATION

$$d \geq e - 1.$$

[It suffices to show that

$$P^{-e+1} \subset \Delta_{\mathbb{K}} \quad (\equiv \pi^{-d}R).$$

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

$$\operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(ar) \in \mathbb{Z}_p.$$

But

$$ar = \pi^{-e}br \in \pi^e P \quad (|br| < 1)$$

or still,

$$ar \in P^{-e+1} \implies \operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(ar) \in \mathbb{Z}_p.]$$

9: REMARK Therefore $d = 0 \implies e = 1$, hence in this situation, \mathbb{K} is unramified.

[Note: There is also a converse, viz. if \mathbb{K} is unramified, then $d = 0$.]

10: N.B. It can be shown that

$$\operatorname{tr}_{\mathbb{K}/\mathbb{Q}_p}(R) = \mathbb{Z}_p \quad \text{iff} \quad d = e - 1.$$

11: CRITERION Fix $b \in \mathbb{K}$ –then

$$b \in \Delta_{\mathbb{K}} \Leftrightarrow \forall a \in R, \chi_{\mathbb{K},p}(ab) = 1.$$

PROOF

- $a \in R, b \in \Delta_{\mathbb{K}} \implies ab \in \Delta_{\mathbb{K}}$
 $\implies \text{tr}_{\mathbb{K}/\mathbb{Q}_p}(ab) \in \mathbb{Z}_p$
 \implies
 $\chi_{\mathbb{K},p}(ab) = \chi_p(\text{tr}_{\mathbb{K}/\mathbb{Q}_p}(ab)) = 1.$
- $\forall a \in R, \chi_{\mathbb{K},p}(ab) = 1$
 $\implies \forall a \in R, \text{tr}_{\mathbb{K}/\mathbb{Q}_p}(ab) \in \mathbb{Z}_p$
 $\implies b \in \Delta_{\mathbb{K}}.$

Normalize Haar measure on \mathbb{K} by the condition

$$\mu_{\mathbb{K}}(R) = \int_R da = q^{-d/2}.$$

Let χ_R be the characteristic function of R –then

$$\int_{\mathbb{K}} \chi_R(a) \chi_{\mathbb{K},p}(ab) da = \int_R \chi_{\mathbb{K},p}(ab) da.$$

- $b \in \Delta_{\mathbb{K}} \implies \chi_{\mathbb{K},p}(ab) = 1 \quad (\forall a \in R)$
 $\implies \int_R \chi_{\mathbb{K},p}(ab) da = \mu_{\mathbb{K}}(R) = q^{-d/2}.$
- $b \notin \Delta_{\mathbb{K}} \implies \chi_{\mathbb{K},p}(ab) \neq 1 \quad (\exists a \in R)$
 $\implies \int_R \chi_{\mathbb{K},p}(ab) da = 0.$

Consequently, as a function of b ,

$$\int_R \chi_{\mathbb{K},p}(ab) da = q^{-d/2} \chi_{\Delta_{\mathbb{K}}}(b),$$

$\chi_{\Delta_{\mathbb{K}}}$ the characteristic function of $\Delta_{\mathbb{K}}$.

12: LEMMA

$$[\pi^{-d}R : R] = q^d.$$

Therefore

$$\begin{aligned}\mu_{\mathbb{K}}(\Delta_{\mathbb{K}}) &= \mu_{\mathbb{K}}(\pi^{-d}R) \\ &= q^d \mu_{\mathbb{K}}(R) \\ &= q^d q^{-d/2} \\ &= q^{d/2}.\end{aligned}$$

13: LEMMA $\forall a \in \mathbb{K},$

$$\int_{\mathbb{K}} q^{-d/2} \chi_{\Delta_{\mathbb{K}}}(b) \chi_{\mathbb{K},p}(ab) db = \chi_R(a).$$

PROOF The left hand side reduces to

$$q^{-d/2} \int_{\Delta_{\mathbb{K}}} \chi_{\mathbb{K},p}(ab) db$$

and there are two possibilities

- $a \in R \implies ab \in \Delta_{\mathbb{K}} \quad (\forall b \in \Delta_{\mathbb{K}})$
 $\implies \text{tr}_{\mathbb{K}/\mathbb{Q}_p}(ab) \in \mathbb{Z}_p$
 $\implies \chi_{\mathbb{K},p}(ab) = 1$
 \implies

$$\begin{aligned}q^{-d/2} \int_{\Delta_{\mathbb{K}}} \chi_{\mathbb{K},p}(ab) db &= q^{-d/2} \mu_{\mathbb{K}}(\Delta_{\mathbb{K}}) \\ &= q^{-d/2} q^{d/2} \\ &= 1.\end{aligned}$$

- $a \notin R : \chi_{K,p}(ab) \neq 1 \quad (\exists b \in \Delta_{\mathbb{K}})$
 \implies

$$q^{-d/2} \int_{\Delta_{\mathbb{K}}} \chi_{\mathbb{K},p}(ab) db = 0.$$

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,

$$x \in \pi^n R \Leftrightarrow |x|_{\mathbb{K}} \leq q^{-n}.$$

Fix $a \notin R$ —then the claim is that $b \rightarrow \chi_{\mathbb{K},p}(ab)$ ($b \in \Delta_{\mathbb{K}}$) is nontrivial. For

$$\begin{aligned} \chi_{\mathbb{K},p}(ab) = 1 &\Leftrightarrow ab \in \pi^{-d}R \\ &\Leftrightarrow |ab|_{\mathbb{K}} \leq q^d \\ &\Leftrightarrow |a|_{\mathbb{K}} |b|_{\mathbb{K}} \leq q^d \\ &\Leftrightarrow |b|_{\mathbb{K}} \leq \frac{q^d}{|a|_{\mathbb{K}}} = q^{d+v(a)}. \end{aligned}$$

But

$$\begin{aligned} a \notin R &\implies v(a) < 0 \\ &\implies -v(a) > 0 \\ &\implies -d - v(a) > -d \\ &\implies \pi^{-d-v(a)}R \subsetneq \pi^{-d}R, \end{aligned}$$

a proper containment.

§9. MULTIPLICATIVE p-ADIC CHARACTER THEORY

Recall that

$$\mathbb{Q}_p^\times \approx \mathbb{Z} \times \mathbb{Z}_p^\times,$$

the abstract reflection of the fact that for ever $x \in \mathbb{Q}_p^\times$, there is a unique $v(x) \in \mathbb{Z}$ and a unique $u(x) \in \mathbb{Z}_p^\times$ such that $x = p^{v(x)}u(x)$. Therefore

$$\widehat{(\mathbb{Q}_p^\times)} \approx \widehat{\mathbb{Z}} \times \widehat{(\mathbb{Z}_p^\times)} \approx \mathbb{T} \times \widehat{(\mathbb{Z}_p^\times)}.$$

1: N.B. A character of \mathbb{Q}_p is necessarily unitary (cf. §8, #4) but this is definitely not the case for \mathbb{Q}_p^\times (cf. infra).

2: DEFINITION A character $\chi : \mathbb{Q}_p^\times \rightarrow \mathbb{C}^\times$ is unramified if it is trivial on \mathbb{Z}_p^\times .

3: EXAMPLE Given any complex number s , the arrow $x \rightarrow |x|_p^s$ is an unramified character of \mathbb{Q}_p^\times .

4: LEMMA If $\chi : \mathbb{Q}_p^\times \rightarrow \mathbb{C}^\times$ 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 $\mathbb{Q}_p^\times \rightarrow p^\mathbb{Z}$ defined by $x \rightarrow |x|_p$, hence gives rise to a character $\tilde{\chi} : p^\mathbb{Z} \rightarrow \mathbb{C}^\times$ 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 $\chi : \mathbb{Q}_p^\times \rightarrow \mathbb{C}^\times$ is a character —then χ can be written as

$$\chi(x) = |x|_p^s \underline{\chi}(u(x)),$$

where $s \in \mathbb{C}$ and $\underline{\chi} \equiv \chi|_{\mathbb{Z}_p^\times} \in \widehat{(\mathbb{Z}_p^\times)}$, thus χ is unitary iff s is pure imaginary.

5: LEMMA If $\underline{\chi} \in \widehat{(\mathbb{Z}_p^\times)}$ is nontrivial, then there is an $n \in \mathbb{N}$ such that $\underline{\chi} \equiv 1$ on $U_{p,n}$ but $\underline{\chi} \not\equiv 1$ on $U_{p,n-1}$ (cf. §8, #5).

Assume again that $\chi : \mathbb{Q}_p^\times \rightarrow \mathbb{C}^\times$ is a character.

6: DEFINITION χ is ramified of degree $n \geq 1$ if $\underline{\chi}|_{U_{p,n}} \equiv 1$ and $\underline{\chi}|_{U_{p,n-1}} \not\equiv 1$.

7: DEFINITION The conductor $\text{con } \chi$ of χ is \mathbb{Z}_p^\times if χ is unramified and $U_{p,n}$ if χ is ramified of degree n .

8: RAPPEL If G is a finite abelian group, then the number of unitary characters of G is $\text{card } G$.

9: LEMMA

$$[\mathbb{Z}_p^\times : U_{p,1}] = p - 1 \quad (\text{cf. } \S 4, \#40)$$

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 $\mathbb{Z}_p^\times / U_{p,n}$. But the quotient $\mathbb{Z}_p^\times / U_{p,n}$ is a finite abelian group, thus has

$$\text{card } \mathbb{Z}_p^\times / U_{p,n} = [\mathbb{Z}_p^\times : U_{p,n}]$$

unitary characters. And

$$\begin{aligned} [\mathbb{Z}_p^\times : U_{p,n}] &= [\mathbb{Z}_p^\times : U_{p,1}] \cdot [U_{p,1} : U_{p,n}] \\ &= (p-1)p^{n-1}, \end{aligned}$$

this being the number of unitary characters of \mathbb{Z}_p^\times of degree $\leq n$. Therefore the group \mathbb{Z}_p^\times has $p-2$ unitary characters of degree 1 and for $n \geq 2$, the group \mathbb{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 $\chi \in \widehat{\mathbb{Q}_p^\times}$ -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 $\tau \in \mathbb{Q}_p^\times - (\mathbb{Q}_p^\times)^2$, and form the quadratic extension

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

1: NOTATION Let $\mathbb{Q}_{p,\tau}$ be the set of points of the form $x^2 - \tau y^2$ ($x \neq 0, y \neq 0$).

2: LEMMA $\mathbb{Q}_{p,\tau}$ is a subgroup of \mathbb{Q}_p^\times containing $(\mathbb{Q}_p^\times)^2$.

3: LEMMA

$$[\mathbb{Q}_p^\times : \mathbb{Q}_{p,\tau}] = 2 \text{ and } [\mathbb{Q}_{p,\tau} : (\mathbb{Q}_p^\times)^2] = 2.$$

[Note:

$$[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2] = 4 \quad (\text{cf. §4, \#53}).]$$

4: DEFINITION Given $x \in \mathbb{Q}_p^\times$, let

$$\text{sgn}_\tau(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q}_{p,\tau} \\ -1 & \text{if } x \notin \mathbb{Q}_{p,\tau} \end{cases}.$$

5: LEMMA sgn_τ is a unitary character of $\widehat{\mathbb{Q}}_p$.

§10. TEST FUNCTIONS

The Schwartz space $\mathcal{S}(\mathbb{R}^n)$ consists of those complex valued \mathcal{C}^∞ functions which, together with all their derivatives, vanish at infinity faster than any power of $\|\cdot\|$.

1: DEFINITION The elements f of $\mathcal{S}(\mathbb{R}^n)$ are the test functions on \mathbb{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

$$\int_{\mathbb{R}} x^A \exp(-\pi x^2) e^{2\pi\sqrt{-1}tx} dx = (\sqrt{-1})^A t^A \exp(-\pi t^2),$$

thus $\mathcal{F}_{\mathbb{R}}$ of a standard function is again standard (c.f. §7, 51).

[Note: Henceforth, by definition, the Fourier transform of an $f \in L^1(\mathbb{R})$ will be the function

$$\widehat{f} : \mathbb{R} \longrightarrow \mathbb{C}$$

defined by the rule

$$\begin{aligned} \widehat{f}(t) &= \mathcal{F}_{\mathbb{R}} f(t) \\ &= \int_{\mathbb{R}} f(x) e^{2\pi\sqrt{-1}tx} dx. \end{aligned}$$

3: EXAMPLE Take $n = 2$ and identify \mathbb{R}^2 with \mathbb{C} –then

$$f(z) = Cz^A \bar{z}^B \exp(-2\pi|z|^2),$$

where $A, B \in \mathbb{Z}_{\geq 0}$ & $AB = 0$, is a test function, said to be standard. Here

$$\int_{\mathbb{C}} z^A \bar{z}^B \exp(-2\pi |z|^2) e^{2\pi\sqrt{-1} (wz + \bar{w}\bar{z})} |dz \wedge d\bar{z}| = \sqrt{-1}^{A+B} w^B \bar{w}^A \exp(-2\pi |w|^2),$$

thus $\mathcal{F}_{\mathbb{C}}$ of a standard function is again standard (c.f. §7, #53).

[Note: Henceforth, by definition, the Fourier transform of an $f \in L^1(\mathbb{C})$ will be the function

$$\hat{f} : \mathbb{C} \longrightarrow \mathbb{C}$$

defined by the rule

$$\begin{aligned} \hat{f}(w) &= \mathcal{F}_{\mathbb{C}} f(w) \\ &= \int_{\mathbb{C}} f(z) e^{2\pi\sqrt{-1} (wz + \bar{w}\bar{z})} |dz \wedge d\bar{z}|. \end{aligned}$$

4: DEFINITION Let G be a totally disconnected locally compact group —then a function $f : G \rightarrow \mathbb{C}$ is said to be locally constant 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 .

5: 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 $f(x_i) = f(x)$.

6: DEFINITION The Bruhat space $\mathcal{B}(G)$ 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 , and integer $n \geq 0$, elements x_1, \dots, x_n in G and elements c_1, \dots, c_n in \mathbb{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 $z \in \mathbb{C}$ the pre image $f^{-1}(z)$ 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

$$\begin{aligned} \phi_x : G \times G &\rightarrow \mathbb{C} \\ (x_1, x_2) &\mapsto f(x_1 x x_2) \end{aligned},$$

thus $\phi_x(e, e) = f(x)$ and ϕ_x is continuous if \mathbb{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 $U_x = K_x \times K_x$ —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 $G = \mathbb{Q}_p$.

9: EXAMPLE If $K \subset \mathbb{Q}_p$ is open-compact, then its characteristic function χ_K is a test function on \mathbb{Q}_p .

10: LEMMA Every $f \in \mathcal{B}(\mathbb{Q}_p)$ is a finite linear combination of functions of the form

$$\chi_{x+p^n\mathbb{Z}_p} \quad (x \in \mathbb{Q}_p, n \in \mathbb{Z}).$$

[This is an instance of #8 or argue directly (c.f. §4, #33).]

11: DEFINITION Given $f \in L^1(\mathbb{Q}_p)$, its Fourier transform is the function

$$\widehat{f} : \mathbb{Q}_p \longrightarrow \mathbb{C}$$

defined by the rule

$$\begin{aligned}\widehat{f}(t) &= \int_{\mathbb{Q}_p} f(x) \chi_{p,t}(x) dx \\ &= \int_{\mathbb{Q}_p} f(x) \chi_p(tx) dx.\end{aligned}$$

12: LEMMA $\forall f \in L^1(\mathbb{Q}_p)$,

$$\widehat{\widehat{f}}(t) = \overline{\widehat{f}(-t)}.$$

PROOF

$$\begin{aligned}\widehat{\widehat{f}}(t) &= \int_{\mathbb{Q}_p} \overline{\widehat{f}(x)} \chi_p(tx) dx \\ &= \int_{\mathbb{Q}_p} \overline{f(x) \chi_p(-tx)} dx \\ &= \int_{\mathbb{Q}_p} \overline{f(x) \chi_p((-t)x)} dx \\ &= \overline{\int_{\mathbb{Q}_p} f(x) \chi_p((-t)x) dx} \\ &= \overline{\widehat{f}(-t)}.\end{aligned}$$

13: SUBLEMMA

$$\int_{p^n \mathbb{Z}_p} \chi_p(x) dx = \begin{cases} p^{-n} & (n \geq 0) \\ 0 & (n < 0) \end{cases}.$$

[Recall that

$$\mu_{\mathbb{Q}_p}(p^n \mathbb{Z}_p) = p^{-n}$$

and apply §7, #46 and §8, #12.]

14: LEMMA Take $f = \chi_{p^n \mathbb{Z}_p}$ —then

$$\widehat{\chi}_{p^n \mathbb{Z}_p} = p^{-n} \chi_{p^{-n} \mathbb{Z}_p}.$$

PROOF

$$\begin{aligned} \widehat{\chi}_{p^n \mathbb{Z}_p}(t) &= \int_{\mathbb{Q}_p} \chi_{p^n \mathbb{Z}_p}(x) \chi_{p,t}(x) dx \\ &= \int_{\mathbb{Q}_p} \chi_{p^n \mathbb{Z}_p}(x) \chi_p(tx) dx \\ &= |t|_p^{-1} \int_{\mathbb{Q}_p} \chi_{p^n \mathbb{Z}_p}(t^{-1}x) \chi_p(x) dx \\ &= |t|_p^{-1} \int_{p^{n+v(t)} \mathbb{Z}_p} \chi_p(x) dx. \end{aligned}$$

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

$$t \in p^{-n} \mathbb{Z}_p \Leftrightarrow v(t) \geq -n \Leftrightarrow n + v(t) \geq 0.$$

Since

$$|t|_p^{-1} p^{v(t)} = 1,$$

it therefore follows that

$$\widehat{\chi}_{p^n \mathbb{Z}_p} = p^{-n} \chi_{p^{-n} \mathbb{Z}_p}.$$

In particular,

$$\widehat{\chi}_{\mathbb{Z}_p} = \chi_{\mathbb{Z}_p}.$$

15: THEOREM Take $f = \chi_{x+p^n\mathbb{Z}_p}$ -then

$$\widehat{\chi}_{x+p^n\mathbb{Z}_p}(t) = \begin{cases} \chi_p(tx)p^{-n} & (|t|_p \leq p^n) \\ 0 & (|t|_p > p^n) \end{cases}.$$

PROOF

$$\begin{aligned} \widehat{\chi}_{x+p^n\mathbb{Z}_p}(t) &= \int_{\mathbb{Q}_p} \chi_{x+p^n\mathbb{Z}_p}(y) \chi_{p,t}(y) dy \\ &= \int_{\mathbb{Q}_p} \chi_{x+p^n\mathbb{Z}_p}(y) \chi_p(ty) dy \\ &= \int_{x+p^n\mathbb{Z}_p} \chi_p(ty) dy \\ &= \int_{p^n\mathbb{Z}_p} \chi_p(t(x+y)) dy \\ &= \int_{p^n\mathbb{Z}_p} \chi_p(tx+ty) dy \\ &= \int_{p^n\mathbb{Z}_p} \chi_p(tx) \chi_p(ty) dy \\ &= \chi_p(tx) \int_{p^n\mathbb{Z}_p} \chi_p(ty) dy \\ &= \chi_p(tx) \int_{\mathbb{Q}_p} \chi_{p^n\mathbb{Z}_p}(y) \chi_p(ty) dy \\ &= \chi_p(tx) \int_{\mathbb{Q}_p} \chi_{p^n\mathbb{Z}_p}(y) \chi_{p,t}(y) dy \\ &= \chi_p(tx) \widehat{\chi}_{p^n\mathbb{Z}_p}(t) \\ &= \chi_p(tx) p^{-n} \chi_{p^{-n}\mathbb{Z}_p}(t). \end{aligned}$$

16: APPLICATION Taking into account #10,

$$f \in \mathcal{B}(\mathbb{Q}_p) \Rightarrow \widehat{f} \in \mathcal{B}(\mathbb{Q}_p).$$

17: THEOREM $\forall f \in \mathbf{INV}(\mathbb{Q}_p)$,

$$\widehat{\widehat{f}} = f(-x) \quad (x \in \mathbb{Q}_p).$$

PROOF It suffices to check this for a single function, so take $f = \chi_{\mathbb{Z}_p}$ –then as noted above,

$$\widehat{\chi_{\mathbb{Z}_p}} = \chi_{\mathbb{Z}_p},$$

thus $\forall x$,

$$\widehat{\widehat{\chi_{\mathbb{Z}_p}}}(x) = \chi_{\mathbb{Z}_p}(x) = \chi_{\mathbb{Z}_p}(-x).$$

18: N.B. It is clear that

$$\mathcal{B}(\mathbb{Q}_p) \subset \mathbf{INV}(\mathbb{Q}_p).$$

19: SCHOLIUM The arrow $f \rightarrow \widehat{f}$ is a linear bijection of $\mathcal{B}(\mathbb{Q}_p)$ onto itself.

[Injectivity is manifest. As for surjectivity, the arrow $f \rightarrow \check{f}$, where

$$\check{f} = f(-x),$$

maps $\mathcal{B}(\mathbb{Q}_p)$ into itself. And

$$f = \check{\check{f}} = (\check{f})^\sim = (\check{f})^{\wedge\wedge} = ((\check{f})^\wedge)^\wedge.]$$

20: REMARK As is well-known, the same conclusion obtains if \mathbb{Q}_p is replaced by \mathbb{R} or \mathbb{C} .

Pass now from \mathbb{Q}_p to \mathbb{Q}_p^\times .

21: LEMMA Let $f \in \mathcal{B}(\mathbb{Q}_p^\times)$ –then $\exists n \in \mathbb{N}$:

$$\left\{ \begin{array}{ll} |x|_p < p^{-n} & \implies f(x) = 0 \\ |x|_p > p^n & \implies f(x) = 0 \end{array} \right. .$$

Therefore an element f of $\mathcal{B}(\mathbb{Q}_p^\times)$ can be viewed as an element of $\mathcal{B}(\mathbb{Q}_p)$ with the property that $f(0) = 0$.

22: DEFINITION Given $f \in L^1(\mathbb{Q}_p^\times, d^\times x)$, its Mellin transform \tilde{f} is the Fourier transform of f per \mathbb{Q}_p^\times :

$$\tilde{f}(\chi) = \int_{\mathbb{Q}_p^\times} f(x) \chi(x) d^\times x.$$

[Note: By definition,

$$d^\times x = \frac{p}{p-1} \frac{dx}{|x|_p} \quad (\text{c.f. } \S 6, \#26),$$

so

$$\text{vol}_{d^\times x}(\mathbb{Z}_p^\times) = \text{vol}_{dx}(\mathbb{Z}_p) = 1.]$$

23: EXAMPLE Take $f = \chi_{\mathbb{Z}_p^\times}$ —then

$$\begin{aligned} \tilde{\chi}_{\mathbb{Z}_p^\times}(\chi) &= \int_{\mathbb{Q}_p^\times} \chi_{\mathbb{Z}_p^\times}(x) \chi(x) d^\times x \\ &= \int_{\mathbb{Z}_p^\times} \chi(x) d^\times x. \end{aligned}$$

Decompose χ as in §9, #10, hence

$$\begin{aligned} \int_{\mathbb{Z}_p^\times} \chi(x) d^\times x &= \int_{\mathbb{Z}_p^\times} |x|_p^{\sqrt{-1}t} \underline{\chi}(p^{-v(x)}x) d^\times x \\ &= \int_{\mathbb{Z}_p^\times} \underline{\chi}(x) d^\times x \\ &= \begin{cases} 0 & (\underline{\chi} \neq 1) \\ 1 & (\underline{\chi} \equiv 1) \end{cases}. \end{aligned}$$

According to §9, #2, a unitary character $\chi \in \widehat{(\mathbb{Q}_p^\times)}$ is unramified if its restriction $\underline{\chi}$ to \mathbb{Z}_p^\times is trivial. Therefore the upshot is that the Mellin transform of $\chi_{\mathbb{Z}_p^\times}$ is the characteristic function of the set of unramified elements of $\widehat{(\mathbb{Q}_p^\times)}$.

APPENDIX

Let \mathbb{K} be a finite extension of \mathbb{Q}_p –then

$$\mathbb{K}^\times \approx \mathbb{Z} \times R^\times$$

and the generalities developed in §9 go through with but minor changes when \mathbb{Q}_p is replaced by \mathbb{K} .

In particular: $\forall \chi \in \widehat{K}^\times$, there is a splitting

$$\chi(a) = |a|^{\sqrt{-1} t} \underline{\chi}(\pi^{-v(a)} a),$$

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 (c.f. §5, #10) and $|\pi|_{\mathbb{K}} = \frac{1}{q}$. On the other hand, the "π" in the second instance is 3.14...

The extension of the theory from $\mathcal{B}(\mathbb{Q}_p)$ to $\mathcal{B}(\mathbb{K})$ is straightforward, the point of departure being the observation that

$$\int_{\pi^n R} \chi_{\mathbb{K},p}(a) da = \mu_{\mathbb{K}}(R) \begin{cases} q^{-n} & (n = -d, -d+1, \dots) \\ 0 & (n = -d-1, -d-2, \dots) \end{cases}.$$

2: CONVENTION Normalize the Haar measure on \mathbb{K} by stipulating that $\int_R da = q^{-d/2}$.

3: DEFINITION Given $f \in L^1(\mathbb{K})$, its Fourier transform is the function

$$\widehat{f} : \mathbb{K} \longrightarrow \mathbb{C}$$

defined by the rule

$$\begin{aligned}\widehat{f}(b) &= \int_{\mathbb{K}} f(a) \chi_{\mathbb{K},p,b}(a) da \\ &= \int_{\mathbb{K}} f(a) \chi_{\mathbb{K},p}(ab) da.\end{aligned}$$

4: THEOREM $\forall f \in \mathbf{INV}(\mathbb{K})$,

$$\widehat{\widehat{f}}(a) = f(-a) \quad (a \in \mathbb{K}).$$

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:

$$\begin{aligned}\bullet \quad \widehat{\chi_R}(b) &= \int_{\mathbb{K}} \chi_R(a) \chi_{\mathbb{K},p}(ab) da \\ &= \int_R \chi_{\mathbb{K},p}(ab) da \\ &= q^{-d/2} \chi_{\Delta_{\mathbb{K}}}(b). \\ \bullet \quad \int_{\mathbb{K}} q^{-d/2} \chi_{\Delta_{\mathbb{K}}}(b) \chi_{\mathbb{K},p}(ab) db &= q^{-d/2} \int_{\Delta_{\mathbb{K}}} \chi_{\mathbb{K},p}(ab) db \\ &= \chi_R(a) \quad (\text{loc. cit., \#13}) \\ &= \chi_R(-a).\end{aligned}$$

5: N.B. It is clear that

$$\mathcal{B}(k) \subset \mathbf{INV}(\mathbb{K}).$$

6: SCHOLIUM The arrow $f \rightarrow \widehat{f}$ is a linear bijection of $\mathcal{B}(k)$ onto itself.

7: CONVENTION Put

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

Then $d^\times a$ is a Haar measure on \mathbb{K}^\times and

$$\text{vol}_{d^\times a}(R^\times) = \text{vol}_{da}(R) = q^{-d/2}.$$

8: DEFINITION Given $f \in L^1(\mathbb{K}^\times, d^\times a)$, its Mellin transform \tilde{f} is the Fourier transform of f per \mathbb{K}^\times :

$$\tilde{f}(\chi) = \int_{\mathbb{K}^\times} f(a) \chi(a) d^\times a.$$

9: EXAMPLE Take $f = \chi_{R^\times}$ -then

$$\tilde{\chi}_{R^\times}(\chi) = \begin{cases} 0 & (\chi \neq 1) \\ q^{-d/2} & (\chi \equiv 1) \end{cases}.$$

§11. LOCAL ZETA FUNCTIONS: \mathbb{R}^\times or \mathbb{C}^\times

We shall first consider \mathbb{R}^\times , hence $\widetilde{\mathbb{R}}^\times \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{C}$ and every character has the form

$$\chi(x) \equiv \chi_{\sigma,s}(x) = (\operatorname{sgn} x)^\sigma |x|^s \quad (\sigma \in \{0,1\}, s \in \mathbb{C}) \quad (\text{cf. §7, \#11}).$$

1: DEFINITION Given $f \in \mathcal{S}(\mathbb{R}^n)$ and a character $\chi : \mathbb{R}^\times \rightarrow \mathbb{C}^\times$, the local zeta function attached to the pair (f, χ) is

$$Z(f, \chi) = \int_{\mathbb{R}^\times} f(x) \chi(x) d^\times x, \quad \text{where } d^\times x = \frac{dx}{|x|}.$$

[Note: The parameters σ and s are implicit:

$$Z(f, x) \equiv Z(f, \chi_{\sigma,s}).]$$

2: LEMMA The integral defining $Z(f, \chi)$ is absolutely convergent for $\Re(s) > 0$.

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

$$\begin{aligned} |Z(f, \chi)| &\leq \int_{\mathbb{R}-\{0\}} |f(x)| |x|^{\Re(s)-1} dx \\ &\leq \left(\int_{\mathbb{R}-I} + \int_I \right) |f(x)| |x|^{\Re(s)-1} dx \\ &\leq M + C \int_I |x|^{\Re(s)-1} dx, \end{aligned}$$

a finite quantity.

3: LEMMA $Z(f, \chi)$ is a holomorphic function of s in the strip $\Re(s) > 0$.

[Formally,

$$\frac{d}{ds} Z(f, \chi) = \int_{\mathbb{R}^\times} f(x) (\operatorname{sgn} x)^\sigma (\log |x|) |x|^s d^\times x,$$

and while correct, "differentiation under the integral sign" does require a formal proof]

4: NOTATION Put

$$\tilde{\chi} = \chi^{-1} \|\cdot\|.$$

The integral defining $Z(f, \tilde{\chi})$ is absolutely convergent if $\Re(1-s) > 0$, i.e., if $1 - \Re(s) > 0$ or still, if $\Re(s) < 1$.

5: LEMMA Let $f, g \in \mathcal{S}(\mathbb{R})$ and suppose that $0 < \Re(s) < 1$ –then

$$Z(f, \chi)Z(\hat{g}, \tilde{\chi}) = Z(\hat{f}, \tilde{\chi})Z(g, \chi)$$

PROOF Write

$$Z(f, \chi)Z(\hat{g}, \tilde{\chi}) = \int \int_{\mathbb{R}^\times \times \mathbb{R}^\times} f(x)\hat{g}(y)\chi(xy^{-1})|y|d^\times x d^\times y$$

and make the substitution $t = yx^{-1}$ to get

$$Z(f, \chi)Z(\hat{g}, \tilde{\chi}) = \int_{\mathbb{R}^\times} \left(\int_{\mathbb{R}^\times} f(x)\hat{g}(tx)|x|d^\times x \right) \chi(t^{-1})|t|d^\times t.$$

The claim now is that the inner integral is symmetric in f and g (which then implies that

$$Z(f, \chi)Z(\hat{g}, \tilde{\chi}) = Z(g, \chi)Z(\hat{f}, \tilde{\chi}),$$

the desired equality). To see this is so, observe first that

$$|x|du \cdot d^\times x = |u|dx \cdot d^\times u.$$

Since \mathbb{R}^\times and \mathbb{R} differ by a single element, it therefore follows that

$$\begin{aligned} \int_{\mathbb{R}^\times} f(x)\hat{g}(tx)|x|d^\times x &= \int_{\mathbb{R}^\times} f(x)|x| \left(\int_{\mathbb{R}} g(u)e^{2\pi\sqrt{-1}txu}du \right) d^\times x \\ &= \int \int_{\mathbb{R} \times \mathbb{R}^\times} f(x)g(u)|x|e^{2\pi\sqrt{-1}txu}dud^\times x \end{aligned}$$

$$\begin{aligned}
&= \int_{\mathbb{R}^\times} g(u) |u| \left(\int_{\mathbb{R}} f(x) e^{2\pi\sqrt{-1} \, txu} dx \right) d^\times u \\
&= \int_{\mathbb{R}^\times} g(u) \widehat{f}(tu) |u| d^\times u.
\end{aligned}$$

Fix $\phi \in \mathcal{S}(\mathbb{R})$ and put

$$\rho(\chi) = \frac{Z(\phi, \chi)}{Z(\widehat{\phi}, \widetilde{\chi})}$$

Then $\rho(\chi)$ is independent of the choice of ϕ and $\forall f \in \mathcal{S}(\mathbb{R})$, the functional equation

$$Z(f, \chi) = \rho(\chi) Z(\widehat{f}, \widetilde{\chi})$$

obtains.

