THE CHARACTER GROUP OF Q

KEITH CONRAD

1. Introduction

The characters of a finite abelian group G are the homomorphisms from G to the unit circle $S^1 = \{z \in \mathbf{C} : |z| = 1\}$. Two characters can be multiplied pointwise to define a new character, and under this operation the set of characters of G forms an abelian group, with identity element the trivial character, which sends each $g \in G$ to 1. Characters of finite abelian groups are important, for example, as a tool in estimating the number of solutions to equations over finite fields. [3, Chapters 8, 10].

The extension of the notion of a character to nonabelian or infinite groups is essential to many areas of mathematics, in the context of harmonic analysis or representation theory, but here we will focus on discussing characters on one of the simplest infinite abelian groups, the rational numbers $\mathbf{Q}$. This is a special case of a situation that is well-known in algebraic number theory, but all references I could find in the literature are based on [4], where one can't readily isolate the examination of the character group of $\mathbf{Q}$ without assuming algebraic number theory and Fourier analysis on locally compact abelian groups. (In [2, Chapter 3,§1], the determination of the characters of $\mathbf{Q}$ is made without algebraic number theory, but the Pontryagin duality theorem from Fourier analysis is used at the end.) The prerequisites for the discussion here are more elementary: familiarity with the complex exponential function, the p-adic numbers $\mathbf{Q}_p$, and a few facts about abelian groups. In particular, this discussion should be suitable for someone who has just learned about the p-adic numbers and wants to see how they can arise in answering a basic type of question about the rational numbers.

Concerning notation, r and s will denote rational numbers, p and q will denote prime numbers, and x and y will denote real or p-adic numbers (depending on the context). The word "homomorphism" will always mean "group homomorphism", although sometimes we will add the word "group" for emphasis. The sets $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{Q}_p$, and the p-adic integers $\mathbf{Z}_p$, will be regarded

primarily as additive groups, with multiplication on these sets being used as a tool in the study of the additive structure.

2. Definition and Examples

The definition of characters for finite abelian groups makes sense for any group.

Definition 2.1. A *character* of $\mathbf{Q}$ is a group homomorphism $\mathbf{Q} \to S^1$.

As in the case of characters of finite abelian groups, under pointwise multiplication the characters of $\mathbf{Q}$ form an abelian group, which we denote by $\widehat{\mathbf{Q}}$. Examples of nontrivial characters of $\mathbf{Q}$ are the homomorphisms $r \mapsto e^{ir}$ and $r \mapsto e^{2\pi ir}$. Our goal is to write down all elements of $\widehat{\mathbf{Q}}$ using explicit functions.

The usefulness of $\widehat{\mathbf{Q}}$ can't be discussed here, but hopefully the reader can regard its determination as an interesting problem, especially since the end result will be more complicated than it may seem at first glance.

The prototype for our task is the classification of *continuous* group homomorphisms from $\mathbf{R}$ to S^1. The example $x \mapsto e^{ix}$ is typical. In general, for any $y \in \mathbf{R}$ we have the homomorphism

$$x \mapsto e^{2\pi ixy}.$$

The use of the scaling factor 2π here is prominent in number theory, since it makes certain formulas much cleaner. For the reader who is interested in a proof that these are *all* the continuous homomorphisms $\mathbf{R} \to S^1$, see the appendix. We will not need to know that every continuous homomorphism $\mathbf{R} \to S^1$ has this form, but we want to analyze $\widehat{\mathbf{Q}}$ with a similar goal in mind, namely to find a relatively concrete method of writing down the homomorphisms $\mathbf{Q} \to S^1$. Keep in mind that we are imposing no continuity conditions on the elements of $\widehat{\mathbf{Q}}$; as functions from $\mathbf{Q}$ to S^1, they are merely group homomorphisms. (Or think of $\mathbf{Q}$ as a discrete group, so group homomorphisms are always continuous.)

Let's now give examples of nontrivial characters of $\mathbf{Q}$. First we will think of $\mathbf{Q}$ as lying in the real numbers. For nonzero $y \in \mathbf{R}$, the map $x \mapsto e^{2\pi ixy}$ is continuous on $\mathbf{R}$, hits all of S^1, and $\mathbf{Q}$ is dense in $\mathbf{R}$, so the restriction of this function to $\mathbf{Q}$, *i.e.*, the function

$$r \mapsto e^{2\pi iry},$$

is a nontrivial character of $\mathbf{Q}$. When $y = 0$, this is the trivial character.

It is easy to believe that these may be all of the characters of $\mathbf{Q}$, since the usual picture of $\mathbf{Q}$ inside $\mathbf{R}$ makes it hard to think of any way to write down characters of $\mathbf{Q}$ besides those of the form $r \mapsto e^{2\pi iry}$ ($y \in \mathbf{R}$). However, such characters of $\mathbf{Q}$ are only the tip of the iceberg. We will now show how to make sense of $e^{2\pi iy}$ for p-adic y, and the new characters of $\mathbf{Q}$ which follow from this will allow us to easily write down all characters of $\mathbf{Q}$. That is, in a loose sense, every character of $\mathbf{Q}$ is a mixture of functions that look like $r \mapsto e^{2\pi iry}$ for y in $\mathbf{R}$ or some $\mathbf{Q}_p$.

