ARITHMETIC FROM AN ADVANCED PERSPECTIVE: AN INTRODUCTION TO THE ADÈLES

Edward B. Burger[1]

May, 2010

Abstract

Here we offer an introduction to the adèle ring over the field of rational numbers $\mathbb{Q}$ and highlight some of its beautiful algebraic and topological structure. We then apply this rich structure to revisit some ancient results of number theory and place them within this modern context as well as make some new observations. We conclude by indicating how this theory enables us to extend the basic arithmetic of $\mathbb{Q}$ to the more subtle, complicated, and interesting setting of an arbitrary number field.

2010 Mathematics Subject Classification: 11R56, 11F85, 11H06.

Keywords: *Adèle ring, Nonarchimedean analysis, p-adic numbers*

1. *Department of Mathematics, Williams College, USA.*

A Disparate Yet Connected World of Arithmetic

In this paper we outline a modern approach to arithmetic that begins with Kurt Hensel's discovery of p-adic analysis in the late 1800s (here p is a fixed prime number). Years later, Claude Chevalley and many others saw how to simultaneously study all these p-adic worlds at once and that investigation led to the adèles. This pioneering work brought algebraic, analytic, and topological ideas together in order to better understand the nuance of number. Thus, beyond the important number theoretic implications of this effort, it also provides a beautiful illustration of the interconnections between the three basic pillars of pure mathematics.

We adopt standard mathematical notation; in particular, we write $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ for the set of integers, rational, real, and complex numbers, respectively. The bibliography offers a number of references for further reading and research. This work grew out of my lecture notes from a special weekly evening number theory seminar I ran for interested students and faculty.

I wish to acknowledge the referee who read this manuscript with great care and made a number of fine suggestions. Finally, I thank my colleague Professor Cesar E. Silva for the invitation and encouragement to write this article as well as for his friendship during my 20 years at Williams College.

Contents

1 An Introduction to the Theory of Valuations

Let k be a field. A map $|\ |: k \to [0, +\infty)$ is called a *valuation* or an *absolute value* if the following three **conditions** are statisfied:

1) $|x| = 0$ if and only if $x = 0$.

2) For all $x, y \in k$, $|xy| = |x|\,|y|$.

3) The *triangle inequality* holds: For all $x, y \in k$,

$$|x + y| \leq |x| + |y| \ .$$

If $k^* = k \setminus \{0\}$ is the multiplicative group of nonzero elements of k and $|\ |$ is a valuation on k, then, by condition 2), the map

$$|\ |: k^* \to \Big\{(0, +\infty),\ \cdot\ \Big\}$$

is a homomorphism of multiplicative groups. Hence it immediately follows that

(i) $|1| = 1$.

(ii) If $\xi^n = 1$ for some $\xi \in k$ and nonzero integer n, then $|\xi| = 1$.

(iii) $|-1| = 1$, $|-x| = |x|$ and $|x^m| = |x|^m$ for all $x \in k$ and $m \in \mathbb{Z}$.

If we let $d : k \times k \to [0, +\infty)$ be defined by

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

then conditions 1), 2), and 3) imply that d is a metric on k. Let $|\ |_1$ and $|\ |_2$ be two absolute values on k, and let $\mathcal{T}_1$ and $\mathcal{T}_2$ be the topologies on k induced by the metrics associated with $|\ |_1$ and $|\ |_2$, respectively. That is, $\mathcal{T}_i$ is the collection of all open sets in k determined by the metric $d_i(x, y) = |x - y|_i$ for $i = 1$ and 2. We say that the two absolute values $|\ |_1$ and $|\ |_2$ are *equal* if $|x|_1 = |x|_2$ for all $x \in k$. We say that $|\ |_1$ and $|\ |_2$ are *equivalent* if $\mathcal{T}_1 = \mathcal{T}_2$, that is, if they generate the same topology on k.

We define the map $|\ |_0 : k \to [0, +\infty)$ as follows: $|0|_0 = 0$ and for all $x \in k$, $x \neq 0$, $|x|_0 = 1$. It is easy to verify that $|\ |_0$ is a valuation on k. This map is known as the *trivial absolute value* and although it may not

appear to be very interesting, it does illustrate that given any field k, the set of absolute values on k is never empty. A more important challenge remains: Given a field k, classify *all* (up to equivalence) absolute values on k. We will return to this question in Sections 2 and 8.