6: LEMMA $\rho(\chi)$ is a meromorphic function of s (cf. infra).

7: APPLICATION $\forall f \in \mathcal{S}(\mathbb{R})$, $Z(f, \chi)$ admits a meromorphic continuation to the whole s -plane.

8: NOTATION Set

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2).$$

9: DEFINITION Write

$$L(\chi) = \begin{cases} \Gamma_{\mathbb{R}}(s) & (\sigma = 0) \\ \Gamma_{\mathbb{R}}(s+1) & (\sigma = 1) \end{cases}.$$

Proceeding to the computation of $\rho(\chi)$, distinguish two cases.

- $\sigma = 0$ Take $\phi_0(x)$ to be $e^{-\pi x^2}$ —then

$$Z(\phi_0, \chi) = \int_{\mathbb{R}^\times} e^{-\pi x^2} |x|^s d^\times x$$

$$\begin{aligned}
&= 2 \int_0^\infty e^{-\pi x^2} x^{s-1} dx \\
&= \pi^{-s/2} \Gamma(s/2) \\
&= \Gamma_{\mathbb{R}}(s) \\
&= L(\chi).
\end{aligned}$$

Next $\widehat{\phi}_0 = \phi_0$ (cf. §10, #2) so by the above argument,

$$Z(\widehat{\phi}_0, \check{\chi}) = L(\check{\chi}),$$

from which

$$\begin{aligned}
\rho(\chi) &= \frac{L(\chi)}{L(\check{\chi})} \\
&= \frac{\pi^{-s/2} \Gamma(\frac{s}{2})}{\pi^{-(1-s)/2} \Gamma(\frac{1-s}{2})} \\
&= 2^{1-s} \pi^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s).
\end{aligned}$$

- $\sigma = 1$ Take $\phi_1(x)$ to be $x e^{-\pi x^2}$ –then

$$\begin{aligned}
Z(\phi_1, \chi) &= \int_{\mathbb{R}^\times} x e^{-\pi x^2} \frac{x}{|x|} |x|^s d^\times x \\
&= \int_{\mathbb{R}^\times} e^{-\pi x^2} |x|^{s+1} d^\times x \\
&= 2 \int_0^\infty e^{-\pi x^2} x^s dx \\
&= \pi^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right) \\
&= \Gamma_{\mathbb{R}}(s+1) \\
&= L(\chi).
\end{aligned}$$

Next

$$\widehat{\phi}_1(t) = \sqrt{-1} \, t \exp(-\pi t^2) \quad (\text{cf. §10, #2}).$$

Therefore

$$\begin{aligned}
Z(\widehat{\phi_1}, \check{\chi}) &= \sqrt{-1} \int_{\mathbb{R}^\times} x e^{-\pi x^2} \frac{x}{|x|} |x|^{1-s} d^\times x \\
&= \sqrt{-1} \int_{\mathbb{R}^\times} e^{-\pi x^2} |x|^{2-s} d^\times x \\
&= \sqrt{-1} 2 \int_0^\infty e^{-\pi x^2} x^{1-s} dx \\
&= \sqrt{-1} \pi^{-(2-s)/2} \Gamma\left(\frac{2-s}{2}\right) \\
&= \sqrt{-1} \Gamma_{\mathbb{R}}(2-s) \\
&= \sqrt{-1} L(\check{\chi}).
\end{aligned}$$

Accordingly

$$\begin{aligned}
\rho(\chi) &= -\sqrt{-1} \frac{L(\chi)}{L(\check{\chi})} \\
&= -\sqrt{-1} \frac{\pi^{-(s+1)/2} \Gamma\left(\frac{s+1}{2}\right)}{\pi^{(s-2)/2} \Gamma\left(\frac{2-s}{2}\right)} \\
&= -\sqrt{-1} 2^{1-s} \pi^{-s} \sin\left(\frac{\pi s}{2}\right) \Gamma(s).
\end{aligned}$$

10: FACT

$$\begin{cases} \frac{\zeta(1-s)}{\zeta(s)} = 2^{1-s} \pi^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s) \\ \frac{\zeta(s)}{\zeta(1-s)} = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \end{cases}.$$

To recapitulate: $\rho(\chi)$ is a meromorphic function of s and

$$\rho(\chi) = \epsilon(\chi) \frac{L(\chi)}{L(\check{\chi})},$$

where

$$\epsilon(\chi) = \begin{cases} 1 & (\sigma = 0) \\ -\sqrt{-1} & (\sigma = 1) \end{cases}.$$

Having dealt with \mathbb{R}^\times , let us now turn to \mathbb{C}^\times , hence $\widetilde{\mathbb{C}}^\times \approx \mathbb{Z} \times \mathbb{C}$ and every character has the form

$$\chi(x) \equiv \chi_{n,s}(x) = \exp(\sqrt{-1} \, n \, \arg x) |x|^s \quad (n \in \mathbb{Z}, \, s \in \mathbb{C}) \quad (\text{cf. } \S 7, \, \#12).$$

Here, however, it will be best to make a couple of adjustments.

1. Replace x by z .
2. Replace $|\cdot|$ by $|\cdot|_{\mathbb{C}}$, the normalized absolute value, so

$$|z|_{\mathbb{C}} = |z\bar{z}| = |z|^2 \quad (\text{cf. } \S 6, \, \#15).$$

11: DEFINITION Given $f \in \mathcal{S}(\mathbb{C}) (= \mathcal{S}(\mathbb{R}^2))$ and a character $\chi : \mathbb{C}^\times \rightarrow \mathbb{C}^\times$, the local zeta function attached to the pair (f, χ) is

$$Z(f, \chi) = \int_{\mathbb{C}^\times} f(z) \chi(z) d^\times z,$$

where $d^\times z = \frac{|dz \wedge d\bar{z}|}{|z|_{\mathbb{C}}}.$

[Note: The parameters n and s are implicit:

$$Z(f, \chi) \equiv Z(f, \chi_{n,s}).]$$

12: NOTATION Put

$$\check{\chi} = \chi^{-1} |\cdot|_{\mathbb{C}}.$$

The analogs of #2 and #3 are immediate, as is the analog of #5 (just replace \mathbb{R}^\times by \mathbb{C}^\times and $|\cdot|$ by $|\cdot|_{\mathbb{C}}$), the crux then being the analog of #6.

13: NOTATION Set

$$\Gamma_{\mathbb{C}}(s) = (2\pi)^{1-s}\Gamma(s).$$

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

$$\rho(\chi) = \frac{Z(\phi, \chi)}{Z(\widehat{\phi}, \widetilde{\chi})},$$

let

$$\phi_n(z) = \begin{cases} \bar{z}^n e^{-2\pi|z|^2} & (n \geq 0) \\ z^{-n} e^{-2\pi|z|^2} & (n < 0) \end{cases}.$$

Then

$$\widehat{\phi}_n = \sqrt{-1}^{|n|} \phi_{-n} \quad (\text{cf. §10, \#3}).$$

15: N.B. In terms of polar coordinates $z = r e^{\sqrt{-1} \theta}$,

- $\phi_n(z) = r^{|n|} \exp(-2\pi r^2 - \sqrt{-1} n\theta)$
- $d^{\times} z = \frac{2r dr d\theta}{r^2} = \frac{2}{r} dr d\theta$
- $\chi(z) = e^{\sqrt{-1} n\theta} |z|_{\mathbb{C}}^s = e^{\sqrt{-1} n\theta} r^{2s}.$

Therefore

$$Z(\phi_n, \chi) = \int_0^{2\pi} \int_0^{\infty} r^{|n|} \exp(-2\pi r^2 - \sqrt{-1} n\theta) e^{\sqrt{-1} n\theta} r^{2s} \frac{2}{r} dr d\theta$$

$$\begin{aligned}
&= \int_0^{2\pi} \int_0^\infty r^{2(s-1)+|n|} \exp(-2\pi r^2) 2r dr d\theta \\
&= 2\pi \int_0^\infty t^{(s-1)+|n|/2} \exp(-2\pi t) dt \\
&= (2\pi)^{1-s-|n|/2} \Gamma\left(s + \frac{|n|}{2}\right) \\
&= \Gamma_{\mathbb{C}}\left(s + \frac{|n|}{2}\right) \\
&= L(\chi)
\end{aligned}$$

and

$$\begin{aligned}
Z(\widehat{\phi}_n, \check{\chi}) &= Z((\sqrt{-1})^{|n|} \phi_{-n}, \check{\chi}) \\
&= (\sqrt{-1})^{|n|} (2\pi)^{1-(1-s)-|n|/2} \Gamma\left(1-s + \frac{|n|}{2}\right) \\
&= (\sqrt{-1})^{|n|} (2\pi)^{s-|n|/2} \Gamma\left(1-s + \frac{|n|}{2}\right) \\
&= (\sqrt{-1})^{|n|} \Gamma_{\mathbb{C}}\left(1-s + \frac{|n|}{2}\right) \\
&= (\sqrt{-1})^{|n|} L(\check{\chi}).
\end{aligned}$$

Consequently,

$$\begin{aligned}
\rho(\chi) &= \frac{Z(\phi_n, \chi)}{Z(\widehat{\phi}_n, \check{\chi})} \\
&= (\sqrt{-1})^{-|n|} \frac{L(\chi)}{L(\check{\chi})} \\
&= \epsilon(\chi) \frac{L(\chi)}{L(\check{\chi})},
\end{aligned}$$

where

$$\epsilon(\chi) = (\sqrt{-1})^{-|n|}.$$

And

$$\frac{L(\chi)}{L(\tilde{\chi})} = (2\pi)^{1-2s} \frac{\Gamma(s + \frac{|n|}{2})}{\Gamma(1 - s + \frac{|n|}{2})}.$$

§12. LOCAL ZETA FUNCTIONS: \mathbb{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 $f \in \mathcal{B}(\mathbb{Q}_p)$ and a character $\chi : \mathbb{Q}_p^\times \rightarrow \mathbb{C}^\times$, the local zeta function attached to the pair (f, χ) is

$$Z(f, \chi) = \int_{\mathbb{Q}_p^\times} f(x) \chi(x) d^\times x,$$

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 $\Re(s) > 0$.

PROOF It suffices to check the absolute convergence for $f = \chi_{p^n \mathbb{Z}_p}$ (cf. §10, #10) and then we might just as well take $n = 0$:

$$\begin{aligned} |Z(f, \chi)| &\leq \int_{\mathbb{Q}_p^\times} |f(x)| |x|_p^{\Re(s)} d^\times x \\ &= \int_{\mathbb{Q}_p^\times} \chi_{\mathbb{Z}_p}(x) |x|_p^{\Re(s)} d^\times x \\ &= \int_{\mathbb{Z}_p - \{0\}} |x|_p^{\Re(s)} d^\times x \\ &= \frac{1}{1 - p^{-\Re(s)}} \quad (\text{cf. §6, #27}). \end{aligned}$$

3: LEMMA $Z(f, \chi)$ is a holomorphic function of s in the strip $\Re(s) > 0$.

4: NOTATION Put

$$\tilde{x} = x^{-1} |\cdot|_p.$$

The integral defining $Z(f, \tilde{\chi})$ is absolutely convergent if $\Re(1-s) > 0$, i.e., if $1-\Re(s) > 0$ or still, if $\Re(s) < 1$.

5: LEMMA Let $f, g \in \mathcal{B}(\mathbb{Q}_p)$ and suppose that $0 < \Re(s) < 1$ –then

$$Z(f, \chi)Z(\hat{g}, \tilde{\chi}) = Z(\hat{f}, \tilde{\chi})Z(g, \chi).$$

[Simply follow verbatim the argument employed in §11, #5.]

Fix $\phi \in \mathcal{B}(\mathbb{Q}_p)$ and put

$$\rho(\chi) = \frac{Z(\phi, \chi)}{Z(\hat{\phi}, \tilde{\chi})}.$$

Then $\rho(\chi)$ is independent of the choice of ϕ and $\forall f \in \mathcal{B}(\mathbb{Q}_p)$, the functional equation

$$Z(f, \chi) = \rho(\chi)Z(\hat{f}, \tilde{\chi})$$

obtains.

6: LEMMA $\rho(\chi)$ is a meromorphic function of s (cf. infra).

7: APPLICATION $\forall f \in \mathcal{B}(\mathbb{Q}_p)$, $Z(f, \chi)$ admits a meromorphic continuation to the whole s -plane

8: 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 $\phi_0(x) = \chi_p(x)\chi_{\mathbb{Z}_p}(x)$:

$$Z(\phi_0, \chi) = \int_{\mathbb{Q}_p^\times} \phi_0(x)\chi(x)d^\times x$$

$$\begin{aligned}
&= \int_{\mathbb{Q}_p^\times} \chi_p(x) \chi_{\mathbb{Z}_p}(x) |x|_p^s d^\times x \\
&= \int_{\mathbb{Z}_p - \{0\}} \chi_p(x) |x|_p^s d^\times x \\
&= \int_{\mathbb{Z}_p - \{0\}} |x|_p^s d^\times x \\
&= \frac{1}{1 - p^{-s}} \quad (\text{cf. §6, \#27}) \\
&= \frac{1}{1 - |p|_p^s} \\
&= \frac{1}{1 - \chi(p)} \\
&= L(\chi).
\end{aligned}$$

To finish the determination, it is necessary to explicate the Fourier transform $\widehat{\phi}_0$ of ϕ_0 (cf. §10, #11) :

$$\begin{aligned}
\widehat{\phi}_0(t) &= \int_{\mathbb{Q}_p} \phi_0(x) \chi_p(tx) dx \\
&= \int_{\mathbb{Q}_p} \chi_p(x) \chi_{\mathbb{Z}_p}(x) \chi_p(tx) dx \\
&= \int_{\mathbb{Z}_p} \chi_p(x) \chi_p(tx) dx \\
&= \int_{\mathbb{Z}_p} \chi_p((1+t)x) dx \\
&= \chi_{\mathbb{Z}_p}(t).
\end{aligned}$$

Therefore

$$\begin{aligned}
Z(\widehat{\phi}_0, \check{\chi}) &= \int_{\mathbb{Q}_p^\times} \widehat{\phi}_0(x) \check{\chi}(x) d^\times x \\
&= \int_{\mathbb{Q}_p^\times} \chi_{\mathbb{Z}_p}(x) |x|_p^{1-s} d^\times x \\
&= \int_{\mathbb{Z}_p - \{0\}} |x|_p^{1-s} d^\times x
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{1 - p^{-(1-s)}} \quad (\text{cf. §6, \#27}) \\
&= \frac{1}{1 - |p|_p^{1-s}} \\
&= \frac{1}{1 - \tilde{\chi}(p)} \\
&= L(\tilde{\chi}).
\end{aligned}$$

And finally

$$\rho(\chi) = \frac{Z(\phi_0, \chi)}{Z(\widehat{\phi}, \tilde{\chi})} = \frac{L(\chi)}{L(\tilde{\chi})}$$

or still,

$$\rho(\chi) = \frac{1 - p^{-(1-s)}}{1 - p^{-s}}.$$

9: 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 $\phi_n(x) = \chi_p(x) \chi_{p^{-n}\mathbb{Z}_p}(x)$:

$$\begin{aligned}
Z(\phi_n, \chi) &= \int_{\mathbb{Q}_p^\times} \phi_n(x) \chi(x) d^\times x \\
&= \int_{\mathbb{Q}_p^\times} \chi_p(x) \chi_{p^{-n}\mathbb{Z}_p}(x) |x|_p^s \underline{\chi}(x) d^\times x \\
&= \int_{p^{-n}\mathbb{Z}_p - \{0\}} \chi_p(x) |x|_p^s \underline{\chi}(x) d^\times x \\
&= \sum_{k=-n}^{\infty} \int_{\mathbb{Z}_p^\times} \chi_p(p^k u) \left| p^k u \right|_p^s \underline{\chi}(u) d^\times u
\end{aligned}$$

$$= \sum_{k=-n}^{\infty} p^{-ks} \int_{\mathbb{Z}_p^\times} \chi_p(p^k u) \underline{\chi}(u) d^\times u.$$

10: LEMMA If $|v|_p \neq p^n$, then

$$\int_{\mathbb{Z}_p^\times} \chi_p(vu) \underline{\chi}(u) d^\times u = 0.$$

Since $|p^k|_p = p^{-k}$, $Z(\phi_n, \chi)$ reduces to

$$p^{ns} \int_{\mathbb{Z}_p^\times} \chi_p(p^{-n}u) \underline{\chi}(u) d^\times u.$$

Let $E = \{e_i : i \in I\}$ be a system of coset representatives for $\mathbb{Z}_p^\times / U_{p,n}$ —then by assumption, $\underline{\chi}$ is constant on the cosets mod $U_{p,n}$, hence

$$\int_{\mathbb{Z}_p^\times} \chi_p(p^{-n}u) \underline{\chi}(u) d^\times u = \sum_{i=1}^r \underline{\chi}(e_i) \int_{e_i U_{p,n}} \chi_p(p^{-n}u) d^\times u.$$

But

$$u \in e_i U_{p,n} \implies p^{-n}u \in p^{-n}e_i + \mathbb{Z}_p$$

\implies

$$\begin{aligned} \chi_p(p^{-n}u) &= \chi_p(p^{-n}e_i + x) \quad (x \in \mathbb{Z}_p) \\ &= \chi_p(p^{-n}e_i). \end{aligned}$$

Therefore

$$\begin{aligned} \int_{\mathbb{Z}_p^\times} \chi_p(p^{-n}u) \underline{\chi}(u) d^\times u &= \sum_{i=1}^r \underline{\chi}(e_i) \chi_p(p^{-n}e_i) \int_{e_i U_{p,n}} d^\times u \\ &= \tau(\chi) \int_{U_{p,n}} d^\times u \end{aligned}$$

if

$$\tau(\chi) = \sum_{i=1}^r \underline{\chi}(e_i) \chi_p(p^{-n} e_i).$$

And

$$\begin{aligned} \int_{U_{p,n}} d^\times u &= \int_{1+p^n \mathbb{Z}_p} d^\times u \\ &= \frac{p}{p-1} \int_{1+p^n \mathbb{Z}_p} \frac{du}{|u|_p} \\ &= \frac{p}{p-1} \int_{1+p^n \mathbb{Z}_p} du \\ &= \frac{p}{p-1} \int_{p^n \mathbb{Z}_p} du \\ &= \frac{p}{p-1} p^{-n} \\ &= \frac{p^{1-n}}{p-1}. \end{aligned}$$

So in the end

$$Z(\phi_n, \chi) = \tau(\chi) \frac{p^{1+n(s-1)}}{p-1}.$$

Next

$$\begin{aligned} \widehat{\phi}_n(t) &= \int_{\mathbb{Q}_p} \phi_n(x) \chi_p(tx) dx \\ &= \int_{\mathbb{Q}_p} \chi_p(x) \chi_{p^{-n} \mathbb{Z}_p}(x) \chi_p(tx) dx \\ &= \int_{p^{-n} \mathbb{Z}_p} \chi_p(x) \chi_p(tx) dx \\ &= \int_{p^{-n} \mathbb{Z}_p} \chi_p((1+t)x) dx \\ &= \text{vol}_{dx}(p^{-n} \mathbb{Z}_p) \chi_{p^n \mathbb{Z}_p-1}(t) \\ &= p^n \chi_{p^n \mathbb{Z}_p-1}(t). \end{aligned}$$

Therefore

$$\begin{aligned}
Z(\widehat{\phi}_n, \widetilde{\chi}) &= \int_{\mathbb{Q}_p^\times} \widehat{\phi}_n(x) \widetilde{\chi}(x) d^\times x \\
&= \int_{\mathbb{Q}_p^\times} p^n \chi_{p^n \mathbb{Z}_p - 1}(x) \chi^{-1}(x) |x|_p d^\times x \\
&= p^n \int_{p^n \mathbb{Z}_p - 1} \overline{\chi(x)} |x|_p^{1-s} d^\times x \\
&= p^n \int_{p^n \mathbb{Z}_p - 1} \overline{\chi(x)} d^\times x \\
&= p^n \int_{1+p^n \mathbb{Z}_p} \overline{\chi(-x)} d^\times x \\
&= p^n \overline{\chi(-1)} \int_{1+p^n \mathbb{Z}_p} \overline{\chi(x)} d^\times x \\
&= p^n \chi(-1) \int_{U_{p,n}} d^\times x \\
&= p^n \chi(-1) \frac{p^{1-n}}{p-1} \\
&= \frac{p}{p-1} \chi(-1).
\end{aligned}$$

[Note: $\chi(-1) = \pm 1$:

$$1 = (-1)(-1) \implies 1 = \chi(-1)\chi(-1) = \chi(-1)^2.]$$

Assembling the data then gives

$$\begin{aligned}
\rho(\chi) &= \frac{Z(\phi_n, \chi)}{Z(\widehat{\phi}_n, \widetilde{\chi})} \\
&= \frac{\tau(\chi) \frac{p^{1+n(s-1)}}{p-1}}{\frac{p}{p-1} \chi(-1)} \\
&= \tau(\chi) \frac{p^{1+n(s-1)}}{p-1} \frac{p-1}{p\chi(-1)} \\
&= \tau(\chi) \chi(-1) p^{n(s-1)}
\end{aligned}$$

$$\begin{aligned}
&= \tau(\chi)\chi(-1)p^{n(s-1)}\frac{1}{1} \\
&= \tau(\chi)\chi(-1)p^{n(s-1)}\frac{L(\chi)}{L(\tilde{\chi})}.
\end{aligned}$$

11: THEOREM

$$\rho(\chi) = \epsilon(\chi) \frac{L(\chi)}{L(\tilde{\chi})}, \quad \text{where } \epsilon(\chi) = \begin{cases} 1 & \text{if } \chi \text{ is unramified} \\ \rho(\chi) & \text{if } \chi \text{ is ramified of degree } n \geq 1. \end{cases}$$

12: LEMMA Suppose that χ is ramified of degree $n \geq 1$ –then

$$\epsilon(\chi)\epsilon(\tilde{\chi}) = \chi(-1).$$

PROOF $\forall f \in \mathcal{B}(\mathbb{Q}_p)$,

$$\begin{aligned}
Z(f, \chi) &= \epsilon(\chi)Z(\hat{f}, \tilde{\chi}) \\
&= \epsilon(\chi)\epsilon(\tilde{\chi})Z(\hat{\hat{f}}, \tilde{\tilde{\chi}}).
\end{aligned}$$

But $\tilde{\tilde{\chi}} = \chi$, hence

$$\begin{aligned}
Z(\hat{\hat{f}}, \tilde{\tilde{\chi}}) &= \int_{\mathbb{Q}_p^\times} \hat{\hat{f}}(x)\chi(x)d^\times x \\
&= \int_{\mathbb{Q}_p^\times} f(-x)\chi(x)d^\times x \\
&= \int_{\mathbb{Q}_p^\times} f(x)\chi(-x)d^\times x \\
&= \chi(-1) \int_{\mathbb{Q}_p^\times} f(x)\chi(x)d^\times x \\
&= \chi(-1)Z(f, \chi).
\end{aligned}$$

13: APPLICATION

$$\tau(\chi)\tau(\tilde{\chi}) = p^n\chi(-1).$$

[In fact,

$$\begin{aligned}
\epsilon(\chi)\epsilon(\tilde{\chi}) &= \tau(\chi)p^{n(s-1)}\chi(-1)\tau(\tilde{\chi})p^{n(1-s-1)}\tilde{\chi}(-1) \\
&= \tau(\chi)\tau(\tilde{\chi})p^{-n} \\
&= \chi(-1)
\end{aligned}$$

\implies

$$\tau(\chi)\tau(\tilde{\chi}) = p^n\chi(-1).]$$

14: LEMMA Suppose that χ is ramified of degree $n \geq 1$ –then

$$\epsilon(\bar{\chi}) = \chi(-1)\overline{\epsilon(\chi)}.$$

PROOF $\forall f \in \mathcal{B}(\mathbb{Q}_p)$,

$$\begin{aligned}
Z(\widehat{f}, \chi) &= \int_{\mathbb{Q}_p^\times} \widehat{f}(x)\chi(x)d^\times x \\
&= \int_{\mathbb{Q}_p^\times} \overline{\widehat{f}(-x)}\chi(x)d^\times x \quad (\text{cf. §10, #12}) \\
&= \int_{\mathbb{Q}_p^\times} \widehat{\overline{f}}(x)\chi(-x)d^\times x \\
&= \chi(-1) \int_{\mathbb{Q}_p^\times} \widehat{f}(x)\chi(x)d^\times x \\
&= \chi(-1)Z(\widehat{f}, \chi).
\end{aligned}$$

But $\tilde{\tilde{\chi}} = \bar{\chi}$, hence

$$\begin{aligned}
\overline{Z(f, \chi)} &= Z(\bar{f}, \bar{\chi}) \\
&= \epsilon(\bar{\chi})Z(\widehat{\bar{f}}, \tilde{\tilde{\chi}}) \\
&= \epsilon(\bar{\chi})Z(\widehat{\bar{f}}, \bar{\chi}) \\
&= \epsilon(\bar{\chi})\chi(-1)Z(\widehat{\bar{f}}, \bar{\chi}) \\
&= \epsilon(\bar{\chi})\chi(-1)\overline{Z(\widehat{f}, \chi)}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}\overline{Z(f, \chi)} &= \overline{\epsilon(\chi) Z(\widehat{f}, \check{\chi})} \\ &= \overline{\epsilon(\chi)} \overline{Z(\widehat{f}, \check{\chi})}.\end{aligned}$$

Therefore

$$\begin{aligned}\epsilon(\overline{\chi}) \chi(-1) &= \overline{\epsilon(\chi)} \\ \implies \\ \epsilon(\overline{\chi}) &= \chi(-1) \overline{\epsilon(\chi)}.\end{aligned}$$

15: APPLICATION

$$\tau(\overline{\chi}) = \chi(-1) \overline{\tau(\chi)}.$$

[In fact,

$$\begin{aligned}\epsilon(\overline{\chi}) &= \tau(\overline{\chi}) p^{n(\overline{s}-1)} \overline{\chi}(-1) \\ &= \chi(-1) \overline{\epsilon(\chi)} \\ &= \chi(-1) \overline{\tau(\chi)} p^{n(\overline{s}-1)} \overline{\chi(-1)} \\ &= \chi(-1) \overline{\tau(\chi)} p^{n(\overline{s}-1)} \overline{\chi}(-1) \\ \implies \\ \tau(\overline{\chi}) &= \chi(-1) \overline{\tau(\chi)}.\end{aligned}$$

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

$$W(\underline{\chi}) = \epsilon(| \cdot |_p^{1/2} \underline{\chi}).$$

[Note: If $\underline{\chi}$ is trivial, then $W(\underline{\chi}) = 1$.]

17: LEMMA

$$|W(\underline{\chi})| = 1.$$

PROOF Put $\chi = |\cdot|_p^{1/2} \underline{\chi}$ -then

$$\epsilon(\chi)\epsilon(\tilde{\chi}) = \chi(-1) \quad (\text{cf. \#12})$$

\Rightarrow

$$\begin{aligned} \epsilon(\chi)^{-1} &= \epsilon(\tilde{\chi})\chi(-1)^{-1} \\ &= \epsilon(\tilde{\chi})\chi(-1) \\ &= \epsilon(\bar{\chi})\chi(-1) \quad (\tilde{\chi} = \bar{\chi}) \\ &= \chi(-1)\overline{\epsilon(\chi)}\chi(-1) \quad (\text{cf. \#14}) \\ &= \chi(-1)^2 \overline{\epsilon(\chi)} \\ &= \overline{\epsilon(\chi)}. \end{aligned}$$

\Rightarrow

$$|\epsilon(\chi)| = 1 \implies |W(\underline{\chi})| = 1.$$

18: APPLICATION

$$\left| \tau(|\cdot|_p^{1/2} \chi) \right| = p^{n/2}.$$

[In fact,

$$1 = |W(\underline{\chi})| = \left| \tau(|\cdot|_p^{1/2} \underline{\chi}) p^{n(\frac{1}{2}-1)} \right|.$$

19: EXERCISE AD LIBITUM Show that the theory expounded above for \mathbb{Q}_p can be carried over to any finite extension \mathbb{K} of \mathbb{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

$$\prod_{i \in I} (X_i : K_i) \approx \left(\prod_{i \in I_1} (X_i : K_i) \right) \times \left(\prod_{i \in I_2} (X_i : K_i) \right),$$

the restricted product topology on the left being the product topology on the right.

8: LEMMA The inclusion $\prod_{i \in I} (X_i : K_i) \hookrightarrow \prod_{i \in I} X_i$ 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.

11: NOTATION

$$G = \prod_{i \in I} (G_i : K_i).$$

12: LEMMA G is a locally compact abelian group.

Given $i \in I$, there is a canonical arrow

$$\begin{aligned} \text{in}_i : G_i &\rightarrow G \\ x &\mapsto (\cdots, 1, 1, x, 1, 1, \cdots). \end{aligned}$$

13: 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 $\chi|K_i \equiv 1$ 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

$$K_i^\perp = \{\chi_i \in \hat{G}_i : \chi|K_i \equiv 1\} \quad (\text{cf. §7, \#32})$$

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

$$\hat{K}_i \approx \hat{G}/K_i^\perp, \quad K_i^\perp \approx \widehat{G/K_i}.$$

Then

- K_i compact $\implies \hat{K}_i$ discrete $\implies \hat{G}/K_i^\perp$ discrete $\implies K_i^\perp$ open.
- K_i open $\implies G/K_i$ discrete $\implies \widehat{G/K_i}$ compact $\implies K_i^\perp$ compact.]

Let μ_i be the Haar measure on G_i normalized by the condition

$$\mu_i(K_i) = 1.$$

16: 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.

17: 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 $\widehat{f}_i = \chi_{K_i^\perp}$. Setting

$$f = \prod_{i \in I} f_i,$$

it thus follow that $\forall \chi \in \widehat{G}$,

$$\widehat{f}(\chi) = \prod_{i \in I} \widehat{f}_i(\chi_i).$$

Working within the framework of §7, #45, let $\mu_{\widehat{G}_i}$ be the Haar measure on \widehat{G}_i per Fourier inversion.

20: LEMMA

$$\mu_{\widehat{G}_i}(K_i^\perp) = 1.$$

PROOF Since $\chi_{K_i} \in \mathbf{INV}(G_i)$, $\forall x_i \in G_i$,

$$\begin{aligned}\chi_{K_i}(x_i) &= \int_{\widehat{G}_i} \widehat{\chi}_{K_i}(x_i) \overline{\chi_i(x_i)} d\mu_{\widehat{G}_i}(\chi_i) \\ &= \int_{K_i^\perp} \overline{\chi_i(x_i)} d\mu_{\widehat{G}_i}(\chi_i).\end{aligned}$$

Now set $x_i = 1$ to get

$$\begin{aligned}1 &= \int_{K_i^\perp} d\mu_{\widehat{G}_i}(\chi_i) \\ &= \mu_{\widehat{G}_i}(K_i^\perp).\end{aligned}$$

Let $\mu_{\widehat{G}}$ be the Haar measure on \widehat{G} constructed as in #16 (i.e., replace G by \widehat{G} , bearing in mind #20).

21: LEMMA $\mu_{\widehat{G}}$ is the Haar measure on \widehat{G} figuring in the Fourier inversion per μ_G .

PROOF Take

$$f = \prod_{i \in I} f_i,$$

where $f_i = \chi_{K_i}$ (cf. #19) –then

$$\begin{aligned}\int_{\widehat{G}} \widehat{f}(\chi) \overline{\chi(x)} d\mu_{\widehat{G}}(\chi) &= \prod_{i \in I} \int_{\widehat{G}_i} \widehat{f}_i(\chi_i) \overline{\chi_i(x_i)} d\mu_{\widehat{G}_i}(\chi_i) \\ &= \prod_{i \in I} f_i(x_i) \\ &= f(\{x_i\}) \\ &= f(x).\end{aligned}$$

§14. ADELES AND IDELES

1: DEFINITION The set of finite adeles is the restricted product

$$\mathbb{A}_{\text{fin}} = \prod_p (\mathbb{Q}_p : \mathbb{Z}_p).$$

2: DEFINITION The set of adeles is the product

$$\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{R}.$$

3: LEMMA \mathbb{A} is a locally compact abelian group (under addition).

4: N.B. \mathbb{A} is a subring of $\prod_p \mathbb{Q}_p \times \mathbb{R}$.