Technically, $e^{2\pi iry}$ is meaningless if y is a general p-adic number. We introduce a formalism that should be thought of as allowing us to make sense of this expression anyway.

For $x \in \mathbf{Q}_p$, define the *p-adic fractional part* of x, denoted $\{x\}_p$, to be the sum of the negative-power-of-p terms in the usual p-adic expansion of x.

Let's compute the p-adic fractional part of $21/50$ for several p. In $\mathbf{Q}_2, \mathbf{Q}_3$, and $\mathbf{Q}_5$,

$$\frac{21}{50} = \frac{1}{2}+2+2^2+2^3+\dots, \quad \frac{21}{50} = 2\cdot 3+3^2+3^6+\dots, \quad \frac{21}{50} = \frac{3}{25}+\frac{4}{5}+2+2\cdot 5+\dots.$$

Therefore

$$\left\{\frac{21}{50}\right\}_2 = \frac{1}{2}, \quad \left\{\frac{21}{50}\right\}_3 = 0, \quad \left\{\frac{21}{50}\right\}_5 = \frac{3}{25}+\frac{4}{5} = \frac{23}{25}.$$

For any $p \neq 2, 5$, $\{\frac{21}{50}\}_p = 0$. More generally, any $r \in \mathbf{Q}$ is in $\mathbf{Z}_p$ for all but finitely many p, so $\{r\}_p = 0$ for all but finitely many p.

Note that for $0 \leq m \leq p^n - 1$, $\{\frac{m}{p^n}\}_p = \frac{m}{p^n}$.

In thinking of p-adic expansions as analogous to Laurent series in complex analysis, the p-adic fractional part is analogous to the polar part of a p-adic number. (One difference: the polar part of a sum of two meromorphic functions at a point is the sum of the polar parts, but the p-adic fractional part of a sum of two p-adic numbers is *not* usually the sum of their individual p-adic fractional parts. Carrying in p-adic addition can allow the sum of p-adic fractional parts to "leak" into a p-adic integral part; consider $3/5 + 4/5 = 2/5 + 1$.) There is an analogue in $\mathbf{Q}$ of the partial fraction decomposition of rational functions:

$$r = \sum_p \{r\}_p + \text{integer}. \tag{2.1}$$

This sum over all p makes sense, since most terms are 0. It expresses r as a sum of rational numbers with prime power denominator, up to addition by

an integer. For example,

$$\begin{aligned}\sum_p \left\{\frac{21}{50}\right\}_p &= \left\{\frac{21}{50}\right\}_2 + \left\{\frac{21}{50}\right\}_5 \\ &= \frac{1}{2} + \frac{23}{25} \\ &= \frac{71}{50} \\ &= \frac{21}{50} + 1.\end{aligned}$$

To prove (2.1), we show the difference $r - \sum_p \{r\}_p$, which is rational, has no prime in its denominator. For $p \neq q$, $\{r\}_p \in \mathbf{Z}_q$, while $r - \{r\}_q \in \mathbf{Z}_q$ by the definition of $\{r\}_q$. Thus $r - \sum_p \{r\}_p = r - \{r\}_q - \sum_{p \neq q} \{r\}_p$ is in $\mathbf{Z}_q$. Applying this to all q, $r - \sum_p \{r\}_p$ is in $\mathbf{Z}$.

Remark 2.2. If we view Equation 2.1 not in $\mathbf{Q}$ but in $\mathbf{Q}/\mathbf{Z}$, it expresses an element of $\mathbf{Q}/\mathbf{Z}$ as a sum of elements of p-power order for different primes. This is the explicit realization of the torsion abelian group $\mathbf{Q}/\mathbf{Z}$ as the direct sum of its p-power torsion subgroups.

The p-adic fractional part should be thought of as a p-adic analogue of the usual fractional part function $\{\cdot\}$ on $\mathbf{R}$, where $\{x\} \in [0, 1)$ and $x - \{x\} \in \mathbf{Z}$. In particular, for real x we have $\{x\} = 0$ precisely when $x \in \mathbf{Z}$. The p-adic fractional part has similar features. For $x \in \mathbf{Q}_p$,

$$\{x\}_p = \frac{m}{p^n} \in [0, 1) \ (0 \leq m \leq p^n - 1), \quad x - \{x\}_p \in \mathbf{Z}_p, \quad \{x\}_p = 0 \Leftrightarrow x \in \mathbf{Z}_p.$$

While the ordinary fractional part on $\mathbf{R}$ is not additive, the deviation from additivity is given by an integer:

$$\{x + y\} = \{x\} + \{y\} + \text{integer}.$$

This deviation from additivity gets wiped out when we take the complex exponential of both sides: $e^{2\pi i\{x+y\}} = e^{2\pi i\{x\}} e^{2\pi i\{y\}}$. Of course $e^{2\pi i\{x\}} = e^{2\pi ix}$ for $x \in \mathbf{R}$, so there is no need to use the fractional part. But in the p-adic case, the fractional-part viewpoint gives us the following basic definition:

For $x \in \mathbf{Q}_p$, set

$$\psi_p(x) = e^{2\pi i\{x\}_p}.$$

This is not the exponential of a p-adic number: $\{x\}_p$ is a rational number with p-power denominator, so $e^{2\pi i\{x\}_p}$ is some p-th power root of unity.