We recall that the *discrete topology* on a set X is the topology in which each element of X is an open set; that is, $\{x\}$ is an open set for all $x \in X$. Our first proposition offers a necessary and sufficient condition for an absolute value on k to generate the discrete metric topology.

Proposition 1.1. *The absolute value* $|\ |$ *on the field* k *induces the discrete topology on* k *if and only if* $|\ | = |\ |_0$.

Proof. For any $\alpha \in k$, we note that the open set $\{x \in k : |x - \alpha|_0 < 1\}$ equals $\{\alpha\}$. Thus $|\ |_0$ generates the discrete topology on k. Conversely, suppose that $|\ |$ generates the discrete topology on k and further assume that it is not the trivial absolute value. Since $|\ |$ is not the trivial absolute value on k, there must exist an element $\alpha \in k$ such that $|\alpha| \neq 0$ and $|\alpha| \neq 1$. By replacing α by α^{-1}, if necessary, we may assume without loss of generality that $0 < |\alpha| < 1$. Therefore

$$\lim_{n \to \infty} |\alpha^n - 0| = \lim_{n \to \infty} |\alpha|^n = 0 \ .$$

That is, $\{\alpha^n\}_{n=1}^{\infty}$ is a sequence of nonzero elements of k converging to 0 with respect to $|\ |$. Thus any open set containing 0 must also contain an element of this sequence. However, since the topology is discrete, $\{0\}$ is an open set containing 0, but clearly does not contain any element of our nonzero sequence. This contradiction implies that $|\ | = |\ |_0$. □

Moving beyond the trivial absolute value, the example with which we are most familiar is $k = \mathbb{R}$, with $|\ |$ as the usual Euclidean absolute value. If we consider the field of complex numbers $\mathbb{C}$, then the map defined by

$$|u + iv| = \sqrt{u^2 + v^2}$$

is an absolute value on $\mathbb{C}$ that when restricted to $\mathbb{R}$ produces the familiar Euclidean absolute value. Thus the absolute value on $\mathbb{C}$ extends the Euclidean absolute value of $\mathbb{R}$.

Let x be a variable and define the *field of rational functions in* x, denoted by $\mathbb{Q}(x)$, to be the field of all $p(x)/q(x)$ in which both $p(x)$ and $q(x)$ are polynomials having rational coefficients with $q(x)$ not identically 0. For a fixed transcendental number T, we define $|\ |_T$ on $\mathbb{Q}(x)$ by

$$\left|\frac{p(x)}{q(x)}\right|_T = \left|\frac{p(T)}{q(T)}\right| ,$$

where $|\ |$ is the usual absolute value on $\mathbb{C}$. It is easy to verify that $|\ |_T$ is an absolute value on $\mathbb{Q}(x)$. A more interesting map on $\mathbb{Q}(x)$, $|\ |_{\deg}$, is given by:

$$\left|\frac{p(x)}{q(x)}\right|_{\deg} = e^{\deg(p(x))-\deg(q(x))} ,$$

where $e = 2.718281\ldots$ and $\deg(p(x))$ is the degree of the polynomial $p(x)$, with $\deg(0)$ defined to be $-\infty$ (and, of course, $e^{-\infty}$ is defined to be 0).

Theorem 1.2. *The map* $|\ |_{deg}$ *is an absolute value on the field* $\mathbb{Q}(x)$.

Proof. We first establish that this map is well-defined. For any nonzero polynomial $r(x)$, we observe that

$$\begin{aligned}\left|\frac{p(x)r(x)}{q(x)r(x)}\right|_{\deg} &= e^{\deg(pr)-\deg(qr)} \\ &= e^{\deg(p)+\deg(r)-\deg(q)-\deg(r)} \\ &= e^{\deg(p)-\deg(q)} = \left|\frac{p(x)}{q(x)}\right|_{\deg} ,\end{aligned}$$

which shows that $|\ |_{\deg}$ is indeed well-defined.