The image of the diagonal map

$$\mathbb{Q} \rightarrow \prod_p \mathbb{Q}_p \times \mathbb{R}$$

lies in \mathbb{A} , so \mathbb{Q} can be regarded as a subring of \mathbb{A} .

5: LEMMA \mathbb{Q} is a discrete subspace of \mathbb{A} .

PROOF To establish the discreteness of $\mathbb{Q} \subset \mathbb{A}$, one need only exhibit a neighborhood U of 0 in \mathbb{A} such that $\mathbb{Q} \cap U = \{0\}$. To this end, consider

$$U = \prod_p \mathbb{Z}_p \times]-\frac{1}{2}, \frac{1}{2}[.$$

If $x \in \mathbb{Q} \cap U$, then $|x|_p \leq 1 \ \forall p$. But $\bigcap_p (\mathbb{Q} \cap \mathbb{Z}_p) = \mathbb{Z}$, so $x \in \mathbb{Z}$. 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 \mathbb{A}/\mathbb{Q} is a compact Hausdorff space.

PROOF Since $\mathbb{Q} \subset \mathbb{A}$ is a discrete subgroup, \mathbb{Q} must be closed in \mathbb{A} and the quotient \mathbb{A}/\mathbb{Q} must be Hausdorff. As for compactness, it suffices to show that the compact set $\prod_p \mathbb{Z}_p \times [0, 1]$ contains a set of representatives of \mathbb{A}/\mathbb{Q} because this implies that the projection

$$\prod_p \mathbb{Z}_p \times [0, 1] \rightarrow \mathbb{A}/\mathbb{Q}$$

is surjective, hence that \mathbb{A}/\mathbb{Q} is the continuous image of a compact set. So let $x \in \mathbb{A}$ –then there is a finite set S of primes such that $p \notin S \implies x_p \in \mathbb{Z}_p$. For $p \in S$, write

$$x_p = f(x_p) + [x_p],$$

thus $[x_p] \in \mathbb{Z}_p$ and if $q \neq p$ is another prime,

$$\begin{aligned} |f(x_p)|_q &= \left| \sum_{n=v(x_p)}^{-1} a_n p^n \right|_q \\ &\leq \sup\{|a_n p^n|_q\} \\ &\leq 1. \end{aligned}$$

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 $\forall p, y_p \in \mathbb{Z}_p$, and $r \in \mathbb{Q}$. At infinity,

$$x_\infty = y_\infty + r \quad (r_\infty = r)$$

and there is a unique $k \in \mathbb{Z}$ such that

$$y_\infty = (y_\infty - k) + k$$

with $0 \leq y_\infty - k < 1$. Accordingly,

$$y = y + r = (y - k) + k + r.$$

And

$$\forall p, \quad (y - k)_p = y_p - k_p = y_p - k \in \mathbb{Z}_p,$$

while

$$x_\infty = (y_\infty - k) + k + r.$$

It therefore follows that x can be written as the sum of an element in $\prod_p \mathbb{Z}_p \times [0, 1]$ and a rational number, the contention.

8: DEFINITION The topological group \mathbb{A}/\mathbb{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

$$D = \prod_p \mathbb{Z}_p \times [0, 1[$$

is a fundamental domain for \mathbb{A}/\mathbb{Q} .

PROOF The claim is that every $x \in \mathbb{A}$ can be written uniquely as $d + r$, where $d \in D, r \in \mathbb{Q}$. The proof of #7 settles existence, thus the remaining issue is uniqueness:

$$d_1 + r_1 = d_2 + r_2 \implies d_1 = d_2, \quad r_1 = r_2$$

To see this, consider

$$\rho = d_1 - d_2 = r_2 - r_1 \in (D - D) \cap \mathbb{Q}.$$

- $\forall p, \rho = \rho_p \in D_p - D_p = D_p = \mathbb{Z}_p$
 $\implies \rho \in \bigcap_p (\mathbb{Q} \cap \mathbb{Z}_p) = \mathbb{Z}.$
- $\rho = \rho_\infty \in D_\infty - D_\infty =]-1, 1[.$

Therefore

$$\rho \in \mathbb{Z} \cap]-1, 1[\implies \rho = 0.$$

11: REMARK \mathbb{Q} is dense in \mathbb{A}_{fin} .

[The point is that \mathbb{Z} is dense in $\prod_p \mathbb{Z}_p$.]

12: DEFINITION The set of finite ideles is the restricted product

$$\mathbb{I}_{\text{fin}} = \prod_p (\mathbb{Q}_p^\times : \mathbb{Z}_p^\times).$$

13: DEFINITION The set of ideles is the product

$$\mathbb{I} = \mathbb{I}_{\text{fin}} \times \mathbb{R}^\times.$$

14: LEMMA \mathbb{I} is a locally compact abelian group (under multiplication).

Algebraically, \mathbb{I} can be identified with \mathbb{A}^\times but there is a topological issue since when endowed with the relative topology, \mathbb{A}^\times is not a topological group: Multiplication is continuous but inversion is not continuous.

15: LEMMA Equip $\mathbb{A} \times \mathbb{A}$ with the product topology and define

$$\begin{aligned} \phi : \mathbb{I} &\rightarrow \mathbb{A} \times \mathbb{A} \\ x &\mapsto \left(x, \frac{1}{x}\right). \end{aligned}$$

Endow the image $\phi(\mathbb{I})$ with the relative topology —then ϕ is a topological isomorphism of \mathbb{I} onto $\phi(\mathbb{I})$.

The image of the diagonal map

$$\mathbb{Q}^\times \longrightarrow \prod_p \mathbb{Q}_p \times \mathbb{R}^\times$$

lies in \mathbb{I} , so \mathbb{Q}^\times can be regarded as a subgroup of \mathbb{I} .

16: LEMMA \mathbb{Q}^\times is a discrete subspace of \mathbb{I} .

PROOF \mathbb{Q} is a discrete subspace of \mathbb{A} (cf. #5), hence $\mathbb{Q} \times \mathbb{Q}$ is a discrete subspace of $\mathbb{A} \times \mathbb{A}$, hence $\phi(\mathbb{Q}^\times)$ is a discrete subspace of $\phi(\mathbb{I})$.

Consequently, \mathbb{Q}^\times is a closed subgroup of \mathbb{I} and the quotient $\mathbb{I}/\mathbb{Q}^\times$ is a locally compact Hausdorff space but, as opposed to the adelic situation, it is not compact (see below).

17: DEFINITION The topological group $\mathbb{I}/\mathbb{Q}^\times$ is called the idele class group.

18: NOTATION Given $x \in \mathbb{I}$, put

$$|x|_{\mathbb{A}} = \prod_{p \leq \infty} |x_p|_p.$$

Extend the definition of $|\cdot|_{\mathbb{A}}$ to all of \mathbb{A} by setting $|x|_{\mathbb{A}} = 0$ if $x \in \mathbb{A} - \mathbb{A}^\times$.

19: LEMMA $\forall x \in \mathbb{Q}^\times, |x|_{\mathbb{A}} = 1$ (cf. §1, #21).

20: LEMMA The homomorphism

$$|\cdot|_{\mathbb{A}} : \mathbb{I} \rightarrow \mathbb{R}_{>0}^\times$$

is continuous and surjective.

PROOF Omitting the verification of continuity, fix $t \in \mathbb{R}_{>0}^\times$ and let x be the idele specified by

$$x_p = \begin{cases} 1 & (p < \infty) \\ t & (p = \infty) \end{cases}.$$

Then $|x|_{\mathbb{A}} = t$.

21: SCHOLIUM The idele class group $\mathbb{I}/\mathbb{Q}^\times$ is not compact.

22: NOTATION Let

$$\mathbb{I}^1 = \ker |\cdot|_{\mathbb{A}}.$$

23: N.B. $x \in \mathbb{I}^1 \implies x_\infty \in \mathbb{Q}^\times$.

24: THEOREM The quotient $\mathbb{I}^1/\mathbb{Q}^\times$ is a compact Hausdorff space, in fact

$$\mathbb{I}^1/\mathbb{Q}^\times \approx \prod_p \mathbb{Z}_p^\times,$$

hence

$$\prod_p \mathbb{Z}_p^\times \times \{1\}$$

is a fundamental domain for $\mathbb{I}^1/\mathbb{Q}^\times$.

PROOF The arrow

$$\prod_p \mathbb{Z}_p^\times \rightarrow \mathbb{I}^1/\mathbb{Q}^\times$$

that sends x to $(x, 1)\mathbb{Q}^\times$ is an isomorphism of topological groups.

[In obvious notation, the inverse is the map

$$x = (x_{\text{fin}}, x_\infty) \rightarrow \frac{1}{x_\infty} x_{\text{fin}}.]$$

25: REMARK $\forall p$, \mathbb{Z}_p^\times is totally disconnected. But a product of totally disconnected spaces is totally disconnected, thus $\prod_p \mathbb{Z}_p^\times$ is totally disconnected, thus $\mathbb{I}^1/\mathbb{Q}^\times$ is totally disconnected.

26: N.B. $\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}^\times$ is a fundamental domain for $\mathbb{I}^1/\mathbb{Q}^\times$.

[Note: If $r \in \mathbb{Q}$ and if $|r|_p = 1 \forall p$, then $r = \pm 1$.]

27: LEMMA

$$\mathbb{I} \approx \mathbb{I}^1 \times \mathbb{R}_{>0}^\times.$$

PROOF The arrow

$$\mathbb{I} \rightarrow \mathbb{I}^1 \times \mathbb{R}_{>0}^\times$$

that sends x to $(\tilde{x}, |x|_\mathbb{A})$, where

$$(\tilde{x})_p = \begin{cases} x_p & (p < \infty) \\ \frac{x_\infty}{|x|_\mathbb{A}} & (p = \infty) \end{cases},$$

is an isomorphism of topological groups.

28: LEMMA There is a disjoint decomposition

$$\mathbb{I}_{\text{fin}} = \coprod_{q \in \mathbb{Q}_{>0}^\times} q \left(\prod_p \mathbb{Z}_p^\times \right).$$

PROOF The right hand side is obviously contained in the left hand side. To go the other way, fix an $x \in \mathbb{I}_{\text{fin}}$ —then $|x|_\mathbb{A} \in \mathbb{Q}_{>0}^\times$. Moreover, $|x|_\mathbb{A} x \in \mathbb{I}_{\text{fin}}$ and $\forall p$, $||x|_\mathbb{A} x|_p = 1$ (for $x_p = p^k u$ ($u \in \mathbb{Z}_p^\times$) $\implies |x|_\mathbb{A} = p^{-k} r$ ($r \in \mathbb{Q}_p^\times$, r coprime to p)), hence

$$|x|_\mathbb{A} x \in \prod_p \mathbb{Z}_p^\times.$$

Now write

$$x = |x|_\mathbb{A}^{-1} (|x|_\mathbb{A} x)$$

to conclude that

$$x \in q \prod_p \mathbb{Z}_p^\times \quad (q = |x|_{\mathbb{A}}^{-1}).$$

29: LEMMA There is a disjoint decomposition

$$\mathbb{I}_{\text{fin}} \cap \prod_p \mathbb{Z}_p = \coprod_{n \in \mathbb{N}} n \left(\prod_p \mathbb{Z}_p^\times \right).$$

Normalize the Haar measure $d^\times x$ on \mathbb{I}_{fin} by assigning the open-compact subgroup $\prod_p \mathbb{Z}_p^\times$ total volume 1.

30: EXAMPLE Suppose that $\Re(s) > 1$ –then

$$\begin{aligned} \int_{\mathbb{I}_{\text{fin}} \cap \prod_p \mathbb{Z}_p} |x|_{\mathbb{A}}^s d^\times x &= \sum_{n \in \mathbb{N}} \int_{n \left(\prod_p \mathbb{Z}_p^\times \right)} |x|_{\mathbb{A}}^s d^\times x \\ &= \sum_{n \in \mathbb{N}} \int_{\prod_p \mathbb{Z}_p^\times} |nx|_{\mathbb{A}}^s d^\times x \\ &= \sum_{n \in \mathbb{N}} n^{-s} \text{vol}_{d^\times x} \left(\prod_p \mathbb{Z}_p^\times \right) \\ &= \sum_{n \in \mathbb{N}} n^{-s} \\ &= \zeta(s). \end{aligned}$$

[Note: Let $x \in \prod_p \mathbb{Z}_p^\times$:

$$\implies |x_p|_p = 1 \quad \forall p,$$

$$\begin{aligned} \implies |nx|_{\mathbb{A}} &= \prod_p |nx_p|_p \\ &= \prod_p |n|_p |x_p|_p \\ &= \prod_p |n|_p \end{aligned}$$

$$\begin{aligned}
&= \prod_p |n|_p \cdot n \cdot \frac{1}{n} \\
&= 1 \cdot \frac{1}{n} \\
&= n^{-1}.]
\end{aligned}$$

The idelic absolute value $|\cdot|_{\mathbb{A}}$ can be interpreted measure theoretically.

31: NOTATION Write

$$dx_{\mathbb{A}} = \prod_{p \leq \infty} dx_p$$

for the Haar measure $\mu_{\mathbb{A}}$ on \mathbb{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 \mathbb{Q}_p and for all but a finite number of $p, f_p = \chi_{\mathbb{Z}_p}$ —then

$$\int_{\mathbb{A}} f(x) dx_{\mathbb{A}} = \prod_{p \leq \infty} \int_{\mathbb{Q}_p} f_p(x_p) dx_p \quad (\text{cf. §13, #18}),$$

it being understood that $\mathbb{Q}_{\infty} = \mathbb{R}$.

32: LEMMA Let $M \subset \mathbb{A}$ be a Borel set with $0 < \mu_{\mathbb{A}}(M) < \infty$ —then $\forall x \in \mathbb{I}$,

$$\frac{\mu_{\mathbb{A}}(xM)}{\mu_{\mathbb{A}}(M)} = |x|_{\mathbb{A}}.$$

PROOF Take $M = D = \prod_p \mathbb{Z}_p \times [0, 1[$ (cf. #10):

$$\begin{aligned}
\mu_{\mathbb{A}}(xM) &= \prod_p \mu_{\mathbb{Q}_p}(x_p \mathbb{Z}_p) \times \mu_{\mathbb{R}}(x_{\infty} [0, 1[) \\
&= \prod_p |x_p|_p \mu_{\mathbb{Q}_p}(\mathbb{Z}_p) \times |x_{\infty}| \mu_{\mathbb{R}}([0, 1[) \\
&= \prod_p |x_p|_p \times |x_{\infty}|_{\infty}
\end{aligned}$$

$$\begin{aligned}
&= \prod_{p \leq \infty} |x_p|_p \\
&= |x|_{\mathbb{A}}.
\end{aligned}$$

[Note: Needless to say, multiplication by an idele x is an automorphism of \mathbb{A} , thus transforms $\mu_{\mathbb{A}}$ into a positive constant multiple of itself, the multiplier being $|x|_{\mathbb{A}}$.]

§15. GLOBAL ANALYSIS

By definition,

$$\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{R}.$$

Therefore

$$\widehat{\mathbb{A}} \approx \widehat{\mathbb{A}}_{\text{fin}} \times \widehat{\mathbb{R}}.$$

And

$$\mathbb{A}_{\text{fin}} = \prod_p (\mathbb{Q}_p : \mathbb{Z}_p)$$

\implies

$$\widehat{\mathbb{A}}_{\text{fin}} \approx \prod_p (\widehat{\mathbb{Q}}_p : \mathbb{Z}_p^\perp) \quad (\text{cf. §13, \#15}).$$

Put

$$\chi_{\mathbb{Q}} = \prod_{p \leq \infty} \chi_p,$$

where

$$\chi_{\infty} = \exp(-2\pi\sqrt{-1} x) \quad (x \in \mathbb{R}) \quad (\text{cf. §8, \#27}).$$

Then

$$\chi_{\mathbb{Q}} \in \widehat{\mathbb{A}}.$$

Given $t \in \mathbb{A}$, define $\chi_{\mathbb{Q},t} \in \widehat{\mathbb{A}}$ by the rule

$$\chi_{\mathbb{Q},t}(x) = \chi_{\mathbb{Q}}(tx).$$

Then the arrow

$$\Xi_{\mathbb{Q}} : \mathbb{A} \rightarrow \widehat{\mathbb{A}}$$

that sends t to $\chi_{\mathbb{Q},t}$ is an isomorphism of topological groups (cf. §8, \#24).

Recall now that $\forall q \in \mathbb{Q}$,

$$\chi_{\mathbb{Q}}(q) = 1 \quad (\text{cf. } \S 8, \#28).$$

Accordingly, $\chi_{\mathbb{Q}}$ passes to the quotient and defines a unitary character of the adèle class group \mathbb{A}/\mathbb{Q} . So, $\forall q \in \mathbb{Q}$, $\chi_{\mathbb{Q},q}$ is constant on the cosets of \mathbb{A}/\mathbb{Q} , thus it too determines an element of $\widehat{\mathbb{A}/\mathbb{Q}}$.

Equip \mathbb{Q} with the discrete topology.

1: THEOREM The induced map

$$\begin{aligned} \Xi_{\mathbb{Q}}|_{\mathbb{Q}} : \mathbb{Q} &\rightarrow \widehat{\mathbb{A}/\mathbb{Q}} \\ q &\mapsto \chi_{\mathbb{Q},q} \end{aligned}$$

is an isomorphism of topological groups.

PROOF Form $\mathbb{Q}^{\perp} \subset \widehat{\mathbb{A}}$, the closed subgroup of $\widehat{\mathbb{A}}$ consisting of those χ that are trivial on \mathbb{Q} —then $\mathbb{Q} \subset \mathbb{Q}^{\perp}$ and $\widehat{\mathbb{A}/\mathbb{Q}} \approx \mathbb{Q}^{\perp}$. But \mathbb{A}/\mathbb{Q} is compact, thus its unitary dual $\widehat{\mathbb{A}/\mathbb{Q}}$ is discrete, thus \mathbb{Q}^{\perp} is discrete. The quotient $\mathbb{Q}^{\perp}/\mathbb{Q} \subset \mathbb{A}/\mathbb{Q}$ ($\mathbb{A} \approx \widehat{\mathbb{A}}$) is therefore discrete and closed, hence discrete and compact, hence finite. But $\mathbb{Q}^{\perp}/\mathbb{Q}$ is a \mathbb{Q} -vector space, so $\mathbb{Q}^{\perp}/\mathbb{Q} = \{0\}$ or still, $\mathbb{Q}^{\perp} = \mathbb{Q}$, which implies that $\mathbb{Q} \approx \widehat{\mathbb{A}/\mathbb{Q}}$.

2: N.B. There are two points of detail that have been tacitly invoked in the foregoing derivation.

- $\mathbb{Q}^{\perp}/\mathbb{Q}$ in the quotient topology is discrete. Reason: Let S be an arbitrary nonempty subset of $\mathbb{Q}^{\perp}/\mathbb{Q}$, say $S = \{x\mathbb{Q} : x \in U\}$, U a subset of \mathbb{Q}^{\perp} —then U is automatically open (\mathbb{Q}^{\perp} being discrete), thus by the very definition of the quotient topology, S is an open subset of $\mathbb{Q}^{\perp}/\mathbb{Q}$.

- The quotient $\mathbb{Q}^{\perp}/\mathbb{Q}$ is closed in \mathbb{A}/\mathbb{Q} . Reason: \mathbb{Q}^{\perp} is a closed subgroup of \mathbb{A} containing \mathbb{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 ($\pi : G \rightarrow G/H$ the projection).

3: SCHOLIUM

$$\mathbb{Q} \approx \widehat{\mathbb{A}/\mathbb{Q}} \implies \widehat{\mathbb{Q}} \approx \widehat{\widehat{\mathbb{A}/\mathbb{Q}}} \approx \mathbb{A}/\mathbb{Q}.$$

[Note: Bear in mind that \mathbb{Q} carries the discrete topology.]

4: DISCUSSION Explicated, if $\chi \in \widehat{\mathbb{Q}}$, then there exists a $t \in \mathbb{A}$ such that $\chi = \chi_{\mathbb{Q},t}$ and $\chi_{\mathbb{Q},t_1} = \chi_{\mathbb{Q},t_2}$ iff $t_1 - t_2 \in \mathbb{Q}$.

5: DEFINITION The Bruhat space $\mathcal{B}(\mathbb{A}_{\text{fin}})$ consists of all finite linear combinations of functions of the form

$$f = \prod_p f_p,$$

where $\forall p, f_p \in \mathcal{B}(\mathbb{Q}_p)$ and $f_p = \chi_{\mathbb{Z}_p}$ for all but a finite number of p .

6: DEFINITION The Bruhat-Schwartz space $\mathcal{B}_{\infty}(\mathbb{A})$ consists of all finite linear combinations of functions of the form

$$f = \prod_p f_p \times f_{\infty},$$

where

$$\prod_p f_p \in \mathcal{B}(\mathbb{A}_{\text{fin}}) \text{ and } f_{\infty} \in \mathcal{S}(\mathbb{R}).$$

Given an $f \in \mathcal{B}_{\infty}(\mathbb{A})$, its Fourier transform is the function:

$$\begin{aligned} \widehat{f} : \mathbb{A} &\rightarrow \mathbb{C} \\ t &\mapsto \int_{\mathbb{A}} f(x) \chi_{\mathbb{Q},t}(x) d\mu_{\mathbb{A}}(x) = \int_{\mathbb{A}} f(x) \chi_{\mathbb{Q}}(tx) d\mu_{\mathbb{A}}(x). \end{aligned}$$

7: LEMMA If

$$f = \prod_p f_p \times f_{\infty}$$

is a Bruhat-Schwartz function, then

$$\widehat{f} = \prod_p \widehat{f}_p \times \widehat{f}_\infty.$$

8: REMARK \widehat{f}_p is computed per §10, #11 but \widehat{f}_∞ 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

$$f \in \mathcal{B}_\infty(\mathbb{A}) \implies \widehat{f} \in \mathcal{B}_\infty(\mathbb{A}) \quad (\text{cf. §10, \#16}).$$

10: N.B. It is clear that

$$\mathcal{B}_\infty(\mathbb{A}) \subset \mathbf{INV}(\mathbb{A})$$

and $\forall f \in \mathcal{B}_\infty(\mathbb{A})$,

$$\widehat{\widehat{f}} = f(-x) \quad (x \in \mathbb{A}).$$

11: LEMMA Given $f \in \mathcal{B}_\infty(\mathbb{A})$, the series

$$\sum_{r \in \mathbb{Q}} f(x+r), \quad \sum_{q \in \mathbb{Q}} \widehat{f}(x+q)$$

are absolutely and uniformly convergent on compact subsets of \mathbb{A} .

12: POISSON SUMMATION FORMULA Given $f \in \mathcal{B}_\infty(\mathbb{A})$,

$$\sum_{r \in \mathbb{Q}} f(r) = \sum_{q \in \mathbb{Q}} \widehat{f}(q).$$

The proof is not difficult but there are some measure theoretic issue to be dealt with first.

On general grounds,

$$\int_{\mathbb{A}} = \int_{\mathbb{A}/\mathbb{Q}} \sum_{\mathbb{Q}} \quad (\text{cf. §6, \#11}).$$

Here the integral $\int_{\mathbb{A}}$ is with respect to the Haar measure $\mu_{\mathbb{A}}$ on \mathbb{A} (cf. §14, \#31). Taking $\mu_{\mathbb{Q}}$ to be counting measure, this choice of data fixes the Haar measure $\mu_{\mathbb{A}/\mathbb{Q}}$ on \mathbb{A}/\mathbb{Q} .

[Note: The restriction of $\mu_{\mathbb{A}}$ to the fundamental domain

$$D = \prod_p \mathbb{Z}_p \times [0, 1[$$

for \mathbb{A}/\mathbb{Q} (cf. §14, \#10) determines $\mu_{\mathbb{A}/\mathbb{Q}}$ and

$$1 = \mu_{\mathbb{A}}(D) = \mu_{\mathbb{A}/\mathbb{Q}}(\mathbb{A}/\mathbb{Q}).]$$

If $\phi : \mathbb{Q} \rightarrow \mathbb{C}$, then $\widehat{\phi} : \widehat{\mathbb{Q}} \rightarrow \mathbb{C}$, i.e. $\widehat{\phi} : \mathbb{A}/\mathbb{Q} \rightarrow \mathbb{C}$ or still,

$$\widehat{\phi}(\chi) = \sum_{r \in \mathbb{Q}} \phi(r) \chi(r).$$

Specialize and suppose that ϕ is the characteristic function of $\{0\}$, so $\forall \chi$,

$$\widehat{\phi}(\chi) = \chi(0) = 1.$$

Therefore $\widehat{\phi}$ is the constant function 1 on \mathbb{A}/\mathbb{Q} . Pass now to $\widehat{\widehat{\phi}}$, thus $\widehat{\widehat{\phi}} : \widehat{\mathbb{A}/\mathbb{Q}} \rightarrow \mathbb{C}$ or still,

$$\begin{aligned} \widehat{\widehat{\phi}} : (\chi_{\mathbb{Q},q}) &= \int_{\mathbb{A}/\mathbb{Q}} \widehat{\phi}(x) \chi_{\mathbb{Q},q}(x) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} \chi_{\mathbb{Q},q}(x) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \end{aligned}$$

which is 1 if $q = 0$ and is 0 otherwise (cf. §7, \#46 (\mathbb{A}/\mathbb{Q} is compact)), hence $\widehat{\widehat{\phi}} = \phi$. But

$\phi(r) = \phi(-r)$, thereby leading to the conclusion that the Haar measure $\mu_{\mathbb{A}/\mathbb{Q}}$ on \mathbb{A}/\mathbb{Q} is the one singled out by Fourier inversion (cf. §7, #45).

Summary: Per Fourier inversion,

- $\mu_{\mathbb{Q}}$ is paired with $\mu_{\mathbb{A}/\mathbb{Q}}$.
- $\mu_{\mathbb{A}/\mathbb{Q}}$ is paired with $\mu_{\mathbb{Q}}$.

Given $f \in \mathcal{B}_{\infty}(\mathbb{A})$, put

$$F(x) = \sum_{r \in \mathbb{Q}} f(x + r).$$

Then F lives on \mathbb{A}/\mathbb{Q} , so \widehat{F} lives on $\widehat{\mathbb{A}/\mathbb{Q}} \approx \mathbb{Q}$:

$$\begin{aligned} \widehat{F}(q) &= \int_{\mathbb{A}/\mathbb{Q}} F(x) \chi_{\mathbb{Q},q}(x) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} F(x) \chi_{\mathbb{Q}}(qx) d\mu_{\mathbb{A}/\mathbb{Q}}(x). \end{aligned}$$

On the other hand,

$$\begin{aligned} \widehat{f}(q) &= \int_{\mathbb{A}} f(x) \chi_{\mathbb{Q},q}(x) d\mu_{\mathbb{A}}(x) \\ &= \int_{\mathbb{A}} f(x) \chi_{\mathbb{Q}}(qx) d\mu_{\mathbb{A}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} \left(\sum_{r \in \mathbb{Q}} f(x + r) \chi_{\mathbb{Q}}(q(x + r)) \right) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} \left(\sum_{r \in \mathbb{Q}} f(x + r) \chi_{\mathbb{Q}}(qx + qr) \right) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} \left(\sum_{r \in \mathbb{Q}} f(x + r) \chi_{\mathbb{Q}}(qx) \chi_{\mathbb{Q}}(qr) \right) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} \left(\sum_{r \in \mathbb{Q}} f(x + r) \right) \chi_{\mathbb{Q}}(qx) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \int_{\mathbb{A}/\mathbb{Q}} F(x) \chi_{\mathbb{Q}}(qx) d\mu_{\mathbb{A}/\mathbb{Q}}(x) \\ &= \widehat{F}(q). \end{aligned}$$

To finish the proof, per Fourier inversion, write

$$F(x) = \sum_{q \in \mathbb{Q}} \widehat{F}(q) \overline{\chi_{\mathbb{Q}}(qx)}$$

and then put $x = 0$:

$$F(0) = \sum_{r \in \mathbb{Q}} f(r) = \sum_{q \in \mathbb{Q}} \widehat{F}(q) = \sum_{q \in \mathbb{Q}} \widehat{f}(q).$$

13: THEOREM Let $x \in \mathbb{I}$ —then $\forall f \in \mathcal{B}_{\infty}(\mathbb{A})$,

$$\sum_{r \in \mathbb{Q}} f(rx) = \frac{1}{|x|_{\mathbb{A}}} \sum_{q \in \mathbb{Q}} \widehat{f}(qx^{-1}).$$

PROOF Work with $f_x \in \mathcal{B}_{\infty}(\mathbb{A})$ ($f_x(y) = f(xy)$) :

$$\sum_{r \in \mathbb{Q}} f_x(r) = \sum_{q \in \mathbb{Q}} \widehat{f_x}(q).$$

But

$$\begin{aligned} \widehat{f_x}(q) &= \int_{\mathbb{A}} f_x(y) \chi_{\mathbb{Q},q}(y) d\mu_{\mathbb{A}}(y) \\ &= \int_{\mathbb{A}} f_x(y) \chi_{\mathbb{Q}}(qy) d\mu_{\mathbb{A}}(y) \\ &= \int_{\mathbb{A}} f(xy) \chi_{\mathbb{Q}}(qxx^{-1}y) d\mu_{\mathbb{A}}(y) \\ &= \frac{1}{|x|_{\mathbb{A}}} \int_{\mathbb{A}} f(y) \chi_{\mathbb{Q}}(qx^{-1}y) d\mu_{\mathbb{A}}(y) \\ &= \frac{1}{|x|_{\mathbb{A}}} \widehat{f}(qx^{-1}). \end{aligned}$$

§16. FUNCTIONAL EQUATIONS

Let

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\Re(s) > 1)$$

be the Riemann zeta function —then $\zeta(s)$ can be meromorphically continued into the whole s -plane with a simple pole at $s = 1$ and satisfies there the functional equation

$$\pi^{-s/2} \Gamma(s/2) \zeta(s) = \pi^{-(1-s)/2} \Gamma((1-s)/2) \zeta(1-s).$$

1: REMARK The product $\pi^{-s/2} \Gamma(s/2)$ was denoted by $\Gamma_{\mathbb{R}}(s)$ 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

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^s \frac{dx}{x} \quad (\Re(s) > 1).$$

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

$$\theta(x) = 1 + 2\psi(x) = \sum_{n \in \mathbb{Z}} e^{-n^2 \pi x}.$$

2: LEMMA

$$\theta\left(\frac{1}{x}\right) = \sqrt{x} \theta(x).$$

Therefore

$$\begin{aligned} \psi\left(\frac{1}{x}\right) &= -\frac{1}{2} + \frac{1}{2} \theta\left(\frac{1}{x}\right) \\ &= -\frac{1}{2} + \frac{\sqrt{x}}{2} \theta(x) \\ &= -\frac{1}{2} + \frac{\sqrt{x}}{2} + \sqrt{x} \psi(x). \end{aligned}$$

One may then write

$$\begin{aligned} \pi^{-s/2} \Gamma(s/2) \zeta(s) &= \int_0^\infty \psi(x) x^{s/2} \frac{dx}{x} \\ &= \int_0^1 \psi(x) x^{s/2} \frac{dx}{x} + \int_1^\infty \psi(x) x^{s/2} \frac{dx}{x} \\ &= \int_1^\infty \psi\left(\frac{1}{x}\right) x^{-s/2} \frac{dx}{x} + \int_1^\infty \psi(x) x^{s/2} \frac{dx}{x} \\ &= \int_1^\infty \left(-\frac{1}{2} + \frac{\sqrt{x}}{2} + \sqrt{x} \psi(x)\right) x^{-s/2} \frac{dx}{x} + \int_1^\infty \psi(x) x^{s/2} \frac{dx}{x} \\ &= \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \psi(x) (x^{s/2} + x^{(1-s)/2}) \frac{dx}{x}. \end{aligned}$$

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 adèle-idele machinery.