Example 2.3.

$$\psi_2(21/50) = e^{2\pi i(1/2)} = -1, \quad \psi_3(21/50) = 1, \quad \psi_5(21/50) = e^{2\pi i(23/25)}.$$

Example 2.4. Let $a \in \mathbf{Q}_7$ be the solution to $x^2 = 2$ such that $a \equiv 3 \bmod 7\mathbf{Z}_7$. Then $a \equiv 3 + 7 + 2 \cdot 7^2 \bmod 7^3\mathbf{Z}_7$, so $\psi_7(a/7^3) = e^{2\pi i\{a/7^3\}_7} = e^{2\pi i(3+7+7^2)/7^3} = e^{2\pi i \cdot 59/343}$.

The function ψ_p is a group homomorphism: $e^{2\pi i\{x+y\}_p} = e^{2\pi i\{x\}_p} e^{2\pi i\{y\}_p}$. To see this, we have to understand the extent to which the p-adic fractional part fails to be additive. For $x, y \in \mathbf{Q}_p$,

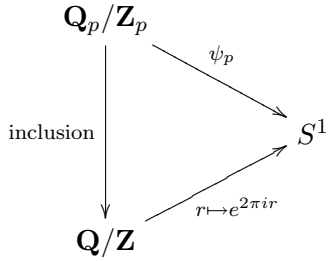
$$x - \{x\}_p, \ y - \{y\}_p, \ x + y - \{x + y\}_p \in \mathbf{Z}_p.$$

Adding the first two terms and subtracting the third, we see that the rational number $\{x\}_p + \{y\}_p - \{x + y\}_p$ is a p-adic integer. As a sum/difference of p-adic fractional parts, it has a power of p as denominator. Since it is also a p-adic integer, there is no power of p in the denominator, so the denominator must be 1. Therefore

$$\{x\}_p + \{y\}_p - \{x + y\}_p \in \mathbf{Z}.$$

Thus ψ_p is a group homomorphism. This is the technical way we make sense of the meaningless expression $e^{2\pi ix}$ for $x \in \mathbf{Q}_p$; $e^{2\pi ix}$ can be thought of precisely as $e^{2\pi i\{x\}_p}$. (*Warning*: when x is rational, so $e^{2\pi ix}$ makes sense in the usual way, but this is generally not the same as $e^{2\pi i\{x\}_p}$. Referring to $e^{2\pi i\{x\}_p}$ as just a "sensible interpretation" of $e^{2\pi ix}$ for p-adic x should only be considered as a loose manner of speaking.)

Remark 2.5. The group $\mathbf{Q}_p/\mathbf{Z}_p$ is isomorphic to the p-power torsion subgroup of $\mathbf{Q}/\mathbf{Z}$: $\mathbf{Q}/\mathbf{Z} \cong \bigoplus_p \mathbf{Q}_p/\mathbf{Z}_p$. The character ψ_p fits into the commutative diagram



Unlike the function $x \mapsto e^{2\pi ix}$ for real x, the function $\psi_p\colon x \mapsto e^{2\pi i\{x\}_p}$ does not take on all values in S^1. Its image is exactly the pth power roots

of unity. It is also locally constant (so continuous in an elementary way), since $\psi_p(x+y) = \psi_p(x)$ for $y \in \mathbf{Z}_p$, and $\mathbf{Z}_p$ is a neighborhood of 0.

By the same type of "interior scaling" argument as for the basic character $e^{2\pi ix}$ on the reals, we can use ψ_p to construct many continuous characters of $\mathbf{Q}_p$. Choosing any $y \in \mathbf{Q}_p$, we have a group homomorphism $\mathbf{Q}_p \to S^1$ by

$$x \mapsto \psi_p(xy) = e^{2\pi i\{xy\}_p}.$$

By varying y in $\mathbf{Q}_p$, we get lots of examples of nontrivial continuous homomorphisms $\mathbf{Q}_p \to S^1$. It is a fact that all continuous homomorphisms $\mathbf{Q}_p \to S^1$ are of the above type, but we will not need this fact in our study of the character group $\widehat{\mathbf{Q}}$ of $\mathbf{Q}$. However, our analysis of $\widehat{\mathbf{Q}}$ contains the essential ingredients for a proof, so we will discuss this again in the appendix.

By restricting a character of $\mathbf{Q}_p$ to the subset $\mathbf{Q}$, we get new characters of $\mathbf{Q}$. For fixed $y \in \mathbf{Q}_p$, let

$$r \mapsto e^{2\pi i\{ry\}_p}.$$

This character of $\mathbf{Q}$ takes as values only the pth power roots of unity, so it is quite different (for $y \neq 0$) from the functions $r \mapsto e^{2\pi iry}$ for real y.

Example 2.6. For a 5-adic number y, let $\chi\colon \mathbf{Q} \to S^1$ be defined by $\chi(r) = e^{2\pi i\{ry\}_5}$. We want to calculate $\chi(21/50)$. Since

$$\frac{21}{50} = \frac{3}{25} + \frac{4}{5} + \dots,$$

we need to know the 5-adic expansion of y out to the multiple of 5. If, for instance, $y = 4 + 1 \cdot 5 + \dots$, then $(21/50)y = 2/25 + 1/5 + \dots$, so $\chi(21/50) = e^{14\pi i/25}$. To compute $\chi(r)$ for a specific rational number r, we only need to know the 5-adic expansion of y to an appropriate finite number of places, depending on the 5-adic expansion of r.