Clearly the map $|\ |_{\deg}$ takes on values from the set of nonnegative real numbers and $|p(x)/q(x)|_{\deg} = 0$ if and only if $p(x)/q(x)$ is the constant function 0. Next we compute

$$\begin{aligned}
\left|\frac{p_1(x)}{q_1(x)}\frac{p_2(x)}{q_2(x)}\right|_{\deg} &= e^{\deg(p_1p_2)-\deg(q_1q_2)} \\
&= e^{\deg(p_1)-\deg v(q_1)+\deg(p_2)-\deg(q_2)} \\
&= e^{\deg(p_1)-\deg(q_1)}\ e^{\deg(p_2)-\deg(q_2)} \\
&= \left|\frac{p_1(x)}{q_1(x)}\right|_{\deg}\left|\frac{p_2(x)}{q_2(x)}\right|_{\deg},
\end{aligned}$$

thus condition 2) is satisfied for this function.

Finally we establish condition 3), the triangle inequality, holds for $|\ |_{\deg}$. We abbreviate our notation and write p for the polynomial $p(x)$. Let p_1/q_1 and p_2/q_2 be two elements of $\mathbb{Q}(x)$. Without loss of generality we may assume that

$$|p_1/q_1|_{\deg} \leq |p_2/q_2|_{\deg}\ .$$

That is, $\deg(p_1)-\deg(q_1) \leq \deg(p_2)-\deg(q_2)$, or equivalently,

$$\deg(p_1) + \deg(q_2) \leq \deg(p_2) + \deg(q_1)\ . \tag{1.1}$$

From basic polynomial arithmetic we recall that

$$\deg(p_1+p_2) \leq \max\{\deg(p_1), \deg(p_2)\} \text{ and } \deg(p_1p_2) = \deg(p_1)+\deg(p_2)\ .$$

This observation along with inequality (1.1) yields

$$\begin{aligned}
\left|\frac{p_1}{q_1}+\frac{p_2}{q_2}\right|_{\deg} &= \left|\frac{p_1q_2+p_2q_1}{q_1q_2}\right|_{\deg} \\
&= e^{\deg(p_1q_2+p_2q_1)-\deg(q_1q_2)} \\
&\leq e^{max\{\deg(p_1q_2),\deg(p_2q_1)\}-\deg(q_1q_2)}
\end{aligned}$$

$$\begin{aligned} &= e^{\deg(p_2)+\deg(q_1)-\deg(q_1)-\deg(q_2)} \\ &= e^{\deg(p_2)-\deg(q_2)} = |p_2/q_2|_{\deg} \\ &= \max\{|p_1/q_1|_{\deg}, |p_2/q_2|_{\deg}\} \\ &\leq \left|\frac{p_1}{q_1}\right|_{\deg} + \left|\frac{p_2}{q_2}\right|_{\deg} . \end{aligned}$$

Hence the map $|\ |_{\deg}$ is an absolute value on $\mathbb{Q}(x)$. □

In our previous proof of the triangle inequality we actually proved a stronger inequality. Instead of condition 3) we proved:

3′) The *strong triangle inequality*: for all $x, y \in k$,

$$|x+y| \leq \max\{|x|, |y|\} .$$

Clearly condition 3′) implies condition 3). If an absolute value satisfies condition 3′), then it is called a *nonarchimedean absolute value*. If an absolute value does not satisfy condition 3′), then it is called an *archimedean absolute value*. The usual Euclidean absolute value on $\mathbb{R}$ is an archimedean absolute value since, for example, $|1+3| \not\leq \max\{|1|, |3|\}$. On the other hand, the trivial absolute value on a field k is always nonarchimedean. As we have just seen, $|\ |_{\deg}$ is a nontrivial example of a nonarchimedean absolute value on $\mathbb{Q}(x)$.

We now investigate algebraic properties of nonarchimedean valuations. Again, let k be a field and let $|\ |$ be a nonarchimedean absolute value on k. We define the subsets $\mathcal{O} = \mathcal{O}(k, |\ |)$ and $\mathcal{P} = \mathcal{P}(k, |\ |)$ by

$$\mathcal{O} = \{x \in k : |x| \leq 1\} \quad \text{and} \quad \mathcal{P} = \{x \in k : |x| < 1\} .$$

Theorem 1.3. *The set $\mathcal{O}$ is a ring and $\mathcal{P}$ is the unique maximal ideal in $\mathcal{O}$.*

Proof. Suppose that x and y are elements of $\mathcal{O}$. Then by conditions 2) and 3′), we have that

$$|xy| = |x||y| \leq 1 \quad \text{and} \quad |x+y| \leq \max\{|x|, |y|\} \leq 1 .$$

Thus, $xy \in \mathcal{O}$ and $x+y \in \mathcal{O}$. Of course $|-x| = |x| \leq 1$, so we have that $-x \in \mathcal{O}$ and therefore $\mathcal{O}$ is a ring.