Thus let

$$\Phi(x) = e^{-\pi x_\infty^2} \prod_p \chi_{\mathbb{Z}_p}(x_p) \quad (x \in \mathbb{A}).$$

Then if $\Re(s) > 1$,

$$\begin{aligned} \int_{\mathbb{I}} \Phi(x) |x|_{\mathbb{A}}^s d^\times x &= \int_{\mathbb{R}^\times} e^{-\pi t^2} |t|^s \frac{dt}{|t|} \cdot \prod_p \int_{\mathbb{Q}_p^\times} \chi_{\mathbb{Z}_p}(x_p) |x_p|_p^s d^\times x_p \\ &= \pi^{-s/2} \Gamma(s/2) \cdot \prod_p \int_{\mathbb{Z}_p - \{0\}} |x_p|_p^s d^\times x_p \\ &= \pi^{-s/2} \Gamma(s/2) \cdot \prod_p \frac{1}{1 - p^{-s}} \quad (\text{cf. §6, \#26}) \\ &= \pi^{-s/2} \Gamma(s/2) \zeta(s). \end{aligned}$$

To derive the functional equation, we shall calculate the integral

$$\int_{\mathbb{I}} \Phi(x) |x|_{\mathbb{A}}^s d^\times x$$

in another way. To this end, put

$$D^\times = \prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}^\times,$$

a fundamental domain for $\mathbb{I}/\mathbb{Q}^\times$ (cf. §14, \# 26), so

$$\mathbb{I} = \coprod_{r \in \mathbb{Q}^\times} r D^\times \quad (\text{disjoint union}).$$

Therefore

$$\begin{aligned} \int_{\mathbb{I}} \Phi(x) |x|_{\mathbb{A}}^s d^\times x &= \sum_{r \in \mathbb{Q}^\times} \int_{r D^\times} \Phi(x) |x|_{\mathbb{A}}^s d^\times x \\ &= \int_{D^\times} \sum_{r \in \mathbb{Q}^\times} \Phi(rx) |rx|_{\mathbb{A}}^s d^\times x \end{aligned}$$

$$= \int_{D^\times: |x|_{\mathbb{A}} \leq 1} \sum_{r \in \mathbb{Q}^\times} \Phi(rx) |x|_{\mathbb{A}}^s d^\times x + \int_{D^\times: |x|_{\mathbb{A}} \geq 1} \sum_{r \in \mathbb{Q}^\times} \Phi(rx) |x|_{\mathbb{A}}^s d^\times x.$$

To proceed further, recall that $\widehat{\Phi} = \Phi$ ($\implies \widehat{\Phi}(0) = \Phi(0) = 1$), hence (cf. §15, #13)

$$1 + \sum_{r \in \mathbb{Q}^\times} \Phi(rx) = \frac{1}{|x|_{\mathbb{A}}} + \frac{1}{|x|_{\mathbb{A}}} \sum_{q \in \mathbb{Q}^\times} \Phi(qx^{-1}).$$

Accordingly,

$$\begin{aligned} & \int_{D^\times: |x|_{\mathbb{A}} \leq 1} \sum_{r \in \mathbb{Q}^\times} \Phi(rx) |x|_{\mathbb{A}}^s d^\times x \\ &= \int_{D^\times: |x|_{\mathbb{A}} \leq 1} \left(-1 + \frac{1}{|x|_{\mathbb{A}}} + \frac{1}{|x|_{\mathbb{A}}} \sum_{q \in \mathbb{Q}^\times} \Phi(qx^{-1}) \right) |x|_{\mathbb{A}}^s d^\times x \\ &= \int_{D^\times: |x|_{\mathbb{A}} \leq 1} (|x|_{\mathbb{A}}^{s-1} - |x|_{\mathbb{A}}^s) d^\times x + \int_{D^\times: |x|_{\mathbb{A}} \geq 1} \sum_{q \in \mathbb{Q}^\times} \Phi(qx) |x|_{\mathbb{A}}^{1-s} d^\times x. \end{aligned}$$

But

$$\begin{aligned} \int_{D^\times: |x|_{\mathbb{A}} \leq 1} (|x|_{\mathbb{A}}^{s-1} - |x|_{\mathbb{A}}^s) d^\times x &= \int_0^1 (t^{s-1} - t) \frac{dt}{t} \\ &= \frac{1}{s-1} - \frac{1}{s}. \end{aligned}$$

So, upon assembling the data, we conclude that

$$\int_{\mathbb{I}} \Phi(x) |x|_{\mathbb{A}}^s d^\times x = \frac{1}{s-1} - \frac{1}{s} + \int_{D^\times: |x|_{\mathbb{A}} \geq 1} \sum_{q \in \mathbb{Q}^\times} \Phi(qx) (|x|_{\mathbb{A}}^s + |x|_{\mathbb{A}}^{1-s}) d^\times x.$$

Since the second expression is invariant under the transformation $s \rightarrow 1-s$, the functional equation for $\zeta(s)$ follows once again.

3: REMARK Consider

$$\int_{D^\times: |x|_{\mathbb{A}} \geq 1} \sum_{q \in \mathbb{Q}^\times} \Phi(qx) \dots$$

Then from the definitions,

$$\begin{aligned} x \in D^\times &\implies x_p \in \mathbb{Z}_p^\times \text{ \& } qx_p \in \mathbb{Z}_p \\ &\implies q \in \mathbb{Z}. \end{aligned}$$

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

$$1 \rightarrow \mathbb{I}^1/\mathbb{Q}^\times \rightarrow \mathbb{I}/\mathbb{Q}^\times \rightarrow \mathbb{R}_{>0}^\times \rightarrow 1 \quad (\text{cf. §14, \#27})$$

and $\mathbb{I}^1/\mathbb{Q}^\times$ is compact (cf. §14, \#24).

1: DEFINITION Given $f \in \mathcal{B}_\infty(\mathbb{A})$ and a unitary character $\omega : \mathbb{I}/\mathbb{Q}^\times \rightarrow \mathbb{T}$, the global zeta function attached to the pair (f, ω) is

$$Z(f, \omega, s) = \int_{\mathbb{I}} f(x) \omega(x) |x|_{\mathbb{A}}^s d^\times x \quad (\Re(s) > 1).$$

2: EXAMPLE In the notation of §16, take

$$f(x) = \Phi(x) = e^{-\pi x_\infty^2} \prod_p \chi_{\mathbb{Z}_p}(x_p) \quad (x \in \mathbb{A})$$

and let $\omega = 1$ —then as shown there

$$Z(f, 1, s) = \pi^{-s/2} \Gamma(s/2) \zeta(s).$$

3: LEMMA $Z(f, \omega, s)$ is a holomorphic function of s in the strip $\Re(s) > 1$.

4: THEOREM $Z(f, \omega, s)$ can be meromorphically continued into the whole s -plane and satisfies the functional equation

$$Z(f, \omega, s) = Z(\widehat{f}, \overline{\omega}, 1 - s).$$

[Note:

$$f \in \mathcal{B}_\infty(\mathbb{A}) \implies \widehat{f} \in \mathcal{B}_\infty(\mathbb{A}) \quad (\text{cf. §15, \#9}).]$$

The proof is a computation, albeit a lengthy one.

To begin with,

$$\mathbb{I} \approx \mathbb{R}_{>0}^\times \times \mathbb{I}^1 \quad (\text{cf. } \S 14, \#27).$$

Therefore

$$\begin{aligned} Z(f, \omega, s) &= \int_{\mathbb{I}} f(x) \omega(x) |x|_{\mathbb{A}}^s d^\times x \\ &= \int_{\mathbb{R}_{>0}^\times \times \mathbb{I}^1} f(tx) \omega(tx) |tx|_{\mathbb{A}}^s \frac{dt}{t} d^\times x \\ &= \int_0^\infty \left(\int_{\mathbb{I}^1} f(tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t}. \end{aligned}$$

5: NOTATION Put

$$Z_t(f, \omega, s) = \int_{\mathbb{I}^1} f(tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x.$$

6: LEMMA

$$\begin{aligned} Z_t(f, \omega, s) + f(0) \int_{\mathbb{I}^1/\mathbb{Q}^\times} \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \\ = Z_{t^{-1}}(\widehat{f}, \overline{\omega}, 1-s) + \widehat{f}(0) \int_{\mathbb{I}^1/\mathbb{Q}^\times} \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x. \end{aligned}$$

PROOF Write

$$\begin{aligned} \int_{\mathbb{I}^1} f(tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x &= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{r \in \mathbb{Q}^\times} f(rtx) \omega(rtx) |rtx|_{\mathbb{A}}^s \right) d^\times x \\ &= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{r \in \mathbb{Q}^\times} f(rtx) \omega(tx) |tx|_{\mathbb{A}}^s \right) d^\times x. \end{aligned}$$

Then

$$\begin{aligned}
& Z_t(f, \omega, s) + f(0) \int_{\mathbb{I}^1/\mathbb{Q}^\times} \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \\
&= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{q \in \mathbb{Q}} f(rtx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \right. \\
&= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\frac{1}{|tx|_{\mathbb{A}}} \sum_{q \in \mathbb{Q}} \widehat{f}(qt^{-1}x^{-1}) \right) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \quad (\text{cf. §15, \#13}) \\
&= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{q \in \mathbb{Q}} \widehat{f}(qt^{-1}x) \right) |t^{-1}x|_{\mathbb{A}} \omega(tx^{-1}) |tx^{-1}|_{\mathbb{A}}^s d^\times x \quad (x \rightarrow x^{-1}) \\
&= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{q \in \mathbb{Q}} \widehat{f}(qt^{-1}x) \right) \omega^{-1}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x \\
&= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{q \in \mathbb{Q}} \widehat{f}(qt^{-1}x) \right) \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x \\
&= \int_{\mathbb{I}^1/\mathbb{Q}^\times} \left(\sum_{q \in \mathbb{Q}^\times} \widehat{f}(qt^{-1}x) \overline{\omega}(qt^{-1}x) |qt^{-1}x|_{\mathbb{A}}^{1-s} \right) d^\times x \\
&\quad + \widehat{f}(0) \int_{\mathbb{I}^1/\mathbb{Q}^\times} \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x \\
&= \int_{\mathbb{I}^1} \widehat{f}(t^{-1}x) \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x \\
&\quad + \widehat{f}(0) \int_{\mathbb{I}^1/\mathbb{Q}^\times} \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x \\
&= Z_{t^{-1}}(\widehat{f}, \overline{\omega}, 1-s) + \widehat{f}(0) \int_{\mathbb{I}^1/\mathbb{Q}^\times} \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^\times x.
\end{aligned}$$

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

$$\int_{\mathbb{I}:|x|_{\mathbb{A}} \geq 1} f(x) \omega(x) |x|_{\mathbb{A}}^s d^{\times} x.]$$

This leaves

$$\int_0^1 Z_t(f, \omega, s) \frac{dt}{t},$$

which can thus be represented as

$$\int_0^1 (Z_{t^{-1}}(\widehat{f}, \overline{\omega}, 1-s) - f(0) \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \omega(tx) |tx|_{\mathbb{A}}^s d^{\times} x + \widehat{f}(0) \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^{\times} x) \frac{dt}{t}.$$

To carry out the analysis, subject

$$\int_0^1 Z_{t^{-1}}(\widehat{f}, \overline{\omega}, 1-s) \frac{dt}{t}$$

to the change of variable $t \rightarrow t^{-1}$, thereby leading to

$$\int_1^{\infty} Z_t(\widehat{f}, \overline{\omega}, 1-s) \frac{dt}{t},$$

a holomorphic function of s (cf. #7 supra).

It remains to discuss

$$\begin{aligned} R(f, \omega, s) &= \int_0^1 (-f(0) \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \omega(tx) |tx|_{\mathbb{A}}^s d^{\times} x + \widehat{f}(0) \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \overline{\omega}(t^{-1}x) |t^{-1}x|_{\mathbb{A}}^{1-s} d^{\times} x) \frac{dt}{t} \\ &= \int_0^1 (-f(0) \omega(t) |t|^s \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \omega(x) d^{\times} x + \widehat{f}(0) \overline{\omega}(t^{-1}) |t^{-1}|^{1-s} \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \overline{\omega}(x) d^{\times} x) \frac{dt}{t}, \end{aligned}$$

there being two cases.

1. ω is nontrivial on \mathbb{I}^1 . Since $\mathbb{I}^1/\mathbb{Q}^{\times}$ is compact (cf. §14, #24), the integrals

$$\int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \omega(x) d^{\times} x, \quad \int_{\mathbb{I}^1/\mathbb{Q}^{\times}} \overline{\omega}(x) d^{\times} x$$

must vanish (cf. §7, #46). Therefore $R(f, \omega, s) = 0$, hence

$$Z(f, \omega, s) = \int_1^\infty Z_t(f, \omega, s) \frac{dt}{t} + \int_1^\infty Z_t(\widehat{f}, \overline{\omega}, 1-s) \frac{dt}{t},$$

is a holomorphic function of s .

2. ω is trivial on \mathbb{I}^1 . Let $\phi : \mathbb{R}_{>0}^\times \rightarrow \mathbb{I}/\mathbb{I}^1$ be the isomorphism per §14, #27 – then $\omega \circ \phi : \mathbb{R}_{>0}^\times \rightarrow \mathbb{T}$ is a unitary character of $\mathbb{R}_{>0}^\times$, thus for some $w \in \mathbb{R}$, $\omega \circ \phi = |\cdot|^{-\sqrt{-1} w}$, so

$$\omega = |\cdot|^{-\sqrt{-1} w} \circ \phi^{-1} \implies \omega(x) = |x|_{\mathbb{A}}^{-\sqrt{-1} w}.$$

Therefore

$$\begin{aligned} R(f, \omega, s) &= -f(0) \text{vol}(\mathbb{I}^1/\mathbb{Q}^\times) \int_0^1 t^{-\sqrt{-1} w + s - 1} dt + \widehat{f}(0) \text{vol}(\mathbb{I}^1/\mathbb{Q}^\times) \int_0^1 t^{-\sqrt{-1} w + s - 2} dt \\ &= -f(0) \frac{\text{vol}(\mathbb{I}^1/\mathbb{Q}^\times)}{-\sqrt{-1} w + s} + \widehat{f}(0) \frac{\text{vol}(\mathbb{I}^1/\mathbb{Q}^\times)}{-\sqrt{-1} w + s - 1}, \end{aligned}$$

a meromorphic function that has a simple pole at

$$\begin{cases} s = \sqrt{-1} w & \text{with residue} & -f(0) \text{vol}(\mathbb{I}^1/\mathbb{Q}^\times) & \text{if } f(0) \neq 0 \\ s = \sqrt{-1} w + 1 & \text{with residue} & \widehat{f}(0) \text{vol}(\mathbb{I}^1/\mathbb{Q}^\times) & \text{if } \widehat{f}(0) \neq 0 \end{cases}.$$

8: N.B. To explicate $\text{vol}(\mathbb{I}^1/\mathbb{Q}^\times)$ use the machinery of §16: In the notation of #2 above,

$$\begin{aligned} Z(f, 1, s) &= -\frac{1}{s} + \frac{1}{s-1} + \cdots \\ &\implies \text{vol}(\mathbb{I}^1/\mathbb{Q}^\times) = 1. \end{aligned}$$

[Note: Here, $w = 0$ and $f(0) = 1$, $\widehat{f}(0) = 1$.]

That $Z(f, \omega, s)$ can be meromorphically continued into the whole s -plane is now manifest. As for the functional equation, we have

$$\begin{aligned}
Z(f, \omega, s) &= \int_1^\infty Z_t(f, \omega, s) \frac{dt}{t} + \int_1^\infty Z_t(\widehat{f}, \overline{\omega}, 1-s) \frac{dt}{t} + R(f, \omega, s) \\
&= \int_1^\infty \left(\int_{\mathbb{I}^1} f(tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t} + \int_1^\infty \left(\int_{\mathbb{I}^1} \widehat{f}(tx) \overline{\omega}(tx) |tx|_{\mathbb{A}}^{1-s} d^\times x \right) \frac{dt}{t} + R(f, \omega, s).
\end{aligned}$$

And we also have

$$\begin{aligned}
Z(\widehat{f}, \overline{\omega}, 1-s) &= \int_1^\infty Z_t(\widehat{f}, \overline{\omega}, 1-s) \frac{dt}{t} + \int_1^\infty Z_t(\widehat{\widehat{f}}, \overline{\overline{\omega}}, 1-(1-s)) \frac{dt}{t} + R(\widehat{f}, \overline{\omega}, 1-s) \\
&= \int_1^\infty Z_t(\widehat{f}, \overline{\omega}, 1-s) \frac{dt}{t} + \int_1^\infty Z_t(\widehat{\widehat{f}}, \omega, s) \frac{dt}{t} + R(\widehat{f}, \overline{\omega}, 1-s) \\
&= \int_1^\infty \left(\int_{\mathbb{I}^1} \widehat{f}(tx) \overline{\omega}(tx) |tx|_{\mathbb{A}}^{1-s} d^\times x \right) \frac{dt}{t} + \int_1^\infty \left(\int_{\mathbb{I}^1} \widehat{\widehat{f}}(tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t} \\
&\quad + R(\widehat{f}, \overline{\omega}, 1-s).
\end{aligned}$$

The first of these terms can be left as is (since it already figures in the formula for $Z(f, \omega, s)$).

Recalling that

$$\widehat{\widehat{f}}(x) = f(-x) \quad (x \in \mathbb{A}) \quad (\text{cf. §15, \#10}),$$

The second term becomes

$$\int_1^\infty \left(\int_{\mathbb{I}^1} f(-tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t}$$

or still,

$$\int_1^\infty \left(\int_{\mathbb{I}^1} f(tx) \omega(-tx) |-tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t} = \int_1^\infty \left(\int_{\mathbb{I}^1} f(tx) \omega(-tx) |tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t}.$$

But by hypothesis, ω is trivial on \mathbb{Q}^\times , hence

$$\omega(-tx) = \omega((-1)tx) = \omega(-1)\omega(tx) = \omega(tx),$$

and we end up with

$$\int_1^\infty \left(\int_{\mathbb{I}^1} f(tx) \omega(tx) |tx|_{\mathbb{A}}^s d^\times x \right) \frac{dt}{t}$$

which likewise figures in the formula for $Z(f, \omega, s)$. Finally, if ω is trivial on \mathbb{I}^1 , then

$$\begin{aligned} R(\widehat{f}, \overline{\omega}, 1-s) &= -\frac{\widehat{f}(0)}{\sqrt{-1} w + 1 - s} + \frac{\widehat{\widehat{f}}(0)}{\sqrt{-1} w + (1-s) - 1} \\ &= \frac{f(0)}{\sqrt{-1} w - s} - \frac{\widehat{f}(0)}{\sqrt{-1} w + 1 - s} \\ &= -\frac{f(0)}{-\sqrt{-1} w + s} + \frac{\widehat{f}(0)}{-\sqrt{-1} w + s - 1} \\ &= R(f, \omega, s). \end{aligned}$$

On the other hand, if ω is nontrivial on \mathbb{I}^1 , then $\overline{\omega}$ is nontrivial on \mathbb{I}^1 and

$$R(f, \omega, s) = 0, \quad R(\widehat{f}, \overline{\omega}, 1-s) = 0.$$

§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 $f \in \mathcal{S}(\mathbb{R})$ and a unitary character $\omega : \mathbb{R}^\times \rightarrow \mathbb{T}$, the local zeta function attached to the pair (f, ω) is

$$Z(f, \omega, s) = \int_{\mathbb{R}^\times} f(x) \omega(x) |x|^s d^\times x \quad (\Re(s) > 0).$$

2: THEOREM There exists a meromorphic function $\rho(\omega, s)$ such that $\forall f$,

$$\rho(\omega, s) = \frac{Z(f, \omega, s)}{Z(\widehat{f}, \overline{\omega}, 1 - s)}.$$

Decompose ω as a product:

$$\omega(x) = (\text{sgn } x)^\sigma |x|^{-\sqrt{-1} w} \quad (\sigma \in \{0, 1\}, w \in \mathbb{R}).$$

3: DEFINITION Write (cf. §11, #9)

$$L(\omega, s) = \begin{cases} \Gamma_{\mathbb{R}}(s - \sqrt{-1} w) & (\sigma = 0) \\ \Gamma_{\mathbb{R}}(s - \sqrt{-1} w + 1) & (\sigma = 1) \end{cases}.$$

4: FACT

$$\rho(\omega, s) = \begin{cases} \frac{L(\omega, s)}{L(\omega, 1 - s)} & (\sigma = 0) \\ -\sqrt{-1} \frac{L(\omega, s)}{L(\overline{\omega}, 1 - s)} & (\sigma = 1) \end{cases}.$$

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 $\omega : \mathbb{Q}_p^\times \rightarrow \mathbb{T}$, the local zeta function attached to the pair (f, ω) is

$$Z(f, \omega, s) = \int_{\mathbb{Q}_p^\times} f(x) \omega(x) |x|_p^s d^\times x \quad (\Re(s) > 0).$$

7: THEOREM There exists a meromorphic function $\rho(\omega, s)$ such that $\forall f$,

$$\rho(\omega, s) = \frac{Z(f, \omega, s)}{Z(\widehat{f}, \bar{\omega}, 1-s)}.$$

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 ($\omega \neq 1$)

$$\rho(\omega, s) = \tau(\omega) \omega(-1) p^{n(s + \sqrt{-1} - 1)},$$

where

$$\tau(\omega) = \sum_{i=1}^r \omega(e_i) \chi_p(p^{-n} e_i)$$

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 \mathbb{Q}_p^\times (the story for \mathbb{R}^\times being the same), we have

$$\begin{aligned} Z(f, \omega, s) &= \int_{\mathbb{Q}_p^\times} f(x) \omega(x) |x|_p^s d^\times x \\ &= \int_{\mathbb{Q}_p^\times} f(-x) \omega(-x) |-x|_p^s d^\times x \\ &= \omega(-1) \int_{\mathbb{Q}_p^\times} f(x) \omega(x) |x|_p^s d^\times x \\ &= \omega(-1) Z(f, \omega, s) \\ &= -Z(f, \omega, s). \end{aligned}$$

§19. L-FUNCTIONS

Let $\omega : \mathbb{I}/\mathbb{Q}^\times \rightarrow \mathbb{T}$ be a unitary character.

1: LEMMA There is a unique unitary character $\underline{\omega}$ of $\mathbb{I}/\mathbb{Q}^\times$ of finite order and a unique real number w such that

$$\omega = \underline{\omega} | \cdot |_{\mathbb{A}}^{-\sqrt{-1}} w.$$

[Note: To say that $\underline{\omega}$ is of finite order means that there exists a positive integer n such that $\underline{\omega}(x)^n = 1 \ \forall \ x \in \mathbb{I}$.]

2: N.B.

$$\omega = \prod_p \omega_p \times \omega_\infty,$$

where

$$\omega_p = \underline{\omega}_p | \cdot |_p^{-\sqrt{-1}} w$$

and

$$\omega_\infty = (\text{sgn})^\sigma | \cdot |_\infty^{-\sqrt{-1}} w.$$

3: DEFINITION

$$L(\omega, s) = \prod_p L(\omega_p, s) \times L(\omega_\infty, s).$$

4: RAPPEL

$$L(\omega_p, s) = \begin{cases} (1 - \omega_p(p)p^{-s})^{-1} & (\underline{\omega}_p = 1) \\ 1 & (\underline{\omega}_p \neq 1) \end{cases} \quad (\text{cf. §18, \#8}).$$

[Note: The set S_ω of primes for which $\underline{\omega}_p \neq 1$ is finite.]

5: SUBLEMMA

$$|x| < 1 \implies \log(1-x) = -\sum_{k=1}^{\infty} \frac{x^k}{k}.$$

Therefore

$$\begin{aligned} |x| > 1 \implies \log \frac{1}{1-x^{-1}} &= \log 1 - \log(1-x^{-1}) \\ &= -\left(-\sum_{k=1}^{\infty} \frac{x^{-k}}{k}\right) \\ &= \sum_{k=1}^{\infty} \frac{x^{-k}}{k}. \end{aligned}$$

6: N.B.

$$\log f(z) = \log |f(z)| + \sqrt{-1} \arg f(z)$$

\implies

$$\Re \log f(z) = \log |f(z)|.$$

7: LEMMA The product

$$\prod_p L(\omega_p, s)$$

is absolutely convergent provided $\Re(s) > 1$.

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

$$\sum \log\left(\frac{1}{|1 - \omega_p(p)p^{-s}|}\right) = \sum \Re \log\left(\frac{1}{1 - \omega_p(p)p^{-s}}\right)$$

$$\begin{aligned}
&= \Re \sum \log\left(\frac{1}{1 - \omega_p(p)p^{-s}}\right) \\
&= \Re \sum \sum_{k=1}^{\infty} \frac{\omega_p(p)^k p^{-ks}}{k}.
\end{aligned}$$

The claim then is that the series

$$\sum \sum_{k=1}^{\infty} \frac{\omega_p(p)^k p^{-ks}}{k}$$

is absolutely convergent. But

$$\sum \sum_{k=1}^{\infty} \left| \frac{\omega_p(p)^k p^{-ks}}{k} \right| = \sum \sum_{k=1}^{\infty} \frac{p^{-k\Re(s)}}{k}$$

which is bounded by

$$\begin{aligned}
\sum_p \sum_{k=1}^{\infty} \frac{p^{-k\Re(s)}}{k} &= \sum_p \sum_{k=1}^{\infty} \frac{p^{-k(1+\delta)}}{k} \quad (\Re(s) = 1 + \delta) \\
&\leq \sum_p \sum_{k=1}^{\infty} p^{-k(1+\delta)} \\
&= \sum_p \frac{p^{-(1+\delta)}}{1 - p^{-(1+\delta)}} \\
&= \sum_p \frac{1}{p^{1+\delta}(1 - p^{-(1+\delta)})} \\
&= \sum_p \frac{1}{p^{(1+\delta)} - 1} \\
&\leq 2 \sum_p \frac{1}{p^{1+\delta}} \\
&< \infty.
\end{aligned}$$

8: EXAMPLE Take $\omega = 1$ –then

$$\begin{aligned} L(\omega, s) &= \prod_p \frac{1}{1 - p^{-s}} \times \Gamma_{\mathbb{R}}(s) \\ &= \pi^{-s/2} \Gamma(s/2) \zeta(s). \end{aligned}$$

9: LEMMA $L(\omega, s)$ is a holomorphic function of s in the strip $\Re(s) > 1$.

10: LEMMA $L(\omega, s)$ admits a meromorphic continuation to the whole s -plane (see below).

Owing to §17, #4, $\forall f \in \mathcal{B}_{\infty}(\mathbb{A})$,

$$Z(f, \omega, s) = Z(\hat{f}, \bar{\omega}, 1 - s).$$

To exploit this, assume that

$$f = \prod_p f_p \times f_{\infty},$$

where $\forall p, f_p \in \mathcal{B}(\mathbb{Q}_p)$ and $f_p = \chi_{\mathbb{Z}_p}$ for all but a finite number of p , while $f_{\infty} \in \mathcal{S}(\mathbb{R})$ –then

$$\begin{aligned} Z(f, \omega, s) &= \int_{\mathbb{I}} f(x) \omega(x) |x|_{\mathbb{A}}^s d^{\times} x \\ &= \prod_p \int_{\mathbb{Q}_p^{\times}} f_p(x_p) \omega_p(x_p) |x_p|_p^s d^{\times} x_p \times \int_{\mathbb{R}^{\times}} f_{\infty}(x_{\infty}) \omega_{\infty}(x_{\infty}) |x_{\infty}|_{\infty}^s d^{\times} x_{\infty} \\ &= \prod_p Z(f_p, \omega_p, s) \times Z(f_{\infty}, \omega_{\infty}, s) \end{aligned}$$

and analogously for $Z(\hat{f}, \bar{\omega}, 1 - s)$.

Therefore

$$1 = \frac{Z(f, \omega, s)}{Z(\hat{f}, \bar{\omega}, 1 - s)}$$

$$\begin{aligned}
&= \prod_p \frac{Z(f_p, \omega_p, s)}{Z(\widehat{f_p}, \bar{\omega}_p, 1-s)} \times \frac{Z(f_\infty, \omega_\infty, s)}{Z(\widehat{f_\infty}, \bar{\omega}_\infty, 1-s)} \\
&= \prod_p \rho(\omega_p, s) \times \rho(\omega_\infty, s) \\
&= \prod_{p \notin S_\omega} \rho(\omega_p, s) \times \prod_{p \in S_\omega} \rho(\omega_p, s) \times \rho(\omega_\infty, s) \\
&= \prod_{p \notin S_\omega} \frac{L(\omega_p, s)}{L(\bar{\omega}_p, 1-s)} \times \prod_{p \in S_\omega} \rho(\omega_p, s) \times \frac{L(\omega_\infty, s)}{L(\bar{\omega}_\infty, 1-s)} \\
&= \prod_{p \in S_\omega} \rho(\omega_p, s) \times \prod_{p \notin S_\omega} \frac{L(\omega_p, s)}{L(\bar{\omega}_p, 1-s)} \times \prod_{p \in S_\omega} \frac{L(\omega_p, s)}{L(\bar{\omega}_p, 1-s)} \times \frac{L(\omega_\infty, s)}{L(\bar{\omega}_\infty, 1-s)} \\
&= \prod_{p \in S_\omega} \rho(\omega_p, s) \times \prod_p \frac{L(\omega_p, s)}{L(\bar{\omega}_p, 1-s)} \times \frac{L(\omega_\infty, s)}{L(\bar{\omega}_\infty, 1-s)} \\
&= \prod_{p \in S_\omega} \rho(\omega_p, s) \times \frac{\prod_p L(\omega_p, s) \times L(\omega_\infty, s)}{\prod_p L(\bar{\omega}_p, 1-s) \times L(\bar{\omega}_\infty, 1-s)} \\
&= \prod_{p \in S_\omega} \rho(\omega_p, s) \times \frac{L(\omega, s)}{L(\bar{\omega}, 1-s)} \\
&= \prod_{p \in S_\omega} \varepsilon(\omega_p, s) \times \frac{L(\omega, s)}{L(\bar{\omega}, 1-s)} \quad (\text{cf. §12, \#11}) \\
&= \varepsilon(\omega, s) \times \frac{L(\omega, s)}{L(\bar{\omega}, 1-s)},
\end{aligned}$$

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

$$\pi^{-(1-s)/2} \Gamma((1-s)/2) \zeta(1-s) = \pi^{-s/2} \Gamma(s/2) \zeta(s) \quad (\text{cf. \#16}).$$

Make the following explicit choice for

$$f = \prod_p f_p \times f_\infty.$$

- If $\underline{\omega}_p = 1$, let

$$f_p(x_p) = \chi_p(x_p) \chi_{\mathbb{Z}_p}(x_p).$$

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

$$f_p(x_p) = \chi_p(x_p) \chi_{p^{-n}\mathbb{Z}_p}(x_p).$$

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

$$Z(f_\infty, x_\infty, s) = L(\omega_\infty, s).$$

13: 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 \mathbb{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 \mathbb{I}^1 –then $\omega = |\cdot|_{\mathbb{A}}^{-\sqrt{-1} w}$ and there are simple poles at

$$\begin{cases} s = \sqrt{-1} w & \text{with residue } -f(0) \text{ if } f(0) \neq 0 \\ s = \sqrt{-1} w + 1 & \text{with residue } \widehat{f}(0) \text{ if } \widehat{f}(0) \neq 0 \end{cases}.$$

But $\forall p, \omega_p = |\cdot|_p^{-\sqrt{-1} w}$ ($\implies \underline{\omega}_p = 1$), so $f_p(0) = 1$. And likewise $f_\infty(0) = 1$ ($\sigma = 0$). Conclusion: $f(0) = 1$. As for the Fourier transforms, $\widehat{f}_p = \chi_{\mathbb{Z}_p} \implies \widehat{f}_p(0) = 1$. Also $\widehat{f}_\infty = f_\infty$ ($\sigma = 0$) $\implies \widehat{f}_\infty(0) = 1$. Conclusion: $\widehat{f}(0) = 1$. 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

$$L(\omega, s) = \prod_p L(\omega_p, s) \times L(\omega_\infty, s)$$

$$\begin{aligned}
&= \prod_{p \in S} L(\omega_p, s) \prod_{p \notin S} L(1_p, s) \times L(1_\infty, s) \\
&= L(1, s) \prod_{p \in S} \frac{L(\omega_p, s)}{L(1_p, s)} \\
&= L(1, s) \prod_{p \in S} \frac{1 - p^{-s}}{1 - \alpha_p p^{-s}},
\end{aligned}$$

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

$$\omega = \underline{\omega} | \cdot |_{\mathbb{A}}^{-\sqrt{-1}} w \quad (\text{cf. §19, \#1}).$$

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 \mathbb{F}_q of characteristic p (thus q is an integral power of p), then in \mathbb{F}_p^{cl} ,

$$\mathbb{F}_q = \{x : x^q = x\}.$$

1: LEMMA The multiplicative group

$$\mathbb{F}_q^\times = \{x : x^{q-1} = 1\}$$

is cyclic of order $q - 1$.