3. $\widehat{\mathbf{Q}}$ and the Adeles

We shall now use the above homomorphisms from $\mathbf{R}$ and the various $\mathbf{Q}_p$'s to S^1 to construct *all* homomorphisms from $\mathbf{Q}$ to S^1, *i.e.*, all elements of $\widehat{\mathbf{Q}}$. This is a simple example of the "local-global" philosophy in number theory, which says that one should try to analyze a problem over $\mathbf{Q}$ (the "global" field) by first analyzing it over each of the completions $\mathbf{R}, \mathbf{Q}_2, \mathbf{Q}_3, \dots$ of $\mathbf{Q}$ (the "local" fields), and then use this information over the completions to solve the problem over $\mathbf{Q}$. The problem we are concerned with is the

construction of homomorphisms to S^1, and we have already taken care of the "local" problem, at least for our purposes.

Define $\psi_\infty\colon \mathbf{R} \to S^1$ by $x \mapsto e^{-2\pi i x}$ (the reason for the minus sign will be apparent later). Define, as before, $\psi_p\colon \mathbf{Q}_p \to S^1$ by $x \mapsto e^{2\pi i\{x\}_p}$. Now choose any elements $a_\infty \in \mathbf{R}$ and $a_p \in \mathbf{Q}_p$ for all primes p, with the proviso that $a_p \in \mathbf{Z}_p$ *for all but finitely many* p. We define a function $\mathbf{Q} \to S^1$ by

$$\begin{aligned} r &\mapsto \psi_\infty(ra_\infty) \cdot \prod_p \psi_p(ra_p) \\ &= e^{-2\pi i r a_\infty} \cdot \prod_p e^{2\pi i\{ra_p\}_p}. \end{aligned}$$

To show this map makes sense and is a character, note that for any rational r, $r \in \mathbf{Z}_p$ for all but finitely many primes p, so by our convention on the a_p's, $ra_p \in \mathbf{Z}_p$ for all but finitely many primes p. (The finitely many p such that $ra_p \notin \mathbf{Z}_p$ will of course vary with r. It is *not* the case that factors where $a_p \in \mathbf{Z}_p$ play no role, since we may have $ra_p \notin \mathbf{Z}_p$ when $a_p \in \mathbf{Z}_p$, if the denominator of r has a large power of p.) Thus $\psi_p(ra_p) = 1$ for all but finitely many p, so for each $r \in \mathbf{Q}$ the infinite product defining the above function at r is really a finite product.

Each "local function" $\psi_\infty, \psi_2, \psi_3, \dots$ is a homomorphism, so our map above is a homomorphism, hence is an element of $\widehat{\mathbf{Q}}$. The homomorphisms $\psi_\infty, \psi_2, \psi_3, \dots$ are our basic maps, and the numbers $a_\infty, a_2, a_3, \dots$ should be thought of as interior scaling factors that allow us to define many characters of $\mathbf{Q}$ in terms of the one basic character

$$r \mapsto e^{-2\pi i r} \cdot \prod_p e^{2\pi i r}.$$

To understand this construction better, we want to look at the sequences of elements $(a_\infty, a_2, a_3, \dots)$ that have just been used to define characters of $\mathbf{Q}$. This leads us to introduce a ring which plays a prominent role in number theory.

Definition 3.1. The *adeles*, $\mathbf{A}_\mathbf{Q}$, are the elements $(a_\infty, a_2, a_3, \dots)$ in the product set $\mathbf{R} \times \prod_p \mathbf{Q}_p$ such that a_p lies in $\mathbf{Z}_p$ for all but finitely many p.

A "random" adele will not have any rational coordinates. As an example of something which is *not* an adele, consider any element of the product set $\mathbf{R} \times \prod_p \mathbf{Q}_p$ whose p-adic coordinate is $1/p$ for infinitely many primes p. The adele ring of $\mathbf{Q}$ lies between the direct sum $\bigoplus_v \mathbf{Q}_v$ and the direct

product $\prod_v \mathbf{Q}_v$. It is called the restricted direct product of the $\mathbf{Q}_v$'s, and the restricted direct product notation is $\prod'_v \mathbf{Q}_v$

If a is a typical adele, its real coordinate will be written as a_∞ and its p-adic coordinate will be written as a_p. While ψ_∞ includes an awkward-looking minus sign (whose rationale will be explained below), a_∞ does not. It is the real coordinate of a, not its negative.

Under componentwise addition and multiplication, $\mathbf{A_Q}$ is a commutative ring (but not an integral domain). For our purposes, the additive group structure of $\mathbf{A_Q}$ is its most important algebraic feature. Since any rational number r is in $\mathbf{Z}_p$ for all but finitely many primes p, we see that $\mathbf{Q}$ naturally fits into $\mathbf{A_Q}$ by the diagonal map

$$r \mapsto (r, r, r, \dots),$$

making $\mathbf{Q}$ a subring of $\mathbf{A_Q}$. We shall call an adele *rational* if all of its coordinates are the *same* rational number, so the rational adeles are naturally identified with the rational numbers. We will write the rational adele $(r, r, r, \dots)$ just as r.

Let's see how the adeles are a useful notation to describe $\widehat{\mathbf{Q}}$. From what has been done so far, for any adele $a = (a_\infty, a_2, a_3, \dots)$ we have defined a character Ψ_a of $\mathbf{Q}$ by

$$\Psi_a(r) = \psi_\infty(ra_\infty) \cdot \prod_p \psi_p(ra_p) = e^{-2\pi i r a_\infty} \cdot \prod_p e^{2\pi i \{ra_p\}_p}.$$

Since addition in $\mathbf{A_Q}$ is componentwise, a computation shows that for adeles a and b

$$\Psi_{a+b}(r) = \Psi_a(r)\Psi_b(r)$$

for all rational numbers r, so in $\widehat{\mathbf{Q}}$ we have $\Psi_{a+b} = \Psi_a\Psi_b$. Clearly Ψ_0 is the trivial character.

For a *rational* adele s and any $r \in \mathbf{Q}$,

$$\Psi_s(r) = e^{2\pi i(-rs + \sum_p \{rs\}_p)} = 1$$

by (2.1). Thus Ψ_s is the trivial character for all rational adeles s. This is why the minus sign was used in the definition of ψ_∞. If a and b are two adeles whose difference is a rational adele, $\Psi_a = \Psi_b$.

The following theorem, which will be shown in the next section, tells us that we have found all of the characters of $\mathbf{Q}$, and can decide when we have described a character in two different ways.

Theorem 3.2. *Every character of $\mathbf{Q}$ has the form Ψ_a for some $a \in \mathbf{A_Q}$, and $\Psi_a = \Psi_b$ if and only if $a - b$ is a rational adele. In other words, the map $\Psi\colon \mathbf{A_Q} \to \widehat{\mathbf{Q}}$ given by $a \mapsto \Psi_a$ is a surjective homomorphism with kernel equal to the rational adeles $\mathbf{Q}$, so $\widehat{\mathbf{Q}} \cong \mathbf{A_Q}/\mathbf{Q}$.*

4. The Image and Kernel of Ψ

Let $\chi\colon \mathbf{Q} \to S^1$ be a character. We want to write $\chi = \Psi_a$ for some adele a.

We begin by considering $\chi(1)$, which is some number on the unit circle, so $\chi(1) = e^{-2\pi i\theta}$ for a (unique) real $\theta \in [0, 1)$. Define $\chi_\infty\colon \mathbf{Q} \to S^1$ by $\chi_\infty(r) = \psi_\infty(r\theta) = e^{-2\pi ir\theta}$. Then χ_∞ is a character of $\mathbf{Q}$ and $\chi_\infty(1) = \chi(1)$. Let $\chi'(r) = \chi(r)/\chi_\infty(r)$, so χ' is a character with $\chi'(1) = 1$ and $\chi(r) = \chi_\infty(r)\chi'(r)$.

For any rational $r = m/n$,

$$\chi'(r)^n = \chi'(m) = \chi'(1)^m = 1.$$

The image of χ' is inside the roots of unity, so dividing χ by χ_∞ to give us χ' puts us in an algebraic setting.

Every root of unity, say $e^{2\pi is}$ for $s \in \mathbf{Q}$, is a unique product of prime power roots of unity. Indeed, by (2.1)

$$e^{2\pi is} = \prod_p e^{2\pi i\{s\}_p},$$

where $e^{2\pi i\{s\}_p}$ is a pth power root of unity, equal to 1 for all but finitely many p.

Let $\chi_p(r)$ denote the p-th power root of unity that contributes to the root of unity $\chi'(r)$. For example, if $\chi'(r) = e^{3\pi i/7}$, then $\chi_2(r) = -1$, $\chi_7(r) = e^{10\pi i/7}$, and $\chi_p(r) = 1$ for all $p \neq 2, 7$. The function $\chi_p\colon \mathbf{Q} \to S^1$ is a character of $\mathbf{Q}$. Since $\chi'(1) = 1$, $\chi_p(1) = 1$ for all primes p.

Since $\chi'(r) = \prod_p \chi_p(r)$, we have

$$\chi(r) = \chi_\infty(r) \cdot \prod_p \chi_p(r).$$

This decomposition of χ can be viewed as the main step in describing $\widehat{\mathbf{Q}}$ in terms of adeles. We have broken up our character χ into "local" characters $\chi_\infty, \chi_2, \chi_3, \ldots$, and now proceed to analyze each one individually.

By construction, $\chi_\infty(r) = e^{-2\pi i r\theta}$ for some real $\theta \in [0,1)$. We now want to show that $\chi_p(r) = e^{2\pi i\{rc\}_p}$ for some $c \in \mathbf{Z}_p$. This will involve giving an explicit method for constructing c.