2: NOTATION

$$\mathbb{F}_{q^n} = \{x : x^{q^n} = x\} \quad (n \geq 1).$$

3: LEMMA \mathbb{F}_{q^n} is a Galois extension of \mathbb{F}_q of degree n .

4: LEMMA $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n generated by the element $\sigma_{q,n}$, where

$$\sigma_{q,n}(x) = x^q \quad (x \in \mathbb{F}_{q^n}).$$

5: LEMMA The \mathbb{F}_{q^n} are finite abelian extensions of \mathbb{F}_q and they comprise all the finite extensions of \mathbb{F}_q , hence the algebraic closure of $\bigcup_n \mathbb{F}_{q^n}$ is \mathbb{F}_q^{ab} .

6: THEOREM There is a 1-to-1 correspondence between the finite abelian extensions of \mathbb{F}_q and the subgroups of \mathbb{Z} of finite index which is given by

$$\mathbb{F}_{q^n} \longleftrightarrow n\mathbb{Z} \quad (n \geq 1).$$

Schematically:

$$\begin{array}{ccccccc}
 \mathbb{F}_q & \subset & \mathbb{F}_{q^2} & \subset & \mathbb{F}_{q^4} & & \mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \\
 \cap & & \cap & & & & \cup \quad \cup \\
 \mathbb{F}_{q^3} & \subset & \mathbb{F}_{q^6} & & \longleftrightarrow & 3\mathbb{Z} \supset 6\mathbb{Z} & . \\
 \cap & & & & & \cup & \\
 \mathbb{F}_{q^9} & & & & & 9\mathbb{Z} &
 \end{array}$$

The “class field” aspect of all this is the existence of a canonical homomorphism

$$\mathrm{rec}_q : \mathbb{Z} \longrightarrow \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q).$$

7: NOTATION Define

$$\sigma_q \in \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$$

by

$$\sigma_q(x) = x^q.$$

8: N.B. Under the arrow of restriction

$$\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q),$$

σ_q is sent to $\sigma_{q,n}$.

9: DEFINITION

$$\mathrm{rec}_q(k) = \sigma_q^k \quad (k \in \mathbb{Z}).$$

10: LEMMA The identification

$$\mathbb{Z}/n\mathbb{Z} \approx \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

is the arrow $k \rightarrow \sigma_{q,n}^k$.

On general grounds,

$$\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q) = \varprojlim \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

[Note: The open subgroups of $\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$ are the $\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_{q^n})$ and

$$\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)/\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_{q^n}) \approx \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q).]$$

Therefore

$$\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q) \approx \varprojlim \mathbb{Z}/n\mathbb{Z},$$

another realization of the RHS being $\prod_p \mathbb{Z}_p$ which if invoked leads to

$$\sigma_q \longleftrightarrow (1, 1, 1, \dots).$$

11: N.B. The composition

$$\mathbb{Z} \xrightarrow{\text{rec}_q} \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q) \approx \varprojlim \mathbb{Z}/n\mathbb{Z}$$

coincides with the canonical map

$$k \rightarrow (k \bmod n)_n.$$

12: REMARK Give \mathbb{Z} the discrete topology —then

$$\text{rec}_q : \mathbb{Z} \longrightarrow \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$$

is continuous and injective but it is not a homeomorphism ($\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$ is compact).

[Note: The image $\text{rec}_q(\mathbb{Z})$ is the cyclic subgroup $\langle \sigma_q \rangle$ generated by σ_q . And:

- $\langle \sigma_q \rangle \neq \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$
- $\overline{\langle \sigma_q \rangle} = \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q).$

13: SCHOLIUM The finite abelian extensions of \mathbb{F}_q correspond 1-to-1 with the open subgroups of $\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$.

[Quote the appropriate facts from infinite Galois theory.]

14: SCHOLIUM The open subgroups of $\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$ correspond 1-to-1 with the open subgroups of \mathbb{Z} of finite index.

[Given an open subgroup $U \subset \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$, send it to $\text{rec}_q^{-1}(U) \subset \mathbb{Z}$ (discrete topology). Explicated:

$$\text{rec}_q^{-1}(\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_{q^n})) = n\mathbb{Z}.]$$

APPENDIX

The norm map

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \longrightarrow \mathbb{F}_q^\times$$

is surjective.

[Let $x \in \mathbb{F}_{q^n}^\times$:

$$\begin{aligned} N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) &= \prod_{i=0}^{n-1} (\sigma_{q,n})^{i_x} \\ &= \prod_{i=0}^{n-1} x^{q^i} \\ &= x^{\sum_{i=0}^{n-1} q^i} \end{aligned}$$

$$= x^{(q^n-1)/(q-1)}.$$

Specialize now and take for x a generator of $\mathbb{F}_{q^n}^\times$, hence x is of order q^n-1 , hence $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$ is of order $q-1$, hence is a generator of \mathbb{F}_q .]

§21. LOCAL CLASS FIELD THEORY

Let \mathbb{K} be a local field –then there exists a unique continuous homomorphism

$$\text{rec}_{\mathbb{K}} : \mathbb{K}^{\times} \longrightarrow \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}),$$

the so-called reciprocity map, that has the properties delineated in the results that follow.

1: CHART

finite field	\mathbb{K}	\mathbb{Z}	$\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$
local field	\mathbb{K}	\mathbb{K}^{\times}	$\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$

2: CONVENTION An abelian extension is a Galois extension whose Galois group is abelian.

3: SCHOLIUM The finite abelian extensions \mathbb{L} of \mathbb{K} correspond 1-to-1 with the open subgroups of $\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$:

$$\mathbb{L} \longleftrightarrow \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{L}).$$

[Note: $\text{Gal}(\mathbb{L}/\mathbb{K})$ is a homomorphic image of $\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$:

$$\text{Gal}(\mathbb{L}/\mathbb{K}) \approx \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})/\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{L}).]$$

4: LEMMA Suppose that \mathbb{L} is a finite extension of \mathbb{K} –then

$$N_{\mathbb{L}/\mathbb{K}} : \mathbb{L}^{\times} \rightarrow \mathbb{K}^{\times}$$

is continuous, sends open sets to open sets, and closed sets to closed sets.

5: LEMMA Suppose that \mathbb{L} is a finite extension of \mathbb{K} –then

$$[\mathbb{K}^\times : N_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^\times)] \leq [\mathbb{L} : \mathbb{K}].$$

6: LEMMA Suppose that \mathbb{L} is a finite extension of \mathbb{K} –then

$$[\mathbb{K}^\times : N_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^\times)] = [\mathbb{L} : \mathbb{K}].$$

iff \mathbb{L}/\mathbb{K} is abelian.

7: NOTATION Given a finite abelian extension \mathbb{L}/\mathbb{K} , denote the composition

$$\mathbb{K}^\times \xrightarrow{\text{rec}_{\mathbb{K}}} \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) \xrightarrow{\pi_{\mathbb{L}/\mathbb{K}}} \text{Gal}(\mathbb{K}/\mathbb{L})$$

by $(., \mathbb{L}/\mathbb{K})$, the norm residue symbol.

8: THEOREM Suppose that \mathbb{L} is a finite extension of \mathbb{K} –then the kernel of $(., \mathbb{L}/\mathbb{K})$ is $N_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^\times)$, hence

$$\mathbb{K}^\times / N_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^\times) \approx \text{Gal}(\mathbb{L}/\mathbb{K}).$$

9: EXAMPLE Take $\mathbb{K} = \mathbb{R}$, thus $\mathbb{K}^{\text{ab}} = \mathbb{C}$ and

$$N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) = \mathbb{R}_{>0}^\times.$$

Moreover,

$$\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}_{\mathbb{C}}, \sigma\},$$

where σ is the complex conjugation. Define now

$$\text{rec}_{\mathbb{R}} : \mathbb{R}^\times \longrightarrow \text{Gal}(\mathbb{R}^{\text{ab}}/\mathbb{R})$$

by stipulating that

$$\text{rec}_{\mathbb{R}}(\mathbb{R}_{>0}^{\times}) = \text{id}_{\mathbb{C}}, \quad \text{rec}_{\mathbb{R}}(\mathbb{R}_{<0}^{\times}) = \sigma.$$

10: EXAMPLE Take $\mathbb{K} = \mathbb{C}$ –then $\mathbb{K}^{\text{ab}} = \mathbb{C} = \mathbb{K}$ and matters in this situation are trivial.

11: THEOREM The arrow

$$\mathbb{L} \longrightarrow \text{N}_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^{\times})$$

is a bijection between the finite abelian extensions of \mathbb{K} and the open subgroups of finite index of \mathbb{K}^{\times} .

12: THEOREM The arrow $U \rightarrow \text{rec}_{\mathbb{K}}^{-1}(U)$ is a bijection between open subgroups of $\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$ and the open subgroups of finite index of \mathbb{K}^{\times} .

From this point forward, it will be assumed that \mathbb{K} is non-archimedean, hence is a finite extension of \mathbb{Q}_p for some p (cf. §5, #13).

13: LEMMA $\text{rec}_{\mathbb{K}}$ is injective and its image is a proper, dense subgroup of $\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$.

14: LEMMA

$$(\mathbb{R}^{\times}, \mathbb{L}/\mathbb{K}) = \text{Gal}(\mathbb{L}/\mathbb{K}_{\text{ur}}),$$

where \mathbb{K}_{ur} is the largest unramified extension of \mathbb{K} contained in \mathbb{L} (cf. §5, #33).

[Note: The image

$$(1 + p^i, \mathbb{L}/\mathbb{K}) = G^i \quad (i \geq 1),$$

the i^{th} ramification group in the upper numbering (conventionally, one puts

$$G^0 = \text{Gal}(\mathbb{L}/\mathbb{K}_{\text{ur}})$$

and refers to it as the inertia group.)]

Working within \mathbb{K}^{sep} , the extension \mathbb{K}^{ur} generated by the finite unramified extensions of \mathbb{K} is called the maximal unramified extension of \mathbb{K} . This is a Galois extension and

$$\text{Gal}(\mathbb{K}^{\text{ur}}/\mathbb{K}) \approx \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q),$$

where $\mathbb{F}_q = R/P$ (cf. §5, #19).

15: REMARK The finite unramified extensions \mathbb{L} of \mathbb{K} correspond 1-to-1 with the finite extensions of $R/P = \mathbb{F}_q$ and

$$\text{Gal}(\mathbb{L}/\mathbb{K}) \approx \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \quad (n = [\mathbb{L} : \mathbb{K}]).$$

16: LEMMA \mathbb{K}^{ur} is the field obtained by adjoining to \mathbb{K} all roots of unity having order prime to p .

17: APPLICATION \mathbb{K}^{ur} is a subfield of \mathbb{K}^{ab} .

[Cyclotomic extensions are Galois and abelian.]

18: THEOREM There is a commutative diagram

$$\begin{array}{ccc} \mathbb{K}^\times & \xrightarrow{\text{rec}_{\mathbb{K}}} & \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) \\ v_{\mathbb{K}} \downarrow & & \downarrow \\ \mathbb{Z} & \xrightarrow{\text{rec}_q} & \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q) \end{array},$$

the vertical arrow on the right being the composition

$$\begin{aligned} \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) &\rightarrow \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})/\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}^{\text{ur}}) \\ &\approx \text{Gal}(\mathbb{K}^{\text{ur}}/\mathbb{K}) \\ &\approx \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q). \end{aligned}$$

[Note: $\forall a \in \mathbb{K}^\times$,

$$\text{mod}_{\mathbb{K}}(a) = q^{-\text{ord}_{\mathbb{K}}(a)}.]$$

19: N.B. The image of

$$\text{rec}_{\mathbb{K}}(\pi)|K^{\text{ur}} \in \text{Gal}(\mathbb{K}^{\text{ur}}/\mathbb{K})$$

in $\text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$ is σ_q (cf. §20, #7).

[Note: If \mathbb{L} is a finite unramified extension of \mathbb{K} and if $\tilde{\sigma}_{q,n}$ is the generator of $\text{Gal}(\mathbb{L}/\mathbb{K})$ which is the lift of the generator $\sigma_{q,n}$ of $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ ($n = [\mathbb{L} : \mathbb{K}]$), then

$$(\pi, \mathbb{L}/\mathbb{K}) = \tilde{\sigma}_{q,n}.]$$

20: FUNCTORALITY Suppose that \mathbb{L}/\mathbb{K} is a finite extension of \mathbb{K} –then the diagram

$$\begin{array}{ccc} \mathbb{L}^\times & \xrightarrow{\text{rec}_{\mathbb{L}}} & \text{Gal}(\mathbb{L}^{\text{ab}}/\mathbb{L}) \\ \text{N}_{\mathbb{L}/\mathbb{K}} \downarrow & & \downarrow \text{res} \\ \mathbb{K}^\times & \xrightarrow{\text{rec}_{\mathbb{K}}} & \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) \end{array}$$

commutes.

21: DEFINITION Given a Hausdorff topological group G , let G^* be its commutator subgroup, and put $G^{\text{ab}} = G/\overline{G^*}$ –then $\overline{G^*}$ is a closed normal subgroup of G and G^{ab} is abelian, the topological abelianization of G .

22: EXAMPLE

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})^{\text{ab}} = \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}).$$

23: CONSTRUCTION Let G be a Hausdorff topological group and let H be a closed subgroup of finite index –then the transfer homomorphism $\mathsf{T} : G^{\text{ab}} \rightarrow H^{\text{ab}}$ is defined as follows: Choose a section $s : H \backslash G \rightarrow G$ and for $x \in G$, put

$$\mathsf{T}(x\overline{G^*}) = \prod_{\alpha \in H \backslash G} h_{x,\alpha}(\text{mod } \overline{H^*}),$$

where $h_{x,\alpha} \in H$ is defined by

$$s(\alpha)x = h_{x,\alpha}s(\alpha x).$$

24: EXAMPLE Suppose that \mathbb{L}/\mathbb{K} is a finite extension –then $\mathbb{L}^{\text{sep}} \approx \mathbb{K}^{\text{sep}}$ and

$$\text{Gal}(\mathbb{L}^{\text{sep}}/\mathbb{L}) \subset \text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})$$

is a closed subgroup of finite index (viz. $[\mathbb{L} : \mathbb{K}]$), hence there is a transfer homomorphism

$$\mathsf{T} : \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) \longrightarrow \text{Gal}(\mathbb{L}^{\text{ab}}/\mathbb{L}).$$

25: THEOREM The diagram

$$\begin{array}{ccc} \mathbb{L}^\times & \xrightarrow{\text{rec}_{\mathbb{L}}} & \text{Gal}(\mathbb{L}^{\text{ab}}/\mathbb{L}) \\ \uparrow & & \uparrow \mathsf{T} \\ \mathbb{K}^\times & \xrightarrow{\text{rec}_{\mathbb{K}}} & \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) \end{array}$$

commutes.

§22. WEIL GROUPS: THE ARCHIMEDEAN CASE

1: DEFINITION Put $W_{\mathbb{C}} = \mathbb{C}^{\times}$, call it the Weil group of \mathbb{C} , and leave it at that.

2: DEFINITION Put

$$W_{\mathbb{R}} = \mathbb{C}^{\times} \cup J\mathbb{C}^{\times} \quad (\text{disjoint union}) \quad (J \text{ a formal symbol}),$$

where $J^2 = -1$ and $JzJ^{-1} = \bar{z}$ (obvious topology on $W_{\mathbb{R}}$). Accordingly, there is a nonsplit short exact sequence

$$1 \longrightarrow \mathbb{C}^{\times} \longrightarrow W_{\mathbb{R}} \longrightarrow \text{Gal}(\mathbb{C}/\mathbb{R}) \longrightarrow 1,$$

the image of J in $\text{Gal}(\mathbb{C}/\mathbb{R})$ being complex conjugation.

[Note: $H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^{\times})$ is cyclic of order 2, thus up to equivalence of extensions of $\text{Gal}(\mathbb{C}/\mathbb{R})$ by \mathbb{C}^{\times} per the canonical action of $\text{Gal}(\mathbb{C}/\mathbb{R})$ on \mathbb{C}^{\times} , there are two possibilities:

1. A split extension

$$1 \longrightarrow \mathbb{C}^{\times} \longrightarrow E \longrightarrow \text{Gal}(\mathbb{C}/\mathbb{R}) \longrightarrow 1.$$

2. A nonsplit extension

$$1 \longrightarrow \mathbb{C}^{\times} \longrightarrow E \longrightarrow \text{Gal}(\mathbb{C}/\mathbb{R}) \longrightarrow 1.$$

The Weil group W is a representative of the second situation which is why we took $J^2 = -1$ (rather than $J^2 = +1$).]

3: LEMMA The commutator subgroup $W_{\mathbb{R}}^*$ of $W_{\mathbb{R}}$ consists of all elements of the form $JzJ^{-1}z^{-1} = \frac{\bar{z}}{z}$, i.e., $W_{\mathbb{R}}^* = S$, thus is closed.

Let

$$\text{pr} : W_{\mathbb{R}} \longrightarrow \mathbb{R}^{\times}$$

be the map sending J to -1 and z to $|z|^2$.

4: LEMMA S is the kernel of pr and pr is surjective.

5: LEMMA The arrow

$$\text{pr}^{\text{ab}} : W_{\mathbb{R}}^{\text{ab}} \longrightarrow \mathbb{R}^{\times}$$

induced by pr is an isomorphism.

6: REMARK The inverse $\mathbb{R}^{\times} \rightarrow W_{\mathbb{R}}^{\text{ab}}$ of pr^{ab} is characterized by the conditions

$$\begin{cases} -1 \rightarrow JW_{\mathbb{R}}^* \\ x \rightarrow \sqrt{x} W_{\mathbb{R}}^* \quad (x > 0) \end{cases}.$$

7: NOTATION Define

$$\|\cdot\| : W_{\mathbb{R}} \longrightarrow \mathbb{R}_{>0}^{\times}$$

by the prescription

$$\|z\| = z\bar{z} \quad (z \in \mathbb{C}), \quad \|J\| = 1.$$

8: N.B. $\|\cdot\|$ drops to a continuous homomorphism $W_{\mathbb{R}}^{\text{ab}} \rightarrow \mathbb{R}_{>0}^{\times}$.

9: DEFINITION A representation of $W_{\mathbb{R}}$ is a continuous homomorphism $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$, where V is a finite dimensional complex vector space.

10: EXAMPLE If $s \in \mathbb{C}$, then the assignment $w \rightarrow \|w\|^s$ is a 1-dimensional representation of $W_{\mathbb{R}}$, i.e., is a character.

11: N.B. If χ is a character of \mathbb{R}^\times , then $\chi \circ \text{pr}$ is a character of $W_{\mathbb{R}}$ and all such have this form.

[For any $\rho \in \widetilde{W}_{\mathbb{R}}$,

$$\rho(\bar{z}) = \rho(JzJ^{-1}) = \rho(J)\rho(z)\rho(J)^{-1} = \rho(z).$$

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 \mathbb{R}^\times are described in §7, #11, thus the 1-dimensional representations of $W_{\mathbb{R}}$ 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 \mathbb{C} is algebraically closed]

14: DEFINITION A representation $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$ is semisimple if $\forall w \in W_{\mathbb{R}}$, $\rho(w) : V \rightarrow V$ is semisimple.

15: DEFINITION A representation $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$ is irreducible if $V \neq 0$, and the only ρ -invariant subspaces are 0 and V .

The irreducible 1-dimensional representations of $W_{\mathbb{R}}$ are its characters (which, of course, are automatically semisimple).

16: LEMMA If $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$ is a semisimple irreducible representation of $W_{\mathbb{R}}$ of dimension > 1 , then $\dim V = 2$.

PROOF There is a nonzero vector $v \in V$ and a character $\chi : \mathbb{C}^{\times} \rightarrow \mathbb{C}^{\times}$ such that $\forall z \in \mathbb{C}^{\times}$,

$$\rho(z)v = \chi(z)v.$$

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

$$\begin{cases} \rho(z)\rho(J)v = \rho(zJ)v = \rho(J\bar{z})v = \rho(J)\rho(\bar{z})v = \rho(J)\chi(\bar{z})v \\ \rho(J)\rho(J)v = \rho(J^2)v = \rho(-1)v = \chi(-1)v. \end{cases}.$$

Given an integer k and a complex number s , define a character $\chi_{k,s} : \mathbb{C}^{\times} \rightarrow \mathbb{C}^{\times}$ by the prescription

$$\chi_{k,s}(z) = \left(\frac{z}{|z|}\right)^k (|z|^2)^s$$

and let $\rho_{k,s} = \text{ind}_{\chi_{k,s}}$ be the representation of $W_{\mathbb{R}}$ 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

$$\begin{cases} \rho_1 : W_{\mathbb{R}} \rightarrow \text{GL}(V_1) \\ \rho_2 : W_{\mathbb{R}} \rightarrow \text{GL}(V_2) \end{cases}$$

be representations of $W_{\mathbb{R}}$ —then (ρ_1, V_1) is equivalent to (ρ_2, V_2) if there exists an isomorphism $f : V_1 \rightarrow V_2$ such that $\forall w \in W_{\mathbb{R}}$,

$$f \circ \rho_1(w) = \rho_2(w) \circ f.$$

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: LEMMA Every 2-dimensional semisimple irreducible representation of $W_{\mathbb{R}}$ is equivalent to a unique $\rho_{k, s}$ ($k > 0$).

23: N.B. Therefore the equivalence classes of 2-dimensional semisimple irreducible representations of $W_{\mathbb{R}}$ are parameterized by the points of $\mathbb{N} \times \mathbb{C}$.

24: DEFINITION A representation $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$ is completely reducible if V is the direct sum of a collection of irreducible ρ -invariant subspaces.

25: LEMMA Let $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$ be a semisimple representation —then ρ is completely reducible.

PROOF The characters of \mathbb{C}^{\times} are of the form $z \rightarrow z^{\mu} \bar{z}^{\nu}$ with $\mu, \nu \in \mathbb{C}, \mu - \nu \in \mathbb{Z}$ and V is the direct sum of subspaces $V_{\mu, \nu}$, where $\rho(z)|_{V_{\mu, \nu}} = z^{\mu} \bar{z}^{\nu} \text{id}_{V_{\mu, \nu}}$. Claim:

$$\rho(J)V_{\mu, \nu} = V_{\nu, \mu}.$$

Proof: $\forall v \in V_{\mu, \nu}$,

$$\rho(z)\rho(J)v = \rho(J\bar{z}J^{-1})\rho(J)v$$

$$\begin{aligned}
&= \rho(J)\rho(\bar{z})\rho(J^{-1})\rho(J)v \\
&= \rho(J)\rho(\bar{z})v \\
&= \rho(J)\bar{z}^\mu z^\nu v \\
&= \rho(J)z^\nu \bar{z}^\mu v \\
&= z^\nu \bar{z}^\mu \rho(J)v.
\end{aligned}$$

Proceeding:

- $\mu = \nu$ Choose a basis of eigenvectors for $\rho(J)$ on $V_{\mu,\nu}$ –then the span of each eigenvector is a 1-dimensional ρ -invariant subspace.
- $\mu \neq \nu$ Choose a basis v_1, \dots, v_r for $V_{\mu,\nu}$ and put $v'_i = \rho(J)v_i$ ($1 \leq i \leq r$) –then $\mathbb{C}v_i \oplus \mathbb{C}v'_i$ is a 2-dimensional ρ -invariant subspace and the direct sum

$$\bigoplus_{i=1}^r (\mathbb{C}v_i \oplus \mathbb{C}v'_i)$$

equals

$$V_{\mu,\nu} \oplus V_{\nu,\mu}.$$

26: REMARK Suppose that $\rho : W_{\mathbb{R}} \rightarrow \text{GL}(V)$ is a representation –then

$$\begin{aligned}
J^2 = -1 &\implies (-1)J \cdot J = 1 \\
&\implies (-1)J = J^{-1}
\end{aligned}$$

\implies

$$\begin{aligned}
\rho(J)^{-1} &= \rho(J^{-1}) \\
&= \rho((-1)J) \\
&= \rho(-1)\rho(J).
\end{aligned}$$

On the other hand, if $J^2 = 1$ (the split extension situation (cf. #2)), then

$$\begin{aligned}\mathrm{id}_V &= \rho(1) \\ &= \rho(J^2) \\ &= \rho(J)\rho(J).\end{aligned}$$

\implies

$$\rho(J)^{-1} = \rho(J).$$

§23. WEIL GROUPS: THE NON-ARCHIMEDEAN CASE

Let \mathbb{K} be a non-archimedean local field.

1: NOTATION Put

$$\begin{cases} G_{\mathbb{K}} = \text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K}) \\ G_{\mathbb{K}}^{\text{ab}} = \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) \end{cases}.$$

2: N.B. Every character of $G_{\mathbb{K}}$ factors through $\overline{G_{\mathbb{K}}^*}$, hence gives rise to a character of $G_{\mathbb{K}}^{\text{ab}}$.

To study the characters of $G_{\mathbb{K}}^{\text{ab}}$, precompose with the reciprocity map $\text{rec}_{\mathbb{K}} : \mathbb{K}^{\times} \rightarrow G_{\mathbb{K}}^{\text{ab}}$, thus

$$\chi_{\mathbb{K}} : \begin{cases} (G_{\mathbb{K}}^{\text{ab}})^{\sim} \rightarrow (\mathbb{K}^{\times})^{\sim} \\ \chi \rightarrow \chi \circ \text{rec}_{\mathbb{K}} \end{cases}.$$

3: LEMMA $\chi_{\mathbb{K}}$ is a homomorphism.

4: LEMMA $\chi_{\mathbb{K}}$ is injective.

PROOF Suppose that

$$\chi_{\mathbb{K}}(\chi) = \chi \circ \text{rec}_{\mathbb{K}}$$

is trivial – then $\chi|_{\text{Im rec}_{\mathbb{K}}} = 1$. But $\text{Im rec}_{\mathbb{K}}$ is dense in $G_{\mathbb{K}}^{\text{ab}}$ (cf. §21, #13), so by continuity, $\chi \equiv 1$.

5: LEMMA $\chi_{\mathbb{K}}$ is not surjective.

PROOF $G_{\mathbb{K}}^{\text{ab}}$ is compact abelian and totally disconnected. Therefore $(G_{\mathbb{K}}^{\text{ab}})^{\sim} = (G_{\mathbb{K}}^{\text{ab}})^{\wedge}$ and every χ is unitary and of finite order (cf. §7, #7 and §8, #2), thus the $\chi_{\mathbb{K}}(\chi)$ are unitary and of finite order. But there are characters of \mathbb{K}^{\times} for which this is not the case.

6: N.B. The failure of $\chi_{\mathbb{K}}$ to be surjective will be remedied below (cf. #19).

The kernel of the arrow

$$\mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K}) \longrightarrow \mathrm{Gal}(\mathbb{K}^{\mathrm{ur}}/\mathbb{K})$$

of restriction is $\mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K}^{\mathrm{ur}})$ and there is an exact sequence

$$1 \longrightarrow \mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K}^{\mathrm{ur}}) \longrightarrow \mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K}) \longrightarrow \mathrm{Gal}(\mathbb{K}^{\mathrm{ur}}/\mathbb{K}) \longrightarrow 1.$$

Identify

$$\mathrm{Gal}(\mathbb{K}^{\mathrm{ur}}/\mathbb{K})$$

with

$$\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$$

and put

$$W(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) = \langle \sigma_q \rangle \quad (\text{discrete topology}).$$

7: DEFINITION The Weil group $W(\mathbb{K}^{\mathrm{sep}}/\mathbb{K})$ is the inverse image of $W(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ in $\mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K})$, i.e., the elements of $\mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K})$ which induce an integral power of σ_q .

8: NOTATION Abbreviate $W(\mathbb{K}^{\mathrm{sep}}/\mathbb{K})$ to $W_{\mathbb{K}}$, hence $W_{\mathbb{K}} \subset G_{\mathbb{K}}$.

Setting

$$I_{\mathbb{K}} = \mathrm{Gal}(\mathbb{K}^{\mathrm{sep}}/\mathbb{K}^{\mathrm{ur}}) \quad (\text{the } \underline{\text{inertia group}}),$$

there is an exact sequence

$$\begin{array}{ccccccc} 1 & \longrightarrow & I_{\mathbb{K}} & \longrightarrow & W_{\mathbb{K}} & \longrightarrow & W(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \longrightarrow 1 \\ & & & & & & \updownarrow \approx \\ & & & & & & \mathbb{Z} \end{array} .$$

[Note: Fix an element $\tilde{\sigma}_q \in W_{\mathbb{K}}$ which maps to σ_q –then structurally, $W_{\mathbb{K}}$ is the disjoint union

$$\bigcup_{n \in \mathbb{Z}} (\tilde{\sigma}_q)^n I_{\mathbb{K}}.]$$

Topologize $W_{\mathbb{K}}$ by taking for a neighborhood basis at the identity the

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L}) \cap I_{\mathbb{K}},$$

where \mathbb{L} is a finite Galois extension of \mathbb{K} .

9: REMARK $I_{\mathbb{K}}$ has the relative topology per the inclusion $I_{\mathbb{K}} \rightarrow G_{\mathbb{K}}$ and any splitting $\mathbb{Z} \rightarrow W_{\mathbb{K}}$ induces an isomorphism $W_{\mathbb{K}} \approx I_{\mathbb{K}} \times \mathbb{Z}$ of topological groups, where \mathbb{Z} has the discrete topology.

10: LEMMA $W_{\mathbb{K}}$ is a totally disconnected locally compact group.

[Note: $W_{\mathbb{K}}$ is not compact]

11: LEMMA The inclusion $W_{\mathbb{K}} \rightarrow G_{\mathbb{K}}$ is continuous and has a dense image.

12: LEMMA $I_{\mathbb{K}}$ is open in $W_{\mathbb{K}}$.

13: LEMMA $I_{\mathbb{K}}$ is a maximal compact subgroup of $W_{\mathbb{K}}$.

Suppose that \mathbb{L}/\mathbb{K} is a finite extension of \mathbb{K} –then $G_{\mathbb{L}} \subset G_{\mathbb{K}}$ is the subgroup of $G_{\mathbb{K}}$ fixing \mathbb{L} , hence

$$W_{\mathbb{L}} \subset G_{\mathbb{L}} \subset G_{\mathbb{K}}.$$

14: LEMMA

$$W_{\mathbb{L}} = G_{\mathbb{L}} \cap W_{\mathbb{K}} \subset W_{\mathbb{K}}$$

is open and of finite index in $W_{\mathbb{K}}$, it being normal in $W_{\mathbb{K}}$ iff \mathbb{L}/\mathbb{K} is Galois.

15: THEOREM The arrow

$$\mathbb{L} \rightarrow W_{\mathbb{L}}$$

is a bijection between the finite extensions of \mathbb{K} and the open subgroups of $W_{\mathbb{K}}$.

[By contrast, the arrow

$$\mathbb{L} \rightarrow \text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L})$$

is a bijection between the finite extensions of \mathbb{K} and the open subgroups of $G_{\mathbb{K}}$.]

16: LEMMA

$$\overline{W_{\mathbb{K}}^*} = \overline{G_{\mathbb{K}}^*}.$$

17: APPLICATION The homomorphism $W_{\mathbb{K}}^{\text{ab}} \rightarrow G_{\mathbb{K}}^{\text{ab}}$ is 1-to-1.

18: THEOREM The image of $\text{rec}_{\mathbb{K}} : \mathbb{K}^{\times} \rightarrow G_{\mathbb{K}}^{\text{ab}}$ is $W_{\mathbb{K}}^{\text{ab}}$ and the induced map $\mathbb{K}^{\times} \rightarrow W_{\mathbb{K}}^{\text{ab}}$ is an isomorphism of topological groups (cf. §21, #13).

The characters of $W_{\mathbb{K}}$ “are” the characters of $W_{\mathbb{K}}^{\text{ab}}$, so we have:

19: SCHOLIUM There is a bijective correspondence between the characters of $W_{\mathbb{K}}$ and the characters of \mathbb{K}^{\times} or still, there is a bijective correspondence between the 1-dimensional representations of $W_{\mathbb{K}}$ and the 1-dimensional representations of $\text{GL}_1(\mathbb{K})$.