Since $\chi_p(1) = 1$, $\chi_p(1/p^n)^{p^n} = 1$, so $\chi_p(1/p^n) = e^{2\pi i c_n/p^n}$ for some (unique) integer c_n with $0 \leq c_n \leq p^n - 1$. Since $\chi_p(1/p^{n+1})^p = \chi_p(1/p^n)$, we get $c_{n+1} \equiv c_n \bmod p^n\mathbf{Z}$. Thus $\{c_1, c_2, c_3, \dots\}$ is a p-adic Cauchy sequence in $\mathbf{Z}$, so it has a limit $c \in \mathbf{Z}_p$, and $c \equiv c_n \bmod p^n\mathbf{Z}_p$ for all n. Since $0 \leq c_n \leq p^n - 1$,

$$\left\{\frac{c}{p^n}\right\}_p = \frac{c_n}{p^n}.$$

We now show $\chi_p(r) = e^{2\pi i\{rc\}_p} = \psi_p(rc)$ for all $r \in \mathbf{Q}$. Write $r = s/t$ where $s, t \in \mathbf{Z}$ with $t \neq 0$. Let $t = p^m t'$ for $(p, t') = 1$. Then

$$\chi_p(r)^{t'} = \chi_p(t'r) = \chi_p\left(\frac{s}{p^m}\right) = \varphi\left(\frac{1}{p^m}\right)^s = e^{2\pi i c_m s/p^m}.$$

In $\mathbf{Q}/\mathbf{Z}$,

$$\frac{c_m s}{p^m} == \left\{\frac{c}{p^m}\right\}_p \cdot s \equiv \left\{\frac{cs}{p^m}\right\}_p \equiv \{crt'\}_p \equiv \{cr\}_p t',$$

so $\chi_p(r)^{t'} = e^{2\pi i\{cr\}_p t'}$. Thus the p-th power roots of unity $\chi_p(r)$ and $e^{2\pi i\{cr\}_p}$ have a ratio that is a t'-th root of unity. Since t' is prime to p, this ratio must be 1, so

$$\chi_p\left(\frac{s}{t}\right) = e^{2\pi i\{cr\}_p} = \psi_p(rc).$$

Write $c \in \mathbf{Z}_p$ as a_p, so $\chi_p(r) = \psi_p(ra_p)$ for all $r \in \mathbf{Q}$. Therefore $\chi = \chi_\infty \cdot \prod_p \chi_p = \Psi_a$ for the adele $a = (\theta, a_2, a_3, \dots) \in [0,1) \times \prod_p \mathbf{Z}_p$.

We now know every character of $\mathbf{Q}$ has the form Ψ_a for an adele in the special set $[0,1) \times \prod_p \mathbf{Z}_p$. When the adele a is in this set, we can determine it from the character. Indeed, in this case all a_p are in $\mathbf{Z}_p$, so $\Psi_a(1) = e^{-2\pi i a_\infty}$. Since $a_\infty \in [0,1)$, it is completely determined from knowing $\Psi_a(1)$. We can then multiply Ψ_a by the character $e^{2\pi i r a_\infty}$ to assume $a_\infty = 0$. Then Ψ_a has only roots of unity as its values. The pth power component of $\Psi_a(r)$ is $e^{2\pi i\{a_p r\}_p}$, which upon taking $r = 1/p, 1/p^2$, etc. allows us to successively determine each digit of a_p, so we can determine a_p. Every character of $\mathbf{Q}$ has the form Ψ_a for a *unique* adele a in $[0,1) \times \prod_p \mathbf{Z}_p$. It turns out that every adele can be put into this set upon addition by a suitable rational adele:

$$\mathbf{A_Q} = \mathbf{Q} + [0,1) \times \prod_p \mathbf{Z}_p. \tag{4.1}$$

To prove (4.1), fix an adele a. We know $a_p \in \mathbf{Z}_p$ as long as p is outside of a finite set (say) F. Let $r = \sum_{p \in F} \{a_p\}_p$, the sum of the various pole parts of a. So $a - r$ has no pole parts, hence $a - r \in \mathbf{R} \times \prod_p \mathbf{Z}_p$. Let N be the integer such that $N \leq a_\infty - r < N + 1$. Since $N \in \mathbf{Z}_p$ for all primes p, we see that $a - (r + N) \in [0,1) \times \prod_p \mathbf{Z}_p$, so (4.1) is established.

The decomposition (4.1) is "direct," since $\mathbf{Q} \cap ([0,1) \times \prod_p \mathbf{Z}_p) = \{0\}$ (analogous to the relation $\mathbf{Z} \cap [0,1) = \{0\}$). We put direct in quotes since $[0,1)$ is not a group, so (4.1) is not quite a direct sum of subgroups.

Equation (4.1) is analogous to the decomposition $\mathbf{R} = \mathbf{Z} + [0,1)$. This analogy between the pair $(\mathbf{A_Q}, \mathbf{Q})$ and the pair $(\mathbf{R}, \mathbf{Z})$ can be carried further. For example, if we define $\widehat{\mathbf{Z}}$ to be the character group of $\mathbf{Z}$, then $\widehat{\mathbf{Z}} \cong S^1$ (associate to $z \in S^1$ the element of $\widehat{\mathbf{Z}}$ given by $n \mapsto z^n$). The isomorphism $\widehat{\mathbf{Q}} \cong \mathbf{A_Q}/\mathbf{Q}$ should be thought of as analogous to the isomorphism $\widehat{\mathbf{Z}} \cong \mathbf{R}/\mathbf{Z}$.

Since $\Psi_{a+s} = \Psi_a$ if s is a rational adele, and for $a \in [0,1) \times \prod_p \mathbf{Z}_p$ the character Ψ_a is trivial precisely when $a = 0$, we have proven that the group homomorphism $\Psi\colon \mathbf{A_Q} \to \widehat{\mathbf{Q}}$ is surjective with kernel $\mathbf{Q}$, so every element of $\widehat{\mathbf{Q}}$ has the form Ψ_a for some $a \in \mathbf{A_Q}$, and two characters Ψ_a and Ψ_b are equal if and only if $a - b$ is a rational adele. This is our desired "concrete" desription of $\widehat{\mathbf{Q}}$. Using the completions of $\mathbf{Q}$ to define various explicit homomorphisms $\psi_\infty, \psi_2, \psi_3, \ldots$, we have shown how to "glue" them together using the adeles to get all the characters of $\mathbf{Q}$. To appreciate the choice of $e^{-2\pi i x}$ over $e^{2\pi i x}$ to play the role of the basic real character, we can work through the above argument with $e^{2\pi i x}$. This leads to the homomorphism $\Phi\colon \mathbf{A_Q} \to \widehat{\mathbf{Q}}$ given by

$$\Phi_a(r) = e^{2\pi i a_\infty r} \cdot \prod_p e^{2\pi i \{a_p r\}_p}.$$

It is surjective, like Ψ, but the kernel of Φ is the set of adeles of the form $(-r, r, r, \ldots)$ for rational r, which is not as elegant.

It is left as an exercise for anyone who is familiar with the adeles $\mathbf{A}_k$ of any finite extension field k of $\mathbf{Q}$ to extend our arguments and give an elementary proof that $\widehat{k} \cong \mathbf{A}_k/k$.

Appendix A. Characters of $\mathbf{R}$ and $\mathbf{Q}_p$

Here we shall prove that all continuous homomorphisms $\mathbf{R} \to S^1$ have the form

$$x \mapsto e^{2\pi i x y}$$

for a unique real number y, and all continuous homomorphisms $\mathbf{Q}_p \to S^1$ have the form

$$x \mapsto e^{2\pi i \{xy\}_p}$$

for a unique p-adic number y. The similarity in these descriptions suggests the possibility of having a common proof for these results. Using some general theorems about locally compact abelian groups, it is possible to prove these results in a unified (and rather brief) manner where the only property one uses about $\mathbf{R}$ and $\mathbf{Q}_p$ is that they are locally compact fields with respect to nontrivial absolute values (see [4, Lemma 2.2.1]). However, we take a more elementary path. While we handle the real and p-adic cases separately, there are some basic similarities in the two proofs.

First let's make some general remarks. The above maps certainly are examples of continuous homomorphisms. If $y \neq 0$ in the real case, then evaluating the map at $x = 1/2y$ shows the homomorphism is not trivial, while an evaluation at $x = 1/py$ for nonzero y in the p-adic case shows the homomorphism is not trivial. It follows easily from this that such homomorphisms are uniquely determined by the scaling factor y, so we only need to show every continuous homomorphism has the indicated form. A common step in both cases will be to show that any homomorphism has nontrivial kernel, and then reduce to the case where 1 lies in the kernel. The proof that the kernel is nontrivial will operate on different principles in the two cases (real vs. p-adic), taking into account special features of the topology of $\mathbf{R}$ and $\mathbf{Q}_p$.

Since the p-adic case is easier to handle and may be less familiar to the reader, we present it first. If $\chi\colon \mathbf{Q}_p \to S^1$ is a continuous homomorphism, then for all small x in $\mathbf{Q}_p$, $|\chi(x) - 1| < 1$. In particular, χ sends $p^N\mathbf{Z}_p$ into $\{z \in \mathbf{C}^\times : |z-1| < 1\}$ for large enough N. Since $p^N\mathbf{Z}_p$ is a group, $\chi(p^N\mathbf{Z}_p)$ is a subgroup of $\mathbf{C}^\times$. Clearly there are no nontrivial subgroups of $\mathbf{C}^\times$ entirely within the open ball of radius 1 around 1 in $\mathbf{C}^\times$. Thus $\chi(p^N\mathbf{Z}_p) = \{1\}$, so χ is locally constant and $\chi(p^N) = 1$. Let $\psi(x) = \chi(p^N x)$ for all $x \in \mathbf{Q}_p$, so ψ is a continuous homomorphism $\mathbf{Q}_p \to S^1$ which is trivial on $\mathbf{Z}_p$, in particular $\psi(1) = 1$. Thus $\psi(1/p^n)$ is a p^n-th root of unity, so $\psi(1/p^n) = e^{2\pi i c_n/p^n}$

for some integer c_n with $0 \leq c_n \leq p^n - 1$. Proceeding exactly as in §4, we find that the integers c_n form a Cauchy sequence in $\mathbf{Z}_p$, and their limit c satisfies $\psi(r) = e^{2\pi i\{rc\}_p}$ for all $r \in \mathbf{Q}$, so by continuity $\psi(x) = e^{2\pi i\{xc\}_p}$ for all $x \in \mathbf{Q}_p$. Thus $\chi(x) = \psi(x/p^N) = e^{2\pi i\{xy\}_p}$ for $y = c/p^N$. For a slightly different argument, see [5].

We never used the hypothesis that the image of χ is a subset of S^1, only that it is a subset of $\mathbf{C}^\times$; we proved its image has to lie in S^1. The essential point is that subgroups of $\mathbf{Q}_p$ and $\mathbf{C}^\times$ are quite different. In $\mathbf{Q}_p$, the identity 0 has a neighborhood basis of subgroups ($p^n\mathbf{Z}_p$ for $n \geq 0$), while in $\mathbf{C}^\times$, the identity 1 has a neighborhood containing no nontrivial group.