Suppose that \mathbb{L}/\mathbb{K} is a finite Galois extension of \mathbb{K} —then $G_{\mathbb{L}} \subset G_{\mathbb{K}}$ and

$$G_{\mathbb{K}}/G_{\mathbb{L}} \approx \text{Gal}(\mathbb{L}/\mathbb{K})$$

is finite of cardinality $[\mathbb{L} : \mathbb{K}]$. Since $W_{\mathbb{K}}$ is dense in $G_{\mathbb{K}}$, it follows that the image of the arrow

$$\begin{cases} W_{\mathbb{K}} \longrightarrow G_{\mathbb{K}}/G_{\mathbb{L}} \\ w \longrightarrow wG_{\mathbb{L}} \end{cases}$$

is all of $G_{\mathbb{K}}/G_{\mathbb{L}}$, its kernel being those $w \in W_{\mathbb{K}}$ such that $w \in G_{\mathbb{L}}$, i.e., its kernel is $G_{\mathbb{L}} \cap W_{\mathbb{K}}$ or still, is $W_{\mathbb{L}}$.

20: LEMMA

$$W_{\mathbb{K}}/W_{\mathbb{L}} \approx G_{\mathbb{K}}/G_{\mathbb{L}} \approx \text{Gal}(\mathbb{L}/\mathbb{K}).$$

21: LEMMA $\overline{W_{\mathbb{L}}^*}$ is a normal subgroup of $W_{\mathbb{K}}$.

[Bearing in mind that $W_{\mathbb{L}}$ is a normal subgroup of $W_{\mathbb{K}}$, if $\alpha, \beta \in W_{\mathbb{L}}^*$ and if $\gamma \in W_{\mathbb{K}}$, 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

$$1 \longrightarrow W_{\mathbb{L}}/\overline{W_{\mathbb{L}}^*} \longrightarrow W_{\mathbb{K}}/\overline{W_{\mathbb{L}}^*} \longrightarrow (W_{\mathbb{K}}/\overline{W_{\mathbb{L}}^*})/(W_{\mathbb{L}}/\overline{W_{\mathbb{L}}^*}) \longrightarrow 1$$

or still, there is an exact sequence

$$1 \longrightarrow W_{\mathbb{L}}/\overline{W_{\mathbb{L}}^*} \longrightarrow W_{\mathbb{K}}/\overline{W_{\mathbb{L}}^*} \longrightarrow W_{\mathbb{K}}/W_{\mathbb{L}} \longrightarrow 1.$$

22: NOTATION Put

$$W(\mathbb{L}, \mathbb{K}) = W_{\mathbb{K}}/\overline{W_{\mathbb{L}}^*}.$$

23: SCHOLIUM There is an exact sequence

$$1 \longrightarrow W_{\mathbb{L}}^{\text{ab}} \longrightarrow W(\mathbb{L}, \mathbb{K}) \longrightarrow W_{\mathbb{K}}/W_{\mathbb{L}} \longrightarrow 1$$

and a diagram

$$\begin{array}{ccccc} W_{\mathbb{L}}^{\text{ab}} & \longrightarrow & W(\mathbb{L}, \mathbb{K}) & \longrightarrow & W_{\mathbb{K}}/W_{\mathbb{L}} \\ \uparrow \text{rec}_{\mathbb{L}} & & & & \downarrow \approx \\ 1 & \longrightarrow & \mathbb{L}^{\times} & & \text{Gal}(\mathbb{L}/\mathbb{K}) \longrightarrow 1 \end{array} .$$

24: NOTATION Given $w \in W_{\mathbb{K}}$, let $\|w\|$ denote the effect on w of passing from $W_{\mathbb{K}}$ to $\mathbb{R}_{>0}^{\times}$ via the arrows

$$W_{\mathbb{K}} \longrightarrow W_{\mathbb{K}}^{\text{ab}} \xrightarrow{\text{rec}_{\mathbb{K}}^{-1}} \mathbb{K}^{\times} \xrightarrow{\text{mod}_{\mathbb{K}}} \mathbb{R}_{>0}^{\times} .$$

25: LEMMA $\|\cdot\| : W_{\mathbb{K}} \rightarrow \mathbb{R}_{>0}^{\times}$ is a continuous homomorphism and its kernel is $I_{\mathbb{K}}$.

[Under the arrow

$$W_{\mathbb{K}} \rightarrow W_{\mathbb{K}}^{\text{ab}},$$

$I_{\mathbb{K}}$ drops to

$$\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}^{\text{ur}}) \subset W_{\mathbb{K}}^{\text{ab}}.$$

Consider now the arrow

$$\text{rec}_{\mathbb{K}} : \mathbb{K}^{\times} \longrightarrow W_{\mathbb{K}}^{\text{ab}}.$$

Then R^{\times} is sent to $\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}^{\text{ur}})$ and a prime element $\pi \in R$ is sent to an element $\tilde{\sigma}_q$ in $W_{\mathbb{K}}^{\text{ab}}$ whose image in $W(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q)$ is σ_q . And

$$W_{\mathbb{K}}^{\text{ab}} = \bigcup_{n \in \mathbb{Z}} (\tilde{\sigma}_q)^n \text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}^{\text{ur}}).]$$

26: DEFINITION A representation of $W_{\mathbb{K}}$ is a continuous homomorphism $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$, where V is a finite dimensional complex vector space.

27: LEMMA A homomorphism $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ is continuous per the usual topology on $\text{GL}(V)$ iff it is continuous per the discrete topology on $\text{GL}(V)$.

[$\text{GL}(V)$ has no small subgroups.]

28: SCHOLIUM The kernel of every representation of $W_{\mathbb{K}}$ is trivial on an open subgroup J of $I_{\mathbb{K}}$. Conversely, if $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ is a homomorphism which is trivial on an open subgroup J of $I_{\mathbb{K}}$, then the inverse image of any subset of $\text{GL}(V)$ is a union of cosets of J , hence is open, hence ρ is continuous, so by definition is a representation of $W_{\mathbb{K}}$.

29: EXAMPLE Suppose that \mathbb{L}/\mathbb{K} is a finite Galois extension of \mathbb{K} –then

$$\begin{aligned} W_{\mathbb{L}} \cap I_{\mathbb{K}} &= G_{\mathbb{L}} \cap W_{\mathbb{K}} \cap I_{\mathbb{K}} \\ &= G_{\mathbb{L}} \cap I_{\mathbb{K}} \end{aligned}$$

is an open subgroup of $I_{\mathbb{K}}$. But

$$W_{\mathbb{K}}/W_{\mathbb{L}} \approx \text{Gal}(\mathbb{L}/\mathbb{K}) \quad (\text{cf. \#20}).$$

Therefore every homomorphism $\text{Gal}(\mathbb{L}/\mathbb{K}) \rightarrow \text{GL}(V)$ lifts to a homomorphism $W_{\mathbb{K}} \rightarrow \text{GL}(V)$ which is trivial on an open subgroup of $I_{\mathbb{K}}$, hence is a representation of $W_{\mathbb{K}}$.

30: N.B. Representations of $W_{\mathbb{K}}$ arising in this manner are said to be of Galois type.

31: LEMMA A representation of $W_{\mathbb{K}}$ is of Galois type iff it has finite image.

32: EXAMPLE $\|\cdot\|$ is a character of $W_{\mathbb{K}}$ but as a representation, is not of Galois type.

33: LEMMA Let $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ be a representation –then the image $\rho(I_{\mathbb{K}})$ is finite.

PROOF Suppose that J is an open subgroup of $I_{\mathbb{K}}$ on which ρ is trivial. Since $I_{\mathbb{K}}$ is compact and J is open, the quotient $I_{\mathbb{K}}/J$ is finite, thus $\rho(I_{\mathbb{K}}) = \rho(I_{\mathbb{K}}/J)$ is finite.

34: DEFINITION A representation $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ is irreducible if $V \neq 0$ and the only ρ -invariant subspaces are 0 and V .

35: THEOREM Given an irreducible representation ρ of $W_{\mathbb{K}}$, there exists an irreducible representation $\tilde{\rho}$ of $W_{\mathbb{K}}$ and a complex parameter s such that $\rho \approx \tilde{\rho} \otimes \|\cdot\|^s$.

36: LEMMA Let $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ 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 $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ 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 $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ 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 $\forall w \in W_{\mathbb{K}}$.

§24. THE WEIL-DELIGNE GROUP

1: DEFINITION The Weil-Deligne group $WD_{\mathbb{K}}$ is the semidirect product $\mathbb{C} \rtimes W_{\mathbb{K}}$, the multiplication rule being

$$(z_1, w_1) (z_2, w_2) = (z_1 + \|w_1\| z_2, w_1 w_2).$$

[Note: The identity in $WD_{\mathbb{K}}$ is $(0, e)$ and the inverse of (z, w) is $(-\|w\|^{-1} z, w^{-1})$:

$$\begin{aligned} (z, w)(-\|w\|^{-1} z, w^{-1}) &= (z + \|w\| (-\|w\|^{-1} z), ww^{-1}) \\ &= (z - z, e) \\ &= (0, e).] \end{aligned}$$

2: N.B. The topology on $WD_{\mathbb{K}}$ is the product topology.

3: DEFINITION A Deligne representation of $W_{\mathbb{K}}$ is a triple (ρ, V, N) , where $\rho : W_{\mathbb{K}} \rightarrow \text{GL}(V)$ is a representation of $W_{\mathbb{K}}$ and $N : V \rightarrow V$ is a nilpotent endomorphism of V subject to the relation

$$\rho(w)N\rho(w)^{-1} = \|w\| N \quad (w \in W_{\mathbb{K}}).$$

[Note: $N = 0$ is admissible so every representation of $W_{\mathbb{K}}$ is a Deligne representation.]

4: EXAMPLE Take $V = \mathbb{C}^n$, hence $\text{GL}(V) = \text{GL}_n(\mathbb{C})$. Let e_0, e_1, \dots, e_{n-1} be the usual basis of V . Define ρ by the rule

$$\rho(w)e_i = \|w\|^i e_i \quad (w \in W_{\mathbb{K}}, 0 \leq i \leq n-1)$$

and define N by the rule

$$Ne_i = e_{i+1} \quad (0 \leq i \leq n-2), \quad Ne_{n-1} = 0.$$

Then the triple (ρ, V, N) is a Deligne representation of $W_{\mathbb{K}}$, the n -dimensional special representation, denoted $\mathrm{sp}(n)$.

5: DEFINITION A representation of $WD_{\mathbb{K}}$ is a continuous homomorphism $\rho' : WD_{\mathbb{K}} \rightarrow \mathrm{GL}(V)$ whose restriction to \mathbb{C} is complex analytic, where V is a finite dimensional complex vector space.

6: LEMMA Every Deligne representation (ρ, V, N) of $W_{\mathbb{K}}$ gives rise to a representation $\rho' : WD_{\mathbb{K}} \rightarrow \mathrm{GL}(V)$ of $WD_{\mathbb{K}}$.

PROOF Put

$$\rho'(z, w) = \exp(zN)\rho(w).$$

Then

$$\begin{aligned} \rho'(z_1, w_1)\rho'(z_2, w_2) &= \exp(z_1N)\rho(w_1)\exp(z_2N)\rho(w_2) \\ &= \exp(z_1N)\rho(w_1)\exp(z_2N)\rho(w_1^{-1})\rho(w_1)\rho(w_2) \\ &= \exp(z_1N)\exp(z_2\|w_1\|N)\rho(w_1w_2) \\ &= \exp(z_1N + z_2\|w_1\|N)\rho(w_1w_2) \\ &= \exp((z_1 + \|w_1\|z_2)N)\rho(w_1w_2) \\ &= \rho'(z_1 + \|w_1\|z_2, w_1w_2) \\ &= \rho'((z_1, w_1)(z_2, w_2)). \end{aligned}$$

[Note: The continuity of ρ' is manifest as is the complex analyticity of its restriction to \mathbb{C} .]

One can also go the other way but this is more involved.

7: RAPPEL If $T : V \rightarrow V$ is unipotent, then

$$\log T = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} (T - I)^n$$

is nilpotent.

8: SUBLEMMA Let $\rho' : WD_{\mathbb{K}} \rightarrow GL(V)$ be a representation of $WD_{\mathbb{K}}$ –then $\forall z \neq 0$, $\rho'(z, e)$ is unipotent.

9: SUBLEMMA Let $\rho' : WD_{\mathbb{K}} \rightarrow GL(V)$ be a representation of $WD_{\mathbb{K}}$ –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 .

10: LEMMA Every representation $\rho' : WD_{\mathbb{K}} \rightarrow GL(V)$ of $WD_{\mathbb{K}}$ gives rise to a Deligne representation (ρ, V, N) of $W_{\mathbb{K}}$.

PROOF Put

$$\rho = \rho'|_{\{0\}} \times W_{\mathbb{K}}, \quad N = \log \rho'(1, e).$$

Then $\forall w \in W_{\mathbb{K}}$,

$$\begin{aligned} \rho(w)N\rho(w)^{-1} &= \rho(w) \log \rho'(1, e) \rho(w)^{-1} \\ &= \rho(w) \left(\sum_{n \geq 1} \frac{(-1)^{n+1}}{n} (\rho'(1, e) - I)^n \right) \rho(w)^{-1} \\ &= \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} (\rho(w) \rho'(1, e) \rho(w)^{-1} - I)^n. \end{aligned}$$

And

$$\begin{aligned}
\rho(w)\rho'(1, e)\rho(w)^{-1} &= \rho'(0, w)\rho'(1, e)\rho'(0, w^{-1}) \\
&= \rho'((0, w)(1, e)(0, w^{-1})) \\
&= \rho'(\|w\|, w)(0, w^{-1}) \\
&= \rho'(\|w\|, e).
\end{aligned}$$

Therefore

$$\begin{aligned}
\rho(w)N\rho(w)^{-1} &= \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} (\rho'(\|w\|, e) - I)^n \\
&= \log \rho'(\|w\|, e) \\
&= \|w\| \log \rho'(\|w\|, e) / \|w\| \\
&= \|w\| \log \rho'(1, e) \\
&= \|w\| N.
\end{aligned}$$

11: OPERATIONS

• Direct Sum: Let (ρ_1, V_1, N_1) , (ρ_2, V_2, N_2) be Deligne representations –then their direct sum is the triple

$$(\rho_1 \oplus \rho_2, V_1 \oplus V_2, N_1 \oplus N_2).$$

• Tensor Product: Let (ρ_1, V_1, N_1) , (ρ_2, V_2, N_2) be Deligne representations –then their tensor product is the triple

$$(\rho_1 \otimes \rho_2, V_1 \otimes V_2, N_1 \otimes I_2 + I_1 \otimes N_2).$$

• Contragredient: Let (ρ, V, N) be a Deligne representation –then its contra-

gradient 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 $\forall f \in V^\vee, N^\vee(f) = f \circ N$).]

12: REMARK The definitions of \oplus, \otimes, \vee when transcribed to the “prime picture” are the usual representation-theoretic formalities applied to the group $WD_{\mathbb{K}}$.

13: N.B. Let

$$\begin{cases} (\rho_1, V_1, N_1) \\ (\rho_2, V_2, N_2) \end{cases}$$

be Deligne representations of $W_{\mathbb{K}}$ —then a morphism

$$(\rho_1, V_1, N_1) \rightarrow (\rho_2, V_2, N_2)$$

is a linear map $T : V_1 \rightarrow V_2$ such that

$$T\rho_1(w) = \rho_2(w)T \quad (w \in W_{\mathbb{K}})$$

and $TN_1 = N_2T$.

[Note: If T is a linear isomorphism, then the Deligne representations

$$\begin{cases} (\rho_1, V_1, N_1) \\ (\rho_2, V_2, N_2) \end{cases}$$

are said to be isomorphic.]

14: DEFINITION Suppose that (ρ, V, N) is a Deligne representation of $W_{\mathbb{K}}$ —then a subspace $V_0 \subset V$ is an invariant subspace if it is invariant under ρ and N .

15: LEMMA The kernel of N is an invariant subspace.

PROOF If $Nv = 0$, then $\forall w \in W_{\mathbb{K}}$,

$$N\rho(w)v = \|w^{-1}\| \rho(w)Nv = 0.$$

16: DEFINITION A Deligne representation (ρ, V, N) of $W_{\mathbb{K}}$ is indecomposable if V cannot be written as a direct sum of proper invariant subspaces.

17: EXAMPLE Consider $\mathrm{sp}(n)$ –then it is indecomposable.

[If $\mathbb{C}^n = S \oplus T$ was a nontrivial decomposition into proper invariant subspaces, then both $\begin{cases} S \cap \ker N \\ T \cap \ker N \end{cases}$ would be nontrivial.]

18: DEFINITION A Deligne representation (ρ, V, N) of $W_{\mathbb{K}}$ is semisimple if ρ is semisimple (cf. §23, #37).

19: EXAMPLE Consider $\mathrm{sp}(n)$ –then it is semisimple.

20: LEMMA Let π be an irreducible representation of $W_{\mathbb{K}}$ –then $\mathrm{sp}(n) \otimes \pi$ is semisimple and indecomposable.

[Note: Recall that π is identified with $(\pi, 0)$.]

21: THEOREM Every semisimple indecomposable Deligne representation of $W_{\mathbb{K}}$ is equivalent to a Deligne representation of the form $\mathrm{sp}(n) \otimes \pi$, where π is an irreducible representation of $W_{\mathbb{K}}$ and n is a positive integer.

22: THEOREM Let (ρ, V, N) be a semisimple Deligne representation of $W_{\mathbb{K}}$ –then there is a decomposition

$$(\rho, V, N) = \bigoplus_{i=1}^s \mathrm{sp}(n_i) \otimes \pi_i,$$

where π_i is an irreducible representation of $W_{\mathbb{K}}$ and n_i is a positive integer. Furthermore, if

$$(\rho, V, N) = \bigoplus_{j=1}^t \text{sp}(n'_j) \otimes \pi'_j$$

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

$$WD_{\mathbb{K}} = \mathbb{C} \rtimes W_{\mathbb{K}},$$

some authorities work with

$$SL(2, \mathbb{C}) \times W_{\mathbb{K}},$$

the rationale for this being that the semisimple representations of the two groups are the “same”.

Given $w \in W_{\mathbb{K}}$, let

$$h_w = \begin{pmatrix} \|w\|^{1/2} & 0 \\ 0 & \|w\|^{-1/2} \end{pmatrix}$$

and identify $z \in \mathbb{C}$ with

$$h_w = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}.$$

Then

$$h_w \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} h_w^{-1} = \begin{pmatrix} 1 & \|w\| z \\ 0 & 1 \end{pmatrix}.$$

But conjugation by h_w is an automorphism of $SL(2, \mathbb{C})$, thus one can form the semisimple direct product $SL(2, \mathbb{C}) \rtimes W_{\mathbb{K}}$, the multiplication rule being

$$(X_1, w_1)(X_2, w_2) = (X_1 h_{w_1} X_2 h_{w_1}^{-1}, w_1 w_2).$$

1: LEMMA The arrow

$$(X, w) \longrightarrow (Xh_w, w)$$

from

$$\mathrm{SL}(2, \mathbb{C}) \rtimes W_{\mathbb{K}} \quad \text{to} \quad \mathrm{SL}(2, \mathbb{C}) \times W_{\mathbb{K}}$$

is an isomorphism of groups.

2: DEFINITION A representation of $\mathrm{SL}(2, \mathbb{C}) \times W_{\mathbb{K}}$ is a continuous homomorphism $\rho : \mathrm{SL}(2, \mathbb{C}) \times W_{\mathbb{K}} \rightarrow \mathrm{GL}(V)$ (V a finite dimensional complex vector space) such that the restriction of ρ to $\mathrm{SL}(2, \mathbb{C})$ is complex analytic.

3: N.B. ρ is semisimple iff its restriction to $W_{\mathbb{K}}$ is semisimple.

[The restriction of ρ to $\mathrm{SL}(2, \mathbb{C})$ is necessarily semisimple.]

The finite dimensional irreducible representations of $\mathrm{SL}(2, \mathbb{C})$ are parameterized by the positive integers:

$$n \longleftrightarrow \mathrm{sym}(n), \quad \dim \mathrm{sym}(n) = n.$$

4: THEOREM The isomorphism classes of semisimple Deligne representations of $W_{\mathbb{K}}$ are in a 1-to-1 correspondence with the isomorphism classes of semisimple representations of $\mathrm{SL}(2, \mathbb{C}) \times W_{\mathbb{K}}$.

To explicate matters, start with a semisimple indecomposable Deligne representation of $W_{\mathbb{K}}$, say $\mathrm{sp}(n) \otimes \pi$, and assign to it the external tensor product $\mathrm{sym}(n) \boxtimes \pi$, hence in general

$$\bigoplus_{i=1}^s \mathrm{sp}(n_i) \otimes \pi_i \longrightarrow \bigoplus_{i=1}^s \mathrm{sym}(n_i) \boxtimes \pi_i.$$

APPENDIX A: TOPICS IN TOPOLOGY

NEIGHBORHOODS

COMPACTNESS

CONNECTEDNESS

TOPOLOGICAL GROUPS

NEIGHBORHOODS

1: DEFINITION If X is a topological space and if $x \in X$, then a neighborhood of x is a set U which contains an open set V containing x , the collection \mathcal{U}_x of all neighborhoods of x being the neighborhood system at x .

Therefore U is a neighborhood of x iff $x \in \text{int } U$.

2: PROPERTIES of \mathcal{U}_x

N-a If $U \in \mathcal{U}_x$, then $x \in U$.

N-b If $U_1, U_2 \in \mathcal{U}_x$, then $U_1 \cap U_2 \in \mathcal{U}_x$.

N-c If $U \in \mathcal{U}_x$, then there is a $U_0 \in \mathcal{U}_x$ such that $U \in \mathcal{U}_{x_0}$ for each $x_0 \in U_0$.

N-d If $U \in \mathcal{U}_x$ and $U \subset V$, then $V \in \mathcal{U}_x$.

3: FACT A subset $G \subset X$ is open iff G contains a neighborhood of each of its points.

4: SCHOLIUM If in a set X a nonempty collection \mathcal{U}_x of subsets of X is assigned to each $x \in X$ so as to satisfy N-a through N-d and if a subset $G \subset X$ is deemed “open” provided $\forall x \in G$, there is a $U \in \mathcal{U}_x$ such that $U \subset G$, then the result is a topology on X in which the neighborhood system at each $x \in X$ is \mathcal{U}_x .

5: DEFINITION If X is a topological space and if $x \in X$, then a neighborhood basis at x is a subcollection \mathcal{B}_x of \mathcal{U}_x such that $U \in \mathcal{U}_x$ contains some $V \in \mathcal{B}_x$.

6: EXAMPLE Take $X = \mathbb{R}^2$ with the usual topology –then the set of all squares with sides parallel to the axes and centered at x is a neighborhood basis at x .

7: PROPERTIES of \mathcal{B}_x

NB-a If $V \in \mathcal{B}_x$, then $x \in V$.

NB-b If $V_1, V_2 \in \mathcal{B}_x$, then there is a $V_3 \in \mathcal{B}_x$ such that $V_3 \subset V_1 \cap V_2$.

NB-c If $V \in \mathcal{B}_x$, then there is a $V_0 \in \mathcal{B}_x$ such that if $x_0 \in V_0$, then there is a $W \in \mathcal{B}_{x_0}$ such that $W \subset V$.

8: FACT A subset $G \subset X$ is open iff G contains a basic neighborhood of each of its points.

9: SCHOLIUM If in a set X a nonempty collection \mathcal{B}_x of subsets of X is assigned to each $x \in X$ so as to satisfy NB-a through NB-c and if a subset $G \subset X$ is deemed “open” provided $\forall x \in G$, there is a $V \in \mathcal{B}_x$ such that $V \subset G$, then the result is a topology on X in which a neighborhood basis at each $x \in X$ is \mathcal{B}_x .

[Put

$$\mathcal{U}_x = \{U \subset X : V \subset U \ (\exists V \in \mathcal{B}_x)\}.$$

Then \mathcal{U}_x satisfies N-a through N-d above.]

10: EXAMPLE Take $X = \mathbb{R}$ and given x , let \mathcal{B}_x be the $[x, y[$ ($y > x$) –then \mathcal{B}_x satisfies NB-a through NB-c above, from which a topology on the line, the underlying topological space being the Sorgenfrey line. .

11: DEFINITION Let X be a topological space –then a basis for X (i.e., for the underlying topology ...) is a collection \mathcal{B} of open sets such that for any open set $G \subset X$ and for any point $x \in G$, there is a set $B \in \mathcal{B}$ such that $x \in B \subset G$.

12: FACT If \mathcal{B} is a collection of open sets, then \mathcal{B} is a basis for X iff $\forall x \in X$, the collection

$$\mathcal{B}_x = \{B \in \mathcal{B} : x \in B\}$$

is a neighborhood basis at x .

13: FACT If X is a set and if \mathcal{B} is a collection of subsets of X , then \mathcal{B} is a basis for a topology on X iff

$$X = \bigcup_{B \in \mathcal{B}} B$$

and given $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \cap B_2$, there exists $B_3 \in \mathcal{B}$ such that $x \in B_3 \subset B_1 \cap B_2$.

COMPACTNESS

1: DEFINITION A topological space X is compact if every open cover of X has a finite subcover.

2: EXAMPLE The Cantor set is compact.

3: FACT The continuous image of a compact space is compact.

4: FACT A one-to-one continuous function from a compact space X onto a Hausdorff space Y is a homeomorphism.

5: DEFINITION A topological space X is locally compact if each point in X has a neighborhood basis consisting of compact sets.

6: FACT A Hausdorff space X is locally compact iff each point in X has a compact neighborhood.

7: APPLICATION Every compact Hausdorff space X is locally compact.

8: EXAMPLE The Cantor set is a locally compact Hausdorff space.

9: EXAMPLE \mathbb{R} is a locally compact Hausdorff space.

10: EXAMPLE \mathbb{Q} is a Hausdorff space but it is not locally compact (\mathbb{Q} is first category while a locally compact Hausdorff space is second category).

11: EXAMPLE The Sorgenfrey line is Hausdorff but not locally compact.

12: FACT Suppose that X_i ($i \in I$) is a nonempty topological 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.

CONNECTEDNESS

1: DEFINITION A topological space X is connected if it is not the union of two nonempty disjoint open sets.

2: EXAMPLE \mathbb{Q} is not connected (write

$$\mathbb{Q} = \{x : x > \sqrt{2}\} \cap \mathbb{Q} \cup \{x : x < \sqrt{2}\} \cap \mathbb{Q}.$$

3: EXAMPLE \mathbb{R} is connected and the only connected subsets of \mathbb{R} having more than one point are the intervals (open, closed, or half-open, half-closed).

4: FACT A topological space X is connected iff the only subsets of X that are both open and closed are \emptyset and X .

5: FACT The continuous image of a connected space is connected.

6: DEFINITION Let X be a topological space and let $x \in X$ —then the component $C(x)$ of x is the union of all connected subsets of X containing x .

7: FACT $C(x)$ is a closed subset of X .

8: FACT $C(x)$ is a maximal connected subset of X .

If $x \neq y$ in X , then either $C(x) = C(y)$ or $C(x) \cap C(y) = \emptyset$ (otherwise, $C(x) \cup C(y)$ would be a connected set containing x and y and larger than $C(x)$ or $C(y)$, which is impossible). Therefore the set of distinct components of X forms a partition of X .

9: EXAMPLE Take $X = \mathbb{Q}$ –then $\forall x \in \mathbb{Q}, C(x) = \{x\}$ (under the inclusion $\mathbb{Q} \rightarrow \mathbb{R}$, a connected subset of \mathbb{Q} is sent to a connected subset of \mathbb{R}).

10: DEFINITION A topological space X is totally disconnected if the components of X are singletons, i.e., $\forall x \in X, C(x) = \{x\}$.

11: FACT A topological space X is totally disconnected iff the only nonempty connected subsets of X are the one-point sets (hence X is T_1).

[Note: In every topological space X , the empty set and the one-point sets are connected and in a totally disconnected topological space, these are the only connected subsets.]

12: REMARK Let E be the equivalence relation defined by writing $x \sim y$ if x and y lie in the same component. Equip the set X/E with the identification topology determined by the projection $p : X \rightarrow X/E$ –then X/E is totally disconnected.

13: EXAMPLE The Cantor set is totally disconnected.

14: EXAMPLE \mathbb{Q} is totally disconnected.

15: EXAMPLE The Sorgenfrey line is totally disconnected.

16: FACT Every product of totally disconnected topological spaces is totally disconnected.

17: FACT Every subspace of a totally disconnected topological space is totally disconnected.

18: REMARK The continuous image of a totally disconnected space need not be totally disconnected. To appreciate the point, recall that every compact metric space is the continuous image of the Cantor set.

19: DEFINITION A topological space X is 0-dimensional if each point of X has a neighborhood basis consisting of open-closed sets.

20: FACT A 0-dimensional T_1 -space is totally disconnected.

21: EXAMPLE The Cantor set is 0-dimensional.

22: EXAMPLE \mathbb{Q} is 0-dimensional.

23: EXAMPLE The Sorgenfrey line is 0-dimensional.

24: REMARK As can be shown by example, a totally disconnected metric space need not be 0-dimensional.

25: FACT A locally compact Hausdorff space is 0-dimensional iff it is totally disconnected.

[Note: In such a space, each point has a neighborhood basis consisting of open-compact sets.]

A discrete space is 0-dimensional, hence is totally disconnected, hence a product of discrete spaces is totally disconnected, but an infinite product of nontrivial discrete spaces is never discrete.

26: DEFINITION The Cantor space is the countable product of the two-point discrete space.

27: FACT The Cantor set is homeomorphic to the Cantor space.

TOPOLOGICAL GROUPS

1: DEFINITION A locally compact (compact) group is a topological group G that is both locally compact (compact) and Hausdorff.

2: FACT If G is a locally compact group and if H is a closed subgroup, then G/H is a locally compact Hausdorff space.

3: FACT If G is a locally compact group and if H is a closed normal subgroup, then G/H is a locally compact group.

4: FACT If G is a locally compact group and if H is a locally compact subgroup, then H is closed in G .

5: FACT If G is a locally compact 0-dimensional group and if H is a closed subgroup of G , then G/H is 0-dimensional.

6: FACT If G is a totally disconnected locally compact group, then $\{e\}$ has a neighborhood basis consisting of open-compact subgroups.

7: FACT If G is a totally disconnected compact group, then $\{e\}$ has a neighborhood basis consisting of open-compact normal subgroups.

8: FACT If G is a locally compact group, then a subgroup H is open iff the quotient G/H is discrete.

9: FACT If G is a compact group, then a subgroup H is open iff the quotient G/H is finite.

10: FACT If G is a locally compact group, then every open subgroup of G is closed and every finite index closed subgroup of G is open.

APPENDIX B: TOPICS IN ALGEBRA

PRINCIPAL IDEAL DOMAINS

FIELD EXTENSIONS

ALGEBRAIC CLOSURE

TRACES AND NORMS

PRINCIPAL IDEAL DOMAINS

Let A be a commutative ring with unit.

1: DEFINITION An ideal I in A is an additive subgroup of A such that the relations $a \in A$, $x \in I$ imply that ax ($= xa$) belongs to I .

2: DEFINITION An ideal I in A is a prime ideal if $I \neq A$ and if $ab \in I$ implies that either $a \in I$ or $b \in I$.

3: DEFINITION An ideal I in A is a maximal ideal if $I \neq A$ and there is no larger proper ideal of A that contains I .

4: DEFINITION A is an integral domain if $ab = 0$ implies that $a = 0$ or $b = 0$.

5: N.B. Every field is an integral domain.

6: EXAMPLE \mathbb{Z} is an integral domain but $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime.

7: FACT An ideal $I \neq A$ in A is a prime ideal iff A/I is an integral domain.

8: FACT An ideal $I \neq A$ in A is a maximal ideal iff A/I is a field.

9: EXAMPLE Take $A = \mathbb{Z}[X]$ —then $\langle X \rangle$ is a prime ideal (since $A/\langle X \rangle \approx \mathbb{Z}$ is an integral domain) but $\langle X \rangle$ is not a maximal ideal (since $A/\langle X \rangle \approx \mathbb{Z}$ is not a field).

10: DEFINITION An ideal I in A is a principal ideal if $I = Aa_0$ ($\equiv \langle a_0 \rangle$) for some $a_0 \in A$.

11: DEFINITION A is a principal ideal domain if A is an integral domain and if every ideal in A is principal.

12: FACT For any field \mathbb{K} , the polynomial ring $\mathbb{K}[X]$ is a principal ideal domain.

[If I is a nonzero ideal in $\mathbb{K}[X]$, then I consists of all the multiples of the monic polynomial in I of least degree.]

13: EXAMPLE The polynomial ring $\mathbb{Z}[X]$ is not a principal ideal domain.