It is possible to establish the real case rather quickly, using integrals (see [1, Theorem 9.11]). However, the basic structure of the p-adic case can be carried over to the real case, and we now present this alternate (but longer) argument.

Let $\chi\colon \mathbf{R} \to S^1$ be a continuous homomorphism. We want to show $\chi(x) = e^{2\pi ixy}$ for some $y \in \mathbf{R}$. We may assume χ is nontrivial. If the kernel of χ contains nonzero numbers arbitrarily close to 0, then by translations the kernel of χ is dense in $\mathbf{R}$, so by continuity χ is trivial. Thus, for nontrivial χ and all small $x > 0$, $\chi(x)$ has constant sign on its imaginary part. Replacing χ with χ^{-1} if necessary, we may assume that χ has positive imaginary part on small positive numbers.

Since $\chi(t) \neq 1$ for some $t > 0$, by connectedness $\chi((0,t))$ is an arc in S^1, so contains a root of unity, say $\chi(u)$ for $0 < u < t$. If $\chi(u)$ has order N, then $Nu > 0$ is in the kernel of χ. Replacing χ by the continuous homomorphism $x \mapsto \chi(Nux)$, we may assume that $\chi(1) = 1$. To summarize, we may assume χ is a continuous homomorphism from $\mathbf{R}$ to S^1 which contains 1 in its kernel and which has positive imaginary part for small positive numbers. According to what we are trying to prove, we now expect that $\chi(x) = e^{2\pi ixy}$ for some (positive) *integer* y, and this is what we shall show.

Since the reciprocals of the prime powers generate the dense subgroup $\mathbf{Q}$ of $\mathbf{R}$, by continuity it suffices to find an integer y such that $\chi(1/p^n) = e^{2\pi iy/p^n}$ for all primes p and integers $n \geq 1$. Actually, we'll show for any integer $m > 1$ that there is an integer y_m such that $\chi(1/m^n) = e^{2\pi iy_m/m^n}$ for all $n \geq 1$. Since $\chi(1/(pq)^n)^{p^n} = \chi(1/q^n)$ and $\chi(1/(pq)^n)^{q^n} = \chi(1/p^n)$, it follows that $y_{pq} - y_q \in \cap_n q^n\mathbf{Z} = \{0\}$, so $y_{pq} = y_q$, and similarly that $y_{pq} = y_p$, so $y_p = y_q$. Thus for all primes p, the integers y_p are the same, and this common integer y solves our problem.

Since $\chi(1/m^n)^{m^n} = \chi(1) = 1$,

$$\chi(1/m^n) = e^{2\pi i c_n/m^n}$$

for some integer c_n such that $0 \leq c_n < m^n$. Note c_n depends on m (well, a priori at least). Since

$$\chi(1/m^{n+1})^m = \chi(1/m^n),$$

$c_{n+1}/m^n - c_n/m^n \in \mathbf{Z}$. For large n, contintuity of χ implies $\cos(2\pi c_n/m^n) > 0$ and $\sin(2\pi c_n/m^n)$ is positive and arbitrarily small. Since $0 \leq c_n < m^n$, the cosine condition implies $c_n/m^n \in (0, 1/4) \cup (3/4, 1)$ for large n. We can't have c_n/m^n in $(3/4, 1)$ for large n, since then $\sin(2\pi c_n/m^n)$ is negative (here is where we use the assumption that $\chi(x)$ is in the first quadrant for small positive x). Thus for all large n, $c_n/m^n \in (0, 1/4)$. Since $\sin(2\pi c_n/m^n)$ is arbitrarily small for all large n, it follows by the nature of the sine function and the location of c_n/m^n that c_n/m^n is arbitrarily small for n large. To fix ideas, $0 < c_n/m^n < 1/(m+1)$ for all large n. Then $0 < c_{n+1}/m^n < m/(m+1)$ for all large n, so $|c_n/m^n - c_{n+1}/m^n| < 1$ for all large n. Since the left hand side of this last inequality is an integer, it must be zero, so all c_n's are equal for n sufficiently large. Call this common value y_m. Thus $\chi(1/m^n) = e^{2\pi i y_m/m^n}$ for all large n, hence for all $n \geq 1$; for example, if $\chi(1/m^{100}) = e^{2\pi i y_m/m^{100}}$, then raising both sides to the m^{98}-th power we see that $\chi(1/m^2) = e^{2\pi i y_m/m^2}$.

Acknowledgments. I thank Randy Scott, Eric Sommers and Ravi Vakil for looking over a preliminary version of this manuscript.

References

[1] J.B. Conway, "A Course in Functional Analysis," 2nd ed., Springer-Verlag, New York, 1990.

[2] I. M. Gel'fand, M. I. Graev, I. I. Pyatetskii-Shapiro, "Representation Theory and Automorphic Functions," Academic Press, 1990.

[3] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer-Verlag, New York, 1986.

[4] J. Tate, *Fourier Analysis in Number Fields and Hecke's Zeta-Functions*, in: "Algebraic Number Theory," Academic Press, New York, 1967, 305-347.

[5] L. Washington, *On the Self-Duality of* $\mathbf{Q}_p$, American Mathematical Monthly **81** (4) 1974, 369-370.