[The ideal I consisting of all polynomials with even constant term is not a principal ideal (but it is a maximal ideal).]

14: FACT If A is a principal ideal domain, then every nonzero prime ideal is maximal.

15: FACT For any field \mathbb{K} , the maximal ideals in $\mathbb{K}[X]$ are the nonzero prime ideals.

16: DEFINITION A unit in A is an element $u \in A$ with a multiplicative inverse, i.e., there is a $v \in A$ such that $uv = 1$.

17: EXAMPLE The units in $\mathbb{K}[X]$ are the nonzero constants.

18: EXAMPLE The units in \mathbb{Z} are 1 and -1 .

19: EXAMPLE The units in $\mathbb{Z}/n\mathbb{Z}$ are the congruence classes $[a]$ of a mod n such that $(a, n) = 1$.

20: DEFINITION The elements $a, b \in A$ are said to be associates if there is a unit $u \in A$ such that $a = ub$.

21: DEFINITION A nonzero element $p \in A$ is said to be irreducible if p is not a unit and in every factorization $p = ab$, either a or b is a unit.

22: EXAMPLE Take $A = \mathbb{Z}[X]$ —then $2X + 2 = 2(X + 1)$ is not irreducible, yet it does not factor into a product of polynomials of lower degree.

23: SCHOLIUM For any field \mathbb{K} , a nonzero polynomial $p(X) \in \mathbb{K}[X]$ of degree ≥ 1 is irreducible iff there is no factorization $p(X) = f(X)g(X)$ in $\mathbb{K}[X]$ with $\deg f < \deg p$ and $\deg g < \deg p$.

24: FACT If A is a principal ideal domain, then the nonzero prime ideals are the ideals $\langle p \rangle$, where p is irreducible.

25: FACT If A is a principal ideal domain and if $p \in A$ is irreducible, then $A/\langle p \rangle$ is a field.

[For $\langle p \rangle$ is prime, hence maximal.]

26: DEFINITION A is a unique factorization domain if A is an integral domain subject to:

E Every nonzero $a \in A$ that is not a unit is a product of irreducible elements.

U If

$$p_1 \cdots p_m = q_1 \cdots q_n,$$

where the p and q are irreducible, then $m = n$ and there is a one-to-one correspondence between the factors such that the corresponding factors are associates.

27: FACT Every principal ideal domain is a unique factorization domain.

28: APPLICATION For any field \mathbb{K} , the polynomial ring $\mathbb{K}[X]$ is a unique factorization domain

29: DEFINITION Suppose that A is a unique factorization domain –then a system of representatives of irreducible elements in A is a set of irreducible elements having exactly one element in common with the set of all associates of each irreducible element.

30: SCHOLIUM For any field \mathbb{K} , the monic irreducible polynomials constitute a system of representatives of irreducible elements in $\mathbb{K}[X]$.

[Note: Let f be a nonconstant polynomial in $\mathbb{K}[X]$ and let f_1, \dots, f_n be the distinct monic irreducible factors of f in $\mathbb{K}[X]$ –then

$$f = C \prod_{k=1}^n f_k^{e_k},$$

where C is the leading coefficient of f and e_1, \dots, e_n are positive integers. Moreover, this representation of f is unique up to a permutation of $\{1, \dots, n\}$.]

31: FACT For any field \mathbb{K} and for any irreducible polynomial $p(X)$, the quotient $\mathbb{L}' = \mathbb{K}[X]/\langle p(X) \rangle$ is a field containing an isomorphic copy \mathbb{K}' of \mathbb{K} as a subfield and a zero of $p'(X)$.

[Setting $I = \langle p(X) \rangle$, the map $a \rightarrow a + I$ ($a \in \mathbb{K}$) identifies \mathbb{K} with a subfield \mathbb{K}' of \mathbb{L}' . Write

$$p(X) = a_0 + a_1X + \cdots + a_nX^n.$$

Then in $\mathbb{K}'[X]$,

$$p'(X) = (a_0 + I) + (a_1 + I)X + \cdots + (a_n + I)X^n.$$

Now put $\theta = X + I$:

$$p'(\theta) = (a_0 + I) + (a_1X + I) + \cdots + (a_nX^n + I)$$

$$= a_0 + a_1X + \cdots + a_nX^n + I$$

$$= p(X) + I$$

$$= I,$$

the zero element of \mathbb{L}' .]

FIELD EXTENSIONS

Let \mathbb{K} be a field.

1: DEFINITION A field extension of \mathbb{K} is a field \mathbb{L} having \mathbb{K} as a subfield.

Given \mathbb{L}/\mathbb{K} and elements $x_1, \dots, x_n \in \mathbb{L}$, write $\mathbb{K}(x_1, \dots, x_n)$ for the subfield of \mathbb{L} generated by \mathbb{K} and the x_i ($i = 1, \dots, n$). In particular: $\mathbb{K}(x)$ is the subfield generated by \mathbb{K} and x .

2: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{R}$, $x = \sqrt{2}$ —then $\mathbb{Q}(\sqrt{2})$ consists of all real numbers of the form $r + s\sqrt{2}$ ($r, s \in \mathbb{Q}$).

[Let F be the set of all real numbers of the indicated form, thus

$$\mathbb{Q} \cup \{\sqrt{2}\} \subset F \subset \mathbb{Q}(\sqrt{2}),$$

and, by definition, $\mathbb{Q}(\sqrt{2})$ is the subfield of \mathbb{R} generated by $\mathbb{Q} \cup \{\sqrt{2}\}$. Let now $x = r + s\sqrt{2}$ ($r, s \in \mathbb{Q}$): $r^2 - 2s^2 \neq 0$ ($\sqrt{2}$ irrational)

\implies

$$\begin{aligned} \frac{1}{x} &= \frac{r}{r^2 - 2s^2} + \frac{-s}{r^2 - 2s^2} \sqrt{2} \\ &\in F, \end{aligned}$$

so F is a field, so $F = \mathbb{Q}(\sqrt{2})$.]

3: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{R}$, $x = \sqrt{2}$, $y = \sqrt{3}$ —then

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

[Obviously, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ hence $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In the other

direction

$$(\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3}) = -1$$

\Rightarrow

$$\sqrt{3} - \sqrt{2} = \frac{1}{\sqrt{2} + \sqrt{3}} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

\Rightarrow

$$\begin{cases} \sqrt{3} = ((\sqrt{3} + \sqrt{2}) + (\sqrt{3} - \sqrt{2}))/2 \\ \sqrt{2} = ((\sqrt{3} + \sqrt{2}) - (\sqrt{3} - \sqrt{2}))/2 \end{cases} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}).$

Given $\mathbb{L} \supset \mathbb{K}$, view \mathbb{L} as a vector space over \mathbb{K} and write $[\mathbb{L} : \mathbb{K}]$ for its dimension, the degree of \mathbb{L} over \mathbb{K} .

[Note: In this context, the term “dimension” refers to the cardinal number of a basis for \mathbb{L} over \mathbb{K} .]

4: FACT Let $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ be fields –then

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}].$$

5: EXAMPLE Take $\mathbb{F} = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ –then

$$\begin{aligned} [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= 2 \cdot 2 \\ &= 4. \end{aligned}$$

6: DEFINITION \mathbb{L} is a finite extension of \mathbb{K} if $[\mathbb{L} : \mathbb{K}]$ is finite and \mathbb{L} is an infinite extension of \mathbb{K} if $[\mathbb{L} : \mathbb{K}]$ is infinite.

7: EXAMPLE $[\mathbb{C} : \mathbb{R}] = 2$ but $[\mathbb{C} : \mathbb{Q}] = 2^{\aleph_0}$.

Given \mathbb{L}/\mathbb{K} and $x \in \mathbb{L}$, the ideal I_x of algebraic relations of x is the ideal in $\mathbb{K}[X]$ consisting of all polynomials admitting x as a zero.

8: DEFINITION x is algebraic over \mathbb{K} (transcendental over \mathbb{K}) according to whether I_x is nonzero (zero). I.e.: x is algebraic over \mathbb{K} (transcendental over \mathbb{K}) according to whether it is (or is not) a zero of a nonzero polynomial in $\mathbb{K}[X]$.

9: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{C}$ —then $\sqrt{-1}$ is algebraic over \mathbb{Q} but e and π are transcendental over \mathbb{Q} .

10: FACT Let $x \in \mathbb{L}$ —then x is algebraic over \mathbb{K} iff I_x is a nonzero prime ideal in $\mathbb{K}[X]$ or still, is a maximal ideal in $\mathbb{K}[X]$.

11: FACT If $x \in \mathbb{L}$ is algebraic over \mathbb{K} , then I_x has a unique monic polynomial p_x in $\mathbb{K}[X]$ as a generator: $I_x = \langle p_x \rangle$, the minimal polynomial of x over \mathbb{K} .

[Note: One can characterize p_x as the monic polynomial in $\mathbb{K}[X]$ that admits x as a zero and divides in $\mathbb{K}[X]$ every polynomial admitting x as a zero.]

12: REMARK The minimal polynomial of an element depends on the base field. E.g.: If $\mathbb{K} = \mathbb{Q}$ and $\mathbb{L} = \mathbb{C}$, then $p_{\sqrt{-1}}(X) = X^2 + 1$ but if $\mathbb{K} = \mathbb{L} = \mathbb{C}$, then $p_{\sqrt{-1}}(X) = X - \sqrt{-1}$.

13: FACT If $x \in \mathbb{L}$ is algebraic over \mathbb{K} , then its minimal polynomial p_x is irreducible.

14: FACT If $x \in \mathbb{L}$ is algebraic over \mathbb{K} and if $n = \deg p_x$, then p_x is the only monic polynomial in $\mathbb{K}[X]$ of degree n admitting x as a zero.

15: FACT If $x \in \mathbb{L}$ is algebraic over \mathbb{K} , then the set $\{x^j : 0 \leq j \leq n-1\}$ is a linear basis of $\mathbb{K}(x)$ over \mathbb{K} , hence $[\mathbb{K}(x) : \mathbb{K}] = n$.

16: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{R}$, $x = (2)^{1/3}$ —then $\mathbb{Q}((2)^{1/3})$ is a subfield of \mathbb{R} and $(2)^{1/3}$ is algebraic over \mathbb{Q} , its minimal polynomial being $X^3 - 2$, so $[\mathbb{Q}((2)^{1/3}) : \mathbb{Q}] = 3$.

17: DEFINITION \mathbb{L} is an algebraic extension of \mathbb{K} if every element of \mathbb{L} is algebraic over \mathbb{K} .

18: FACT If $[\mathbb{L} : \mathbb{K}] < \infty$, then \mathbb{L} is an algebraic extension of \mathbb{K} .

[If $n = [\mathbb{L} : \mathbb{K}]$ and if $x \in \mathbb{L}$, then the sequence x^j ($0 \leq j \leq n$) is linearly dependent over \mathbb{K} , so there exists a sequence a_j ($0 \leq j \leq n$) of elements of \mathbb{K} (not all zero) such that $\sum_{j=0}^n a_j x^j = 0$.]

19: FACT Suppose that \mathbb{K} is infinite and \mathbb{L} is an algebraic extension of \mathbb{K} —then

$$\text{card } \mathbb{K} = \text{card } \mathbb{L}.$$

20: EXAMPLE \mathbb{R} is not an algebraic extension of \mathbb{Q} .

21: DEFINITION Let \mathbb{K} be a field and let $\mathbb{L}_1, \mathbb{L}_2$ be field extensions of \mathbb{K} —then a \mathbb{K} -homomorphism $\phi : \mathbb{L}_1 \rightarrow \mathbb{L}_2$ is a ring homomorphism such that $\phi|_{\mathbb{K}} = \text{id}_{\mathbb{K}}$, ϕ being called a \mathbb{K} -isomorphism if it is in addition bijective (injectivity is automatic).

[Note: When $\mathbb{L}_1 = \mathbb{L}_2$, the term is \mathbb{K} -automorphism.]

22: REMARK If $\mathbb{L}_1 = \mathbb{L}_2$, call it \mathbb{L} , and if \mathbb{L} is an algebraic extension of \mathbb{K} , then every \mathbb{K} -homomorphism $\phi : \mathbb{L} \rightarrow \mathbb{L}$ is a \mathbb{K} -isomorphism.

23: FACT Let \mathbb{K} be a field and let $\mathbb{L}_1, \mathbb{L}_2$ be field extensions of \mathbb{K} . Suppose that f is an irreducible polynomial in $\mathbb{K}[X]$ and suppose that x_1, x_2 are, respectively, zeros of f in $\mathbb{L}_1, \mathbb{L}_2$ —then there is a unique \mathbb{K} -isomorphism $\mathbb{K}(x_1) \rightarrow \mathbb{K}(x_2)$ such that $x_1 \rightarrow x_2$.

[Note: The assumption that f is irreducible cannot be dropped.]

ADDENDUM

Let \mathbb{K} be a field, \mathbb{L}/\mathbb{K} a field extension —then a subset S of \mathbb{L} is a transcendence basis for \mathbb{L}/\mathbb{K} if S is algebraically independent over \mathbb{K} and if \mathbb{L} is algebraic over $\mathbb{K}(S)$ (the subfield of \mathbb{L} generated by $\mathbb{K} \cup S$).

1: FACT A transcendence basis for \mathbb{L}/\mathbb{K} always exists and any two have the same cardinality.

2: DEFINITION The transcendence degree $\text{trdeg}(\mathbb{L}/\mathbb{K})$ is the cardinality of any transcendence basis of \mathbb{L}/\mathbb{K} .

3: EXAMPLE Take $\mathbb{K} = \mathbb{Q}, \mathbb{L} = \mathbb{C}$ —then $\text{trdeg}(\mathbb{C}/\mathbb{Q})$ is infinite (in fact uncountable).

4: EXAMPLE Take $\mathbb{K} = \mathbb{Q}, \mathbb{L} = \mathbb{Q}_p$ —then $\text{trdeg}(\mathbb{Q}_p/\mathbb{Q})$ is infinite (in fact uncountable).

ALGEBRAIC CLOSURE

Let \mathbb{K} be a field, \mathbb{L}/\mathbb{K} a field extension.

1: NOTATION $A(\mathbb{L}/\mathbb{K})$ is the set of all elements of \mathbb{L} that are algebraic over \mathbb{K} .

2: DEFINITION $A(\mathbb{L}/\mathbb{K})$ is the algebraic closure of \mathbb{K} in \mathbb{L} .

3: EXAMPLE Take $\mathbb{K} = \mathbb{R}$, $\mathbb{L} = \mathbb{C}$ —then $A(\mathbb{L}/\mathbb{K}) = \mathbb{C}$.

[Given $a + \sqrt{-1}b$, consider the polynomial

$$(X - (a + \sqrt{-1}b))(X - (a - \sqrt{-1}b)) = X^2 - 2aX + a^2 + b^2.]$$

4: FACT \mathbb{L} is an algebraic extension of \mathbb{K} iff $A(\mathbb{L}/\mathbb{K}) = \mathbb{L}$.

5: DEFINITION \mathbb{K} is algebraically closed in \mathbb{L} if every element of \mathbb{L} that is algebraic over \mathbb{K} belongs to \mathbb{K} :

$$A(\mathbb{L}/\mathbb{K}) = \mathbb{K}.$$

6: FACT

$$\mathbb{K} \subset A(\mathbb{L}/\mathbb{K}) \subset \mathbb{L}.$$

7: FACT $A(\mathbb{L}/\mathbb{K})$ is a field.

8: FACT $A(\mathbb{L}/\mathbb{K})$ is algebraically closed in \mathbb{L} .

[Spelled out, if $x \in \mathbb{L}$ is algebraic over $A(\mathbb{L}/\mathbb{K})$, then $x \in A(\mathbb{L}/\mathbb{K})$.]

9: SCHOLIUM If $\mathbb{K} \subset \mathbb{E} \subset \mathbb{L}$ and if \mathbb{E} is an algebraic extension of \mathbb{K} , then

$$\mathbb{E} \subset A(\mathbb{L}/\mathbb{K}).$$

10: DEFINITION Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{C}$ —then an algebraic number is a complex number which is algebraic over \mathbb{Q} , i.e., is an element of $A(\mathbb{C}/\mathbb{Q})$.

11: FACT $\text{card } A(\mathbb{C}/\mathbb{Q}) = \aleph_0$.

12: FACT $[A(\mathbb{C}/\mathbb{Q}) : \mathbb{Q}] = \aleph_0$.

[Let n be a positive integer —then the polynomial $X^n - 2$ is irreducible in $\mathbb{Q}[X]$, thus is the minimal polynomial of $(2)^{1/2}$ over \mathbb{Q} , so $[Q((2)^{1/2}) : \mathbb{Q}] = n$, from which

$$[A(\mathbb{C}/\mathbb{Q}) : \mathbb{Q}] \geq n.$$

And this implies that

$$[A(\mathbb{C}/\mathbb{Q}) : \mathbb{Q}] \geq \aleph_0.$$

On the other hand,

$$[A(\mathbb{C}/\mathbb{Q}) : \mathbb{Q}] \leq \text{card } A(\mathbb{C}/\mathbb{Q}) = \aleph_0.]$$

13: DEFINITION A field \mathbb{F} is algebraically closed if every nonconstant polynomial in $\mathbb{F}[X]$ has a zero in \mathbb{F} .

[Note: This notion is absolute.]

14: EXAMPLE Neither \mathbb{Q} nor \mathbb{R} is algebraically closed but \mathbb{C} is algebraically closed.

15: FACT \mathbb{F} is algebraically closed iff every irreducible polynomial has degree 1.

16: FACT \mathbb{F} is algebraically closed iff every nonconstant polynomial f in $\mathbb{F}[X]$ splits in $\mathbb{F}[X]$.

[Note: I.e.: Given f , there exists a positive integer n and elements a, a_1, \dots, a_n (not necessarily distinct) of \mathbb{F} such that

$$f(X) = a \prod_{k=1}^n (X - a_k).]$$

17: FACT If \mathbb{F} is algebraically closed, then it is its only algebraic extension.

18: FACT If there is an algebraically closed field extension \mathbb{F}' of \mathbb{F} in which \mathbb{F} is algebraically closed, then \mathbb{F} is algebraically closed.

[Let $f \in \mathbb{F}[X]$ be a nonconstant polynomial —then f has a zero a' in \mathbb{F}' , hence a' is algebraic over \mathbb{F} , hence $a' \in \mathbb{F}$ (since \mathbb{F} is algebraically closed in \mathbb{F}').]

19: APPLICATION Suppose that \mathbb{L}/\mathbb{K} is an algebraically closed field extension. Let $\mathbb{F} = A(\mathbb{L}/\mathbb{K})$, $\mathbb{F}' = \mathbb{L}$ to conclude that $A(\mathbb{L}/\mathbb{K})$ is algebraically closed.

20: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{C}$ —then \mathbb{C} is algebraically closed, hence $A(\mathbb{C}/\mathbb{Q})$ is algebraically closed.

21: FACT Let \mathbb{K} be a field, let \mathbb{L} be an algebraic closure of \mathbb{K} , and let \mathbb{M} be an algebraically closed extension of \mathbb{K} —then there exists a \mathbb{K} -monomorphism $\phi : \mathbb{L} \rightarrow \mathbb{M}$.

22: EXAMPLE Take $\mathbb{K} = \mathbb{R}$, $\mathbb{L} = \mathbb{C}$, $\mathbb{M} = \mathbb{C}$ —then the inclusion $\mathbb{R} \rightarrow \mathbb{C}$ admits two distinct extensions to \mathbb{C} , viz. the identity and the complex conjugation (and these are the only \mathbb{R} -automorphisms of \mathbb{C}).

[Note: Therefore uniqueness of the extending \mathbb{K} -monomorphism cannot be asserted.]

23: EXAMPLE If $\mathbb{E} \neq \mathbb{R}$ is an algebraic extension of \mathbb{R} , then \mathbb{E} is isomorphic to \mathbb{C} .

[Take $\mathbb{K} = \mathbb{R}$, $\mathbb{L} = \mathbb{E}$, $\mathbb{M} = \mathbb{C}$ —then there exists an \mathbb{R} -monomorphism $\phi : \mathbb{E} \rightarrow \mathbb{C}$, hence

$$2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \phi(\mathbb{E})] \cdot [\phi(\mathbb{E}) : \mathbb{R}],$$

from which $\mathbb{C} = \phi(\mathbb{E}) \approx \mathbb{E}$.]

24: DEFINITION Given a field \mathbb{F} , an algebraic closure of \mathbb{F} is an algebraically closed algebraic extension of \mathbb{F} .

25: EXAMPLE \mathbb{C} is an algebraic closure of \mathbb{R} but \mathbb{C} is not an algebraic closure of \mathbb{Q} (since it is not algebraic over \mathbb{Q}).

26: EXAMPLE $A(\mathbb{C}/\mathbb{Q})$ is an algebraic closure of \mathbb{Q} .

27: STEINITZ THEOREM Every field \mathbb{F} admits an algebraic closure \mathbb{F}^{cl} and any two algebraic closures of \mathbb{F} are \mathbb{F} -isomorphic.

28: FACT Every automorphism of \mathbb{F} can be extended to an automorphism of \mathbb{F}^{cl} .

[Note: In general, if \mathbb{F}_1 and \mathbb{F}_2 are fields, then every isomorphism from \mathbb{F}_1 to \mathbb{F}_2 can be extended to an isomorphism from \mathbb{F}_1^{cl} to \mathbb{F}_2^{cl} .]

29: FACT If \mathbb{L}/\mathbb{K} is an algebraic extension of \mathbb{K} , then \mathbb{L} is \mathbb{K} -isomorphic to a subfield of \mathbb{K}^{cl} .

TRACES AND NORMS

Let \mathbb{K} be a field, \mathbb{L}/\mathbb{K} a field extension of \mathbb{K} –then each $x \in \mathbb{L}$ gives rise to a linear transformation

$$M_x : \mathbb{L} \rightarrow \mathbb{L}$$

defined by

$$M_x(y) = xy.$$

1: DEFINITION The trace of \mathbb{L} over \mathbb{K} is the function

$$\begin{cases} T_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \rightarrow \mathbb{K} \\ T_{\mathbb{L}/\mathbb{K}}(x) = \text{tr}(M_x). \end{cases}$$

2: DEFINITION The norm of \mathbb{L} over \mathbb{K} is the function

$$\begin{cases} N_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \rightarrow \mathbb{K} \\ N_{\mathbb{L}/\mathbb{K}}(x) = \det(M_x). \end{cases}$$

3: PROPERTIES $\forall x, y \in \mathbb{L}, \forall a \in \mathbb{K}$:

1. $T_{\mathbb{L}/\mathbb{K}}(x + y) = T_{\mathbb{L}/\mathbb{K}}(x) + T_{\mathbb{L}/\mathbb{K}}(y).$
2. $T_{\mathbb{L}/\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}]a.$
3. $N_{\mathbb{L}/\mathbb{K}}(xy) = N_{\mathbb{L}/\mathbb{K}}(x)N_{\mathbb{L}/\mathbb{K}}(y).$
4. $N_{\mathbb{L}/\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}.$

4: FACT If \mathbb{E} is a subfield of \mathbb{L} containing \mathbb{K} , then

$$\begin{cases} T_{\mathbb{L}/\mathbb{K}}(x) = T_{\mathbb{E}/\mathbb{K}}(T_{\mathbb{L}/\mathbb{E}}(x)) \\ N_{\mathbb{L}/\mathbb{K}}(x) = N_{\mathbb{E}/\mathbb{K}}(N_{\mathbb{L}/\mathbb{E}}(x)) \end{cases}.$$

5: EXAMPLE Let $\theta \in \mathbb{K}^\times - (\mathbb{K}^\times)^2$ and put $\mathbb{L} = \mathbb{K}(\sqrt{\theta})$ –then $\forall a, b \in \mathbb{K}$,

$$\begin{cases} \mathrm{T}_{\mathbb{L}/\mathbb{K}}(a + b\sqrt{\theta}) = 2a \\ \mathrm{N}_{\mathbb{L}/\mathbb{K}}(a + b\sqrt{\theta}) = a^2 - b^2\theta \end{cases} \quad .$$

TOPICS IN GALOIS THEORY

GALOIS CORRESPONDENCES

FINITE GALOIS THEORY

INFINITE GALOIS THEORY

\mathbb{K}^{sep} AND \mathbb{K}^{ab}

APPENDIX C-1

GALOIS CORRESPONDENCES

Given a field \mathbb{F} , $\text{Aut}(\mathbb{F})$ stands for its associated group of field automorphisms.

1: EXAMPLE Take $\mathbb{F} = \mathbb{Q}$ –then $\text{Aut}(\mathbb{Q})$ is trivial.

2: EXAMPLE Take $\mathbb{F} = \mathbb{R}$ –then $\text{Aut}(\mathbb{R})$ is trivial.

[Let $\phi \in \text{Aut}(\mathbb{R})$ –then $\phi|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$. Next:

$$\begin{aligned} x < y &\implies \phi(y) - \phi(x) = \phi(y - x) \\ &= \phi((\sqrt{y - x})^2) \\ &= \phi(\sqrt{y - x})^2 \\ &> 0. \end{aligned}$$

If now $\phi \neq \text{id}_{\mathbb{R}}$, choose x such that $\phi(x) \neq x$ –then there are two possibilities.

- $x < \phi(x)$: Choose $q \in \mathbb{Q}$: $x < q < \phi(x)$, so $\phi(x) < \phi(q) = q < \phi(x)$.

Contradiction.

- $\phi(x) < x$: Choose $q \in \mathbb{Q}$: $\phi(x) < q < x$, so $\phi(x) < q = \phi(q) < \phi(x)$.

Contradiction.

3: EXAMPLE Take $\mathbb{F} = \mathbb{C}$ –then $\text{Aut}(\mathbb{C})$ is infinite.

[Any automorphism $\phi : \mathbb{C} \rightarrow \mathbb{C}$ will fix \mathbb{Q} and any continuous automorphism $\phi : \mathbb{C} \rightarrow \mathbb{C}$ will fix its closure \mathbb{R} , there being two such, viz. the identity and the complex conjugation, all others being discontinuous.]

[Note: As an illustration, consider the automorphism

$$a + b\sqrt{2} \rightarrow a - b\sqrt{2} \quad (a, b \in \mathbb{Q})$$

of the field $\mathbb{Q}(\sqrt{2})$ –then it can be extended to an automorphism of \mathbb{C} via the following procedure.

1. Extend to $\mathbb{K} \equiv \mathbb{Q}(\sqrt{2})^{\mathbb{C}^\ell} \subset \mathbb{C}$.
2. Choose a transcendence basis S for \mathbb{C}/\mathbb{K} and extend to $\mathbb{K}(S)$.
3. Extend from $\mathbb{K}(S)$ to \mathbb{C} .]

4: DEFINITION Let G be a group of automorphisms of \mathbb{F} –then the subfield

$$\text{Inv}(G) = \{x : \sigma x = x\} \quad (\sigma \in G)$$

is called the invariant field associated with G .

5: DEFINITION Given a subfield $\mathbb{E} \subset \mathbb{F}$, the group consisting of all automorphisms of \mathbb{F} leaving every element of \mathbb{E} invariant is denoted by $\text{Gal}(\mathbb{F}/\mathbb{E})$, the Galois group of \mathbb{F} over \mathbb{E} .

6: EXAMPLE Take $\mathbb{E} = \mathbb{R}$, $\mathbb{F} = \mathbb{C}$ –then $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}_{\mathbb{C}}, \sigma\}$, where σ is the complex conjugation.

7: EXAMPLE Take $\mathbb{E} = \mathbb{Q}$, $\mathbb{F} = \mathbb{Q}((2)^{1/3})$ –then $\text{Gal}(\mathbb{Q}((2)^{1/3})/\mathbb{Q})$ is trivial.

8: EXAMPLE Take $\mathbb{E} = \mathbb{Q}$, $\mathbb{F} = \mathbb{Q}(\omega_n)$ (ω_n a primitive n^{th} root of unity in \mathbb{C}) –then

$$\text{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^\times.$$

9: FACT We have

$$G \subset \text{Gal}(\mathbb{F}/\text{Inv}(G)).$$

10: FACT We have

$$\mathbb{E} \subset \text{Inv}(\text{Gal}(\mathbb{F}/\mathbb{E})).$$

11: FACT

$$G \subset \text{Gal}(\mathbb{F}/\mathbb{E}) \Leftrightarrow \mathbb{E} \subset \text{Inv}(G).$$

12: FACT

- $G_1 \subset G_2 \subset \text{Aut}(\mathbb{F}) \implies \text{Inv}(G_1) \supset \text{Inv}(G_2).$
- $\mathbb{E}_1 \subset \mathbb{E}_2 \subset \mathbb{F} \implies \text{Gal}(\mathbb{F}/\mathbb{E}_2) \subset \text{Gal}(\mathbb{F}/\mathbb{E}_1).$

13: DEFINITION Let \mathbb{F} be a field.

- A Galois group on \mathbb{F} is a group G of automorphisms of \mathbb{F} such that

$$G = \text{Gal}(\mathbb{F}/\text{Inv}(G)).$$

- An invariant field in \mathbb{F} is a subfield \mathbb{E} of \mathbb{F} such that

$$\mathbb{E} = \text{Inv}(\text{Gal}(\mathbb{F}/\mathbb{E})).$$

14: EXAMPLE $\text{Aut}(\mathbb{F})$ is a Galois group on \mathbb{F} .

[For

$$\begin{aligned} \text{Aut}(\mathbb{F}) &\subset \text{Gal}(\mathbb{F}/\text{Inv}(\text{Aut}(\mathbb{F}))) \\ &= \text{Aut}(\mathbb{F}).] \end{aligned}$$

15: EXAMPLE $\{\text{id}_{\mathbb{F}}\}$ is a Galois group on \mathbb{F}

[For

$$\begin{aligned} \{\text{id}_{\mathbb{F}}\} &\subset \text{Gal}(\mathbb{F}/\text{Inv}(\{\text{id}_{\mathbb{F}}\})) \\ &= \text{Gal}(\mathbb{F}/\mathbb{F}) \\ &= \{\text{id}_{\mathbb{F}}\}.] \end{aligned}$$

16: EXAMPLE \mathbb{F} is an invariant field on \mathbb{F} .

17: REMARK Recall that a field is prime if it possesses no proper subfields, these being the fields isomorphic to \mathbb{Q} (characteristic 0) or isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (characteristic p). A prime field admits no automorphism other than the identity.

18: ABSOLUTE GALOIS CORRESPONDENCE Let \mathbb{F} be a field.

- If \mathbb{E} is a subfield of \mathbb{F} , then $\text{Gal}(\mathbb{F}/\mathbb{E})$ is a Galois group on \mathbb{F} .
- If G is a group of automorphisms of \mathbb{F} , then $\text{Inv}(G)$ is an invariant field in \mathbb{F} .

And: The arrow $\mathbb{E} \rightarrow \text{Gal}(\mathbb{F}/\mathbb{E})$ from the set of all invariant fields in \mathbb{F} to the set of all Galois groups on \mathbb{F} and the arrow $G \rightarrow \text{Inv}(G)$ from the set of all Galois groups on \mathbb{F} to the set of all invariant fields in \mathbb{F} are mutually inverse inclusion reversing bijections.

19: RELATIVE GALOIS CORRESPONDENCE Let \mathbb{K} be a field and let \mathbb{L} be a field extension of \mathbb{K} .

- If $\mathbb{K} \subset \mathbb{E} \subset \mathbb{L}$, then $\text{Gal}(\mathbb{L}/\mathbb{E})$ is a Galois group on \mathbb{L} contained in $\text{Gal}(\mathbb{L}/\mathbb{K})$.
- If G is a subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$, then $\text{Inv}(G)$ is an invariant field in \mathbb{L} containing \mathbb{K} .

And: The arrow $\mathbb{E} \rightarrow \text{Gal}(\mathbb{L}/\mathbb{E})$ from the set of all invariant fields in \mathbb{L} containing \mathbb{K} to the set of all Galois groups on \mathbb{L} contained in $\text{Gal}(\mathbb{L}/\mathbb{K})$ and the arrow $G \rightarrow \text{Inv}(G)$ from the set of all Galois groups on \mathbb{L} contained in $\text{Gal}(\mathbb{L}/\mathbb{K})$ to the set of all invariant fields in \mathbb{L} containing \mathbb{K} are mutually inverse inclusion reversing bijections.

FINITE GALOIS THEORY

1: DEFINITION A field extension \mathbb{L}/\mathbb{K} is Galois over \mathbb{K} (or is a Galois extension of \mathbb{K}) if \mathbb{L} is algebraic over \mathbb{K} and \mathbb{K} is an invariant field on \mathbb{L} or still,

$$\mathbb{K} = \text{Inv}(\text{Gal}(\mathbb{L}/\mathbb{K})).$$

2: FACT If \mathbb{L}/\mathbb{K} is a finite Galois extension and if $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$ is an intermediate field, then \mathbb{L} is Galois over \mathbb{E} .

3: FACT If \mathbb{L}/\mathbb{K} is a finite Galois extension and if $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$ is an intermediate field, then \mathbb{E} is Galois over \mathbb{K} iff $\text{Gal}(\mathbb{L}/\mathbb{E})$ is a normal subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$.

[Note: Under the assumption that \mathbb{E} is Galois over \mathbb{K} , there is an arrow of restriction

$$\text{Gal}(\mathbb{L}/\mathbb{K}) \rightarrow \text{Gal}(\mathbb{E}/\mathbb{K}).$$

It is surjective with kernel $\text{Gal}(\mathbb{L}/\mathbb{E})$, from which an exact sequence of groups:

$$1 \rightarrow \text{Gal}(\mathbb{L}/\mathbb{E}) \rightarrow \text{Gal}(\mathbb{L}/\mathbb{K}) \rightarrow \text{Gal}(\mathbb{E}/\mathbb{K}) \rightarrow 1.]$$

4: RECOGNITION PRINCIPLE If \mathbb{L}/\mathbb{K} is a finite extension, then \mathbb{L} is Galois over \mathbb{K} iff

$$\text{card Gal}(\mathbb{L}/\mathbb{K}) = [\mathbb{L} : \mathbb{K}].$$

[Note: If \mathbb{L}/\mathbb{K} is a finite extension, then a priori

$$\text{card Gal}(\mathbb{L}/\mathbb{K}) \leq [\mathbb{L} : \mathbb{K}],$$

the inequality being strict in general. Matters break down if it is a question of infinite

extensions. E.g.: If $\mathbb{Q}^{c\ell}$ is an algebraic closure of \mathbb{Q} , then

$$[\mathbb{Q}^{c\ell} : \mathbb{Q}] = \aleph_0$$

while

$$\text{card Gal}(\mathbb{Q}^{c\ell}/\mathbb{Q}) = 2^{\aleph_0}.$$

5: EXAMPLE Let \mathbb{F} be a field of characteristic 0 and let $a \in \mathbb{F}^\times - (\mathbb{F}^\times)^2$.

Form the quadratic extension $\mathbb{F}(\sqrt{a})$ –then $[\mathbb{F}(\sqrt{a}) : \mathbb{F}] = 2$, while $\text{Gal}(\mathbb{F}(\sqrt{a})/\mathbb{F}) = \{\text{id}, \sigma\}$ ($\sigma(\sqrt{a}) = -\sqrt{a}$). Therefore $\mathbb{F}(\sqrt{a})$ is a Galois extension of \mathbb{F} .

6: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}((2)^{1/3})$ –then $[\mathbb{Q}((2)^{1/3}) : \mathbb{Q}] = 3$ but $\text{Gal}(\mathbb{Q}((2)^{1/3})/\mathbb{Q})$ is trivial. Therefore $\mathbb{Q}((2)^{1/3})$ is not a Galois extension of \mathbb{Q} .

7: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}((2)^{1/3}, \omega)$, where

$$\omega = \exp(2\pi\sqrt{-1}/3).$$

Then

$$[\mathbb{Q}((2)^{1/3}, \omega) : \mathbb{Q}] = [\mathbb{Q}((2)^{1/3}, \omega) : \mathbb{Q}((2)^{1/3})] \cdot [\mathbb{Q}((2)^{1/3}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

On the other hand, the six functions

$$(2)^{1/3} \rightarrow (2)^{1/3}, \quad \omega \rightarrow \omega$$

$$(2)^{1/3} \rightarrow \omega(2)^{1/3}, \quad \omega \rightarrow \omega$$

$$(2)^{1/3} \rightarrow (2)^{1/3}, \quad \omega \rightarrow \omega^2$$

$$(2)^{1/3} \rightarrow \omega(2)^{1/3}, \quad \omega \rightarrow \omega^2$$

$$(2)^{1/3} \rightarrow \omega^2(2)^{1/3}, \quad \omega \rightarrow \omega$$

$$(2)^{1/3} \rightarrow \omega^2(2)^{1/3}, \quad \omega \rightarrow \omega^2$$

extend to distinct automorphisms of $\mathbb{Q}((2)^{1/3}, \omega)/\mathbb{Q}$. Therefore $\mathbb{Q}((2)^{1/3}, \omega)$ is a Galois extension of \mathbb{Q} .

8: FUNDAMENTAL THEOREM OF FINITE GALOIS THEORY Suppose that \mathbb{L} is a finite Galois extension of \mathbb{K} .

- If $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$, then

$$[\text{Gal}(\mathbb{L}/\mathbb{K}) : \text{Gal}(\mathbb{L}/\mathbb{E})] = [\mathbb{E} : \mathbb{K}].$$

- If $G \subset \text{Gal}(\mathbb{L}/\mathbb{K})$, then

$$[\text{Inv}(G) : \mathbb{K}] = [\text{Gal}(\mathbb{L}/\mathbb{K}) : G].$$

And: The arrow $\mathbb{E} \rightarrow \text{Gal}(\mathbb{L}/\mathbb{E})$ from the set of all intermediate fields between \mathbb{K} and \mathbb{L} to the set of all subgroups of $\text{Gal}(\mathbb{L}/\mathbb{K})$ and the arrow $G \rightarrow \text{Inv}(G)$ from the set of all subgroups of $\text{Gal}(\mathbb{L}/\mathbb{K})$ to the set of all intermediate fields between \mathbb{K} and \mathbb{L} are mutually inverse inclusion reversing bijections.

9: REMARK Given a finite Galois extension \mathbb{L}/\mathbb{K} , the problem of determining all intermediate fields $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$ amounts to finding all subgroups of $\text{Gal}(\mathbb{L}/\mathbb{K})$, a finite problem.

[Note: The fact that there are but finitely many intermediate fields cannot be established by a vector space argument alone.]

10: EXAMPLE The field $\mathbb{Q}((2)^{1/3}, \omega)$ is Galois over \mathbb{Q} and its Galois group is a group of order 6, there being two possibilities, viz. the cyclic group $\mathbb{Z}/6\mathbb{Z}$ and the symmetric group S_3 . Since $\mathbb{Q}((2)^{1/3})$ is not Galois over \mathbb{Q} , the group

$$\text{Gal}(\mathbb{Q}((2)^{1/3}, \omega)/\mathbb{Q}((2)^{1/3}))$$

is not a normal subgroup of $\text{Gal}(\mathbb{Q}((2)^{1/3}, \omega)/\mathbb{Q})$. But every subgroup of an abelian group is normal, so the conclusion is that

$$G \equiv \text{Gal}(\mathbb{Q}((2)^{1/3}, \omega)/\mathbb{Q}) \approx S_3.$$

Proceeding, there are \mathbb{Q} -automorphisms σ, τ of $\mathbb{Q}((2)^{1/3}, \omega)$ defined by the specification

$$\begin{cases} \sigma : (2)^{1/3} \rightarrow \omega(2)^{1/3}, & \omega \rightarrow \omega \\ \tau : (2)^{1/3} \rightarrow (2)^{1/3}, & \omega \rightarrow \omega^2 \end{cases}.$$

Then σ has order 3, τ has order 2, and $\sigma\tau \neq \tau\sigma$. The subgroups of G are

$$\langle \text{id} \rangle, \quad \langle \sigma \rangle, \quad \langle \tau \rangle, \quad \langle \sigma\tau \rangle, \quad \langle \sigma^2\tau \rangle, \quad G$$

and the corresponding intermediate fields are

$$\mathbb{Q}((2)^{1/3}, \omega), \quad \mathbb{Q}(\omega), \quad \mathbb{Q}((2)^{1/3}), \quad \mathbb{Q}(\omega^2(2)^{1/3}), \quad \mathbb{Q}(\omega(2)^{1/3}), \quad \mathbb{Q}.$$

11: FACT Let \mathbb{K} be a finite Galois extension of \mathbb{F} and let \mathbb{L} be an arbitrary finite extension of \mathbb{F} —then $\mathbb{K} \vee \mathbb{L} \supset \mathbb{L}$ is a Galois extension and

$$\text{Gal}(\mathbb{K} \vee \mathbb{L}/\mathbb{L}) \approx \text{Gal}(\mathbb{K}/\mathbb{K} \cap \mathbb{L}).$$

In addition,

$$[\mathbb{K} \vee \mathbb{L} : \mathbb{L}] = [\mathbb{K} : \mathbb{K} \cap \mathbb{L}].$$

[Note: Tacitly, \mathbb{K} and \mathbb{L} lie inside some common field \mathbb{M} , hence $\mathbb{K} \vee \mathbb{L}$ is the subfield of \mathbb{M} generated by \mathbb{K} and \mathbb{L} . This said, the arrow

$$\text{Gal}(\mathbb{K} \vee \mathbb{L}/\mathbb{L}) \rightarrow \text{Gal}(\mathbb{K}/\mathbb{K} \cap \mathbb{L})$$

sends σ to its restriction $\sigma|_{\mathbb{K}}.$

12: FACT Suppose that \mathbb{L} is a finite Galois extension of \mathbb{K} –then

- $N_{\mathbb{L}/\mathbb{K}}(x) = \prod_{\sigma \in \text{Gal}(\mathbb{L}/\mathbb{K})} \sigma x$
- $T_{\mathbb{L}/\mathbb{K}}(x) = \sum_{\sigma \in \text{Gal}(\mathbb{L}/\mathbb{K})} \sigma x.$

13: NORMAL BASIS THEOREM If \mathbb{L}/\mathbb{K} is finite Galois, then $\exists x \in \mathbb{L}$ such that $\{\sigma x : \sigma \in \text{Gal}(\mathbb{L}/\mathbb{K})\}$ is a basis for \mathbb{L}/\mathbb{K} .

INFINITE GALOIS THEORY

1: FACT If \mathbb{K} is a field and if \mathbb{L} is an infinite Galois extension of \mathbb{K} , then

$$\text{card Gal}(\mathbb{L}/\mathbb{K}) \geq 2^{\aleph_0}.$$

2: APPLICATION The Galois group of an infinite Galois extension cannot be cyclic.

3: FACT If \mathbb{F} is a field and if $G \subset \text{Aut}(\mathbb{F})$ is a finite group of automorphisms of \mathbb{F} , then G is a Galois group on \mathbb{F} : The a priori containment

$$G \subset \text{Gal}(\mathbb{F}/\text{Inv}(G))$$

is an equality:

$$G = \text{Gal}(\mathbb{F}/\text{Inv}(G)).$$

4: REMARK In general, an infinite group of automorphisms of a field need not be a Galois group.

Given a field \mathbb{F} and an element $a \in \mathbb{F}$, let D_a denote the discrete topological space having \mathbb{F} as its set of points –then the elements of the product

$$\prod_{a \in \mathbb{F}} D_a$$

are just the maps $\mathbb{F}^{\mathbb{F}}$ from \mathbb{F} to \mathbb{F} .

When equipped with the product topology, $\mathbb{F}^{\mathbb{F}}$ is Hausdorff and totally disconnected (but not discrete if $\text{card } \mathbb{F} \geq \aleph_0$). Since $\text{Aut}(\mathbb{F})$ is contained in $\mathbb{F}^{\mathbb{F}}$, it can be endowed with the relativized product topology, the so-called finite topology.

5: N.B. Given $\phi \in \text{Aut}(\mathbb{F})$ and a finite subset A of \mathbb{F} , let $\Omega_\phi(A)$ be the set of all automorphisms of \mathbb{F} that agree with ϕ on A —then $\Omega_\phi(A)$ is open and the collection $\{\Omega_\phi(A)\}$ is a neighborhood basis at ϕ .

6: FACT In the finite topology, $\text{Aut}(\mathbb{F})$ is a topological group (as well as being Hausdorff and totally disconnected).

In what follows, if $\Gamma \subset \text{Aut}(\mathbb{F})$ is a group of automorphisms of \mathbb{F} , it will be understood that Γ carries the relativized finite topology.

7: FACT Suppose that $\Gamma \subset \text{Aut}(\mathbb{F})$ is compact —then Γ is a Galois group on \mathbb{F} .

8: REMARK A group of automorphisms of \mathbb{F} is compact iff it is closed in $\text{Aut}(\mathbb{F})$ and has finite orbits.

9: FACT If \mathbb{K} is a field and if \mathbb{L} is an extension of \mathbb{K} , then

$$\text{Gal}(\mathbb{L}/\mathbb{K}) \subset \text{Aut}(\mathbb{L})$$

is closed.

10: FACT If \mathbb{K} is a field and if \mathbb{L} is an algebraic extension of \mathbb{K} , then

$$\text{Gal}(\mathbb{L}/\mathbb{K}) \subset \text{Aut}(\mathbb{L})$$

is compact.

[Note: If \mathbb{L} is finite over \mathbb{K} (hence algebraic), then $\text{Gal}(\mathbb{L}/\mathbb{K})$ is discrete.]

11: REMARK The compactness of the Galois group does not characterize algebraic extensions (there exist transcendental extensions with a finite Galois group).

[Note: If \mathbb{K} is an infinite field and if $\mathbb{K}(\xi)$ is a simple transcendental extension of \mathbb{K} , then $\text{Gal}(\mathbb{K}(\xi)/\mathbb{K})$ is not compact.]

12: FUNDAMENTAL THEOREM OF INFINITE GALOIS THEORY

Suppose that \mathbb{L} is an infinite Galois extension of \mathbb{K} (hence algebraic, hence $\text{Gal}(\mathbb{L}/\mathbb{K})$ compact).

- If $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$, then $\text{Gal}(\mathbb{L}/\mathbb{E})$ is a closed subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$ (thus is a compact subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$).
- If G is a closed subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$ (thus is a compact subgroup of $\text{Gal}(\mathbb{L}/\mathbb{K})$), then $\text{Inv}(G)$ is an intermediate field between \mathbb{K} and \mathbb{L} .

And: The arrow $\mathbb{E} \rightarrow \text{Gal}(\mathbb{L}/\mathbb{E})$ from the set of all intermediate fields between \mathbb{K} and \mathbb{L} to the set of all closed subgroups of $\text{Gal}(\mathbb{L}/\mathbb{K})$ and the arrow $G \rightarrow \text{Inv}(G)$ from the set of all closed subgroups of $\text{Gal}(\mathbb{L}/\mathbb{K})$ to the set of all intermediate fields between \mathbb{K} and \mathbb{L} are mutually inverse inclusion reversing bijections.

13: REMARK Since \mathbb{L}/\mathbb{K} is an infinite Galois extension, $\text{Gal}(\mathbb{L}/\mathbb{K})$ always contains a subgroup that is not closed.

[Any infinite group has a countably infinite subgroup (consider the subgroup generated by a countably infinite subset). On the other hand, an infinite compact totally disconnected Hausdorff group has cardinality at least that of the continuum (it has a quotient which is homeomorphic to the Cantor set).]

14: FACT \mathbb{E}/\mathbb{K} is finite iff $\text{Gal}(\mathbb{L}/\mathbb{E})$ is open.

15: FACT \mathbb{E}/\mathbb{K} is Galois iff $\text{Gal}(\mathbb{L}/\mathbb{E})$ is normal.

[Note: Canonically,

$$\text{Gal}(\mathbb{E}/\mathbb{K}) \approx \text{Gal}(\mathbb{L}/\mathbb{K})/\text{Gal}(\mathbb{L}/\mathbb{E}),$$

this being a topological identification if $\text{Gal}(\mathbb{L}/\mathbb{K})/\text{Gal}(\mathbb{L}/\mathbb{E})$ is given the quotient topology.]

16: N.B. \mathbb{L} is Galois over \mathbb{E} .

17: NOTATION

- $\bigvee_{i \in I} \mathbb{E}_i$ is the subfield generated by the union $\bigcup_{i \in I} \mathbb{E}_i$.
- $\bigvee_{i \in I} G_i$ is the subgroup generated by the union $\bigcup_{i \in I} G_i$.

18: FACT Let \mathbb{L} be an infinite Galois extension of \mathbb{K} .

- If \mathbb{E}_i ($i \in I$) is a nonempty family of intermediate fields between \mathbb{K} and \mathbb{L} ,

then

$$\text{Gal}\left(\mathbb{L}/\bigcap_{i \in I} \mathbb{E}_i\right) = \overline{\bigvee_{i \in I} \text{Gal}(\mathbb{L}/\mathbb{E}_i)}.$$

- If G_i ($i \in I$) is a nonempty family of closed subgroups of $\text{Gal}(\mathbb{L}/\mathbb{K})$, then

$$\text{Inv}\left(\bigcap_{i \in I} G_i\right) = \bigvee_{i \in I} \text{Inv}(G_i).$$

19: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$ (incorporate all primes) –then \mathbb{L} is Galois (and infinite) over \mathbb{K} (being the union of \mathbb{Q} , $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and so on). Here $\text{Gal}(\mathbb{L}/\mathbb{K})$ is a countably infinite direct product of copies of $\mathbb{Z}/2\mathbb{Z}$. Accordingly, every \mathbb{K} -automorphism of \mathbb{L} different from $\text{id}_{\mathbb{L}}$ is an element of order 2.

20: EXAMPLE Take $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = A(\mathbb{C}/\mathbb{Q})$ –then \mathbb{L} is Galois (and infinite) over \mathbb{K} .

\mathbb{K}^{sep} AND \mathbb{K}^{ab}

Let \mathbb{K} be a field, \mathbb{L}/\mathbb{K} a field extension.

1: DEFINITION An element of \mathbb{L} is separable if it is algebraic over \mathbb{K} and is a simple zero of its minimal polynomial.

2: NOTATION $S(\mathbb{L}/\mathbb{K})$ is the set of all elements of \mathbb{L} that are separable over \mathbb{K} .

[Note: Therefore

$$S(\mathbb{L}/\mathbb{K}) \subset A(\mathbb{L}/\mathbb{K})$$

and

$$S(\mathbb{L}/\mathbb{K}) = A(\mathbb{L}/\mathbb{K})$$

if the characteristic of \mathbb{K} is zero.]

3: DEFINITION $S(\mathbb{L}/\mathbb{K})$ is the separable closure of \mathbb{K} in \mathbb{L} .

4: FACT $S(\mathbb{L}/\mathbb{K})$ is a field.

5: FACT If $\mathbb{L} \supset \mathbb{E} \supset \mathbb{K}$ and \mathbb{E} is a separable extension of \mathbb{K} , then $\mathbb{E} \subset S(\mathbb{L}/\mathbb{K})$.

6: NOTATION \mathbb{K}^{cl} is the algebraic closure of \mathbb{K} .

7: N.B. If \mathbb{K} is not perfect, then \mathbb{K}^{cl} is not Galois over \mathbb{K} .

8: NOTATION \mathbb{K}^{sep} is the separable closure of \mathbb{K} in \mathbb{K}^{cl} :

$$\mathbb{K}^{\text{sep}} = S(\mathbb{K}^{\text{cl}}/\mathbb{K}).$$

9: FACT \mathbb{K}^{sep} is the maximal separable extension of \mathbb{K} .

10: FACT \mathbb{K}^{sep} is a Galois extension of \mathbb{K} .

11: DEFINITION

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})$$

is the absolute Galois group of \mathbb{K} .

12: FACT If \mathbb{L}/\mathbb{K} is Galois, then $\text{Gal}(\mathbb{L}/\mathbb{K})$ is a homomorphic image of $\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})$.

[This is because $\text{Gal}(\mathbb{L}/\mathbb{K})$ can be identified with the quotient

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})/\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L}).]$$

13: EXAMPLE Take $\mathbb{K} = \mathbb{F}_p$ –then $\text{Gal}(\mathbb{F}_p^{\text{sep}}/\mathbb{F}_p)$ can be identified with $\varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ (the set of all (equivalence classes) of sequences $\{a_n\} = \{a_1, a_2, \dots\}$ of natural numbers such that

$$a_n \equiv a_m \pmod{m}$$

whenever $m|n$).

[Bear in mind that $\forall n \in \mathbb{N}$, there is a Galois extension $\mathbb{K}_n/\mathbb{F}_p$ with $[\mathbb{K}_n : \mathbb{F}_p] = n$ and $\text{Gal}(\mathbb{K}_n/\mathbb{F}_p) \approx \mathbb{Z}/n\mathbb{Z}$.]

[Note: Let $\phi : \mathbb{F}_p^{\text{sep}} \rightarrow \mathbb{F}_p^{\text{sep}}$ be the Frobenius automorphism: $\phi(x) = x^p$. Let $G = \langle \phi \rangle$ –then

$$\text{Inv}(G) = \mathbb{F}_p, \quad \text{Inv}(\text{Gal}(\mathbb{F}_p^{\text{sep}}/\mathbb{F}_p)) = \mathbb{F}_p,$$

yet

$$G \neq \text{Gal}(\mathbb{F}_p^{\text{sep}}/\mathbb{F}_p).]$$

14: NOTATION $\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})$ is the commutator subgroup of $\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})$.

15: FACT

$$\text{Inv}(\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})) = \text{Inv}(\overline{\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})}).$$

[Put

$$\Gamma = \text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}).$$

Then

$$\Gamma \subset \bar{\Gamma} \implies \text{Inv}(\bar{\Gamma}) \subset \text{Inv}(\Gamma).$$

To go the other way, let $x \in \text{Inv}(\Gamma)$, $\bar{\gamma} \in \bar{\Gamma}$ and claim: $\bar{\gamma}x = x$ (hence $x \in \text{Inv}(\bar{\Gamma})$). If $\bar{\gamma} \in \Gamma$, we are through; otherwise, $\bar{\gamma}$ is an accumulation point of Γ , thus since $\Omega_{\bar{\gamma}}(\{x\})$ is a neighborhood of $\bar{\gamma}$, it must contain a $\gamma \in \Gamma$ ($\gamma \neq \bar{\gamma}$). But

$$\gamma \in \Gamma \cap \Omega_{\bar{\gamma}}(\{x\}) \implies \gamma \in \Omega_{\bar{\gamma}}(\{x\}) \implies \gamma x = \bar{\gamma}x.$$

Meanwhile,

$$\gamma \in \Gamma \ \& \ x \in \text{Inv}(\Gamma) \implies \gamma x = x.$$

Therefore $\bar{\gamma}x = x$.]

16: N.B.

$$\overline{\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})}$$

is a closed normal subgroup of $\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})$.

17: DEFINITION

$$\text{Inv}(\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}))$$

is called the maximal abelian extension of \mathbb{K} , denote it by \mathbb{K}^{ab} .

18: FACT \mathbb{K}^{ab} is a Galois extension of \mathbb{K} and $\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K})$ is an abelian group.

[Since

$$\overline{\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})}$$

is a closed normal subgroup of $\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})$, it follows that

$$\begin{aligned}\mathbb{K}^{\text{ab}} &= \text{Inv}(\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})) \\ &= \text{Inv}(\overline{\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})})\end{aligned}$$

is a Galois extension of \mathbb{K} and

$$\begin{aligned}\text{Gal}(\mathbb{K}^{\text{ab}}/\mathbb{K}) &\approx \text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})/\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K}^{\text{ab}}) \\ &= \text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})/\overline{\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})}\end{aligned}$$

But the group on the RHS is isomorphic to

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})/\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})/\overline{\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})}/\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}),$$

thus is a homomorphic image of the abelian group

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})/\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}).]$$

19: DEFINITION A Galois extenssion \mathbb{L}/\mathbb{K} is said to be abelian if $\text{Gal}(\mathbb{L}/\mathbb{K})$ is abelian.

20: FACT The field \mathbb{K}^{ab} has no extensions that are abelian Galois extensions of \mathbb{K} .

[Let $\mathbb{L}/\mathbb{K}^{\text{ab}}$ be an abelian Galois extensions of \mathbb{K} :

$$\mathbb{L} = \text{Inv}(\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})) \supset \mathbb{K}^{\text{ab}} = \text{Inv}(\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}))$$

\implies

$$\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}) \supset \text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L}).$$

On the other hand, $\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L})$ is normal (\mathbb{L}/\mathbb{K} being Galois) and

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{K})/\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L}) \approx \text{Gal}(\mathbb{L}/\mathbb{K}),$$

which is abelian by hypothesis, thus

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L}) \supset \text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}).$$

Therefore

$$\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L}) = \text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K}).$$

And then

$$\begin{aligned} \mathbb{L} &= \text{Inv}(\text{Gal}(\mathbb{K}^{\text{sep}}/\mathbb{L})) \\ &= \text{Inv}(\text{Gal}^*(\mathbb{K}^{\text{sep}}/\mathbb{K})) \\ &= \mathbb{K}^{\text{ab}}.] \end{aligned}$$

21: FACT \mathbb{K}^{ab} is generated by the set of finite abelian Galois extensions of \mathbb{K} in \mathbb{K}^{sep} .

[Every finite Galois extension of \mathbb{K} inside \mathbb{K}^{ab} is necessarily abelian.]

22: DEFINITION Take $\mathbb{K} = \mathbb{Q}$ —then the splitting field $\mathbb{Q}(n)$ of the polynomial $X^n - 1$ is called the cyclotomic field of the n^{th} roots of unity.

23: FACT $\mathbb{Q}(n)$ is a Galois extension of \mathbb{Q} and $\text{Gal}(\mathbb{Q}(n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, hence $\text{Gal}(\mathbb{Q}(n)/\mathbb{Q})$ is abelian.

Accordingly, every intermediate field \mathbb{E} between \mathbb{Q} and $\mathbb{Q}(n)$ is abelian Galois (per \mathbb{Q}).

[$\text{Gal}(\mathbb{Q}(n)/\mathbb{Q})$ is abelian, hence every subgroup of $\text{Gal}(\mathbb{Q}(n)/\mathbb{Q})$ is normal, hence in particular $\text{Gal}(\mathbb{Q}(n)/\mathbb{E})$ is normal, hence \mathbb{E}/\mathbb{Q} is Galois. And

$$\text{Gal}(\mathbb{E}/\mathbb{Q}) \approx \text{Gal}(\mathbb{Q}(n)/\mathbb{Q})/\text{Gal}(\mathbb{Q}(n)/\mathbb{E}).]$$

The Kronecker-Weber theorem states that every finite abelian Galois extension of \mathbb{Q} is contained in some $\mathbb{Q}(n)$, thus \mathbb{Q}^{ab} is the infinite cyclotomic extension $\mathbb{Q}(1, 2, \dots)$.

24: SCHOLIUM \mathbb{Q}^{ab} is generated by the torsion points of the action of \mathbb{Z} on \mathbb{C}^\times .

[Note: Given $n \in \mathbb{Z}$, $x \in \mathbb{C}^\times$, $(n, x) \rightarrow n \cdot x = x^n$.]

ADDENDUM

If G is a group, then the subgroup G^* generated by the commutators $xyx^{-1}y^{-1}$ is the commutator subgroup of G .

- G^* is a normal subgroup of G .
- G/G^* is abelian.

And if $H \subset G$ is normal and if G/H is abelian, then $H \supset G^*$.

FACT If \mathbb{L}/\mathbb{K} is an infinite Galois extension and if $N \subset \text{Gal}(\mathbb{L}/\mathbb{K})$ is a normal subgroup, then $\overline{N} \subset \text{Gal}(\mathbb{L}/\mathbb{K})$ is a closed normal subgroup.

REFERENCES

Arakawa, T. et al.

- [1] Bernoulli Numbers and Zeta Functions, Springer Verlag, 2004.

Cassels, J. and Frölich, A

- [2] Algebraic Number Theory, Academic Press, 1967.

Edwards, H.

- [3] Galois Theory, Springer Verlag, 1984.

Gouvea, F.

- [4] p -adic Numbers, Springer Verlag, 1991.

Howe, R. and Tan, E.

- [5] Non-Abelian Harmonic Analysis, Springer Verlag, 1992.

Iwasawa, K.

- [6] Lectures on p -adic L -functions, Princeton University Press, 1972.

Koblitz, N.

- [7-(a)] p -adic Analysis: A Short Course on Recent Work, Cambridge University Press, 1980.

- [7-(b)] p -adic Numbers, p -adic Analysis, and Zeta-Functions, Springer Verlag, 1984.

Körner, T.

- [8] Fourier Analysis, Cambridge University Press, 1988.

Morandi, P.

- [9] Field and Galois Theory, Springer Verlag, 1996.

Patterson, S.

- [10] An Introduction to the Theory of the Riemann Zeta-Function, Cambridge University Press, 1988.

Srivastava, H. and Junesang, C.

- [11] Zeta and q -Zeta Functions and Associated Series and Integrals, Elsevier, 2012.

Weil, A.

- [12] Basic Number Theory, Springer Verlag, 1967.

Index

- H^\perp , 7-5
- P , 5-1
- R , 5-1
- R^\times , 5-1
- \mathbb{K}_{ur} , 5-6
- \mathbb{Q}_p , 4-1
- \mathbb{C}_p , 4-17
- \mathbb{Z}_p , 4-4
- \mathbb{Z}_p^\times , 4-4
- INV**, 7-7
- rec_q , 20-2
- \mathcal{A} , 4-1
- $\mathcal{B}(G)$, 10-2
- $\mathcal{B}(\mathbb{A}_{\text{fin}})$, 15-3
- $\mathcal{B}_\infty(\mathbb{A})$, 15-3
- n -dimensional special representation, 24-2
- p -adic absolute value, 1-5
- p -adic integers, 4-4
- p -adic units, 4-5
- p -primary group, 8-5
- $p\mathbb{Z}_p$, 4-4
- absolute value, 1-1
- absolute values equivalence , 1-2
- adele class group, 14-3
- adeles, 14-1
- Bruhat space, 10-2, 15-3
- Bruhat-Schwartz space, 15-3
- canonical absolute value, 5-4
- character, 7-1
- compact open topology, 7-2
- completely reducible, 22-5
- conductor, 8-2, 9-2
- Deligne representation, 24-1
- Deligne representation, direct sum, 24-4
- Deligne representation, indecomposable, 24-6
- Deligne representation, invariant subspace, 24-5
- Deligne representation, isomorphic, 24-5
- Deligne representation, semisimple, 24-6
- Deligne representation, tensor product, 24-4
- Deligne representations, contragredient, 24-4
- differential of \mathbb{K} , 8-11
- dual group, 7-2
- equivalent representations, 22-5
- finite adeles, 14-1
- finite ideles, 14-4
- Fourier inversion, 7-7
- Fourier transform, 7-6, 10-4, 10-10
- fractional part, 8-2
- functional equation, 11-3, 12-2
- fundamental domain, 14-3
- global zeta function, 17-1
- Haar measure, 6-1
- i^{th} ramification group in the upper numbering, 21-3

- idele class group, 14-5
- ideles, 14-4
- inertia group, 21-4
- integral part, 8-2
- irreducible, 22-4
- local field, 5-1
- local zeta function, 11-1, 12-1, 18-1, 18-2
- maximal unramified extension, 21-4
- Mellin transform, 10-8, 10-11
- non-archimedean, 1-4
- norm residue symbol, 21-2
- normalized absolute value, 5-4
- normalized Haar measure, 6-8
- order, 1-2
- Parseval theorem, 7-14
- place, 1-4
- Plancherel theorem, 7-13
- Pontryagin duality, 7-5
- prime element, 5-2
- principal units, 4-11
- Product principle, 8-9
- Quadratic extensions, 5-7
- Radon measure, 6-1
- ramification index, 5-4
- ramified, 5-6
- ramified of degree $n \geq 1$, 9-2
- reduction mod p , 4-8
- representation, 22-2, 24-2
- representation of $\mathrm{SL}(2, \mathbb{C})$, 24-8
- residual index, 5-5
- residue field, 5-1
- restricted open rectangle, 13-1
- restricted product, 13-1
- restricted product topology, 13-2
- Schwartz space, 10-1
- semisimple, 22-3
- shells, 4-10
- standard (test function), 10-1, 10-2
- test functions, 10-1
- test functions (on G), 10-2
- the differential exponent of \mathbb{K} , 8-11
- topological abelianization, 21-5
- topological field, 2-2
- transfer homomorphism, 21-6
- triangle inequality, 1-3
- trivial absolute value, 1-1
- ultrametric inequality, 1-4
- unitary character, 7-1
- unramified, 5-6
- Weil group, 22-1
- Weil-Deligne group, 24-1