Again by the strong triangle inequality we have that $(\mathcal{P}, +)$ is an additive subgroup of $\mathcal{O}$. Also if $p \in \mathcal{P}$ and $z \in \mathcal{O}$ are arbitrary elements, then $|zp| = |z||p| \leq |p| < 1$. Hence $\mathcal{P}$ is an ideal of $\mathcal{O}$. Moreover, we note that for any $x \in \mathcal{O} \setminus \mathcal{P}$, we have $|x| = 1$. Thus it follows that $|1/x| = 1$; that is, $\mathcal{O} \setminus \mathcal{P}$ is precisely the set of units in $\mathcal{O}$. To show that $\mathcal{P}$ is maximal, suppose that M, $M \neq \mathcal{P}$, is an ideal of $\mathcal{O}$ with $\mathcal{P} \subset M$. Let m be an element of $M \setminus \mathcal{P}$. As m is a unit, then it follows that the ideal $M = \mathcal{O}$; therefore $\mathcal{P}$ is a maximal ideal.

Finally we establish that $\mathcal{P}$ is the *unique* maximal ideal in $\mathcal{O}$. Suppose that $\mathcal{P}_1$ is another maximal ideal of $\mathcal{O}$ with $\mathcal{P}_1 \neq \mathcal{P}$. Then there must exist an element $w \in \mathcal{P}_1 \subseteq \mathcal{O}$ with $w \notin \mathcal{P}$. Thus, we have that w is a unit the ideal $\mathcal{P}_1$; hence $\mathcal{P}_1 = \mathcal{O}$. However we assumed that $\mathcal{P}_1$ was also maximal, which implies that $\mathcal{P}_1 \neq \mathcal{O}$. Hence $\mathcal{P}_1$ cannot exist; that is, $\mathcal{P}$ is the unique maximal ideal in $\mathcal{O}$. □

The set $\mathcal{O}$ is called the *ring of integers of k with respect to* $|\ |$. As $\mathcal{P}$ is maximal, it follows that the ring $\mathcal{O}/\mathcal{P}$ is a field, known as the *residue class field of k with respect to* $|\ |$. As we will see in the sequel, these algebraic objects are central to the development of advanced arithmetic.

We close this discussion with an important albeit strange observation about nonarchimedean valuations: If $|x| \neq |y|$, then there is always *equality* in the strong triangle inequality.

Theorem 1.4. *Let k be a field and $|\ |$ a nonarchimedean absolute value on k. If x and y are elements of k with $|x| \neq |y|$, then*

$$|x+y| = \max\{|x|, |y|\} \ .$$

Proof. Since $|x| \neq |y|$, without loss of generality we may assume that $|x| < |y|$ and thus $\max\{|x|, |y|\} = |y|$. By the strong triangle inequality we have that $|x+y| \leq \max\{|x|, |y|\}$. We now assume that

$|x+y| < \max\{|x|, |y|\}$; that is, $|x+y| < |y|$. By another application of the strong triangle inequality we discover that

$$\begin{aligned} |y| &= |x+y-x| \\ &\leq \max\{|x+y|, |-x|\} = \max\{|x+y|, |x|\} \\ &< |y| \ , \end{aligned}$$

which is plainly impossible. Therefore we conclude that

$$|x+y| = \max\{|x|, |y|\} \ ,$$

as desired. □

An amusing and surprisingly useful corollary to Theorem 1.4 is the fact that all triangles formed by three elements of k, whose side lengths are measured with the nonarchimedean absolute value $|\ |$, are *isosceles.*

Corollary 1.5. *Any triangle having its vertices given by three points of k is an isosceles triangle with respect to the nonarchimedean absolute value $|\ |$.*

Proof. Let x, y, and z be elements in k. Then the lengths of the sides of the triangle having x, y, and z as its vertices are given by $|x-y|, |y-z|$, and $|x-z|$. Now if $|x-y| = |y-z|$, then the triangle would be isosceles. We now assume that $|x-y| \neq |y-z|$. Thus from Theorem 1.4, there is equality in the strong triangle inequality and therefore

$$|x-z| = |(x-y)+(y-z)| = \max\{|x-y|, |y-z|\} \ .$$

Hence the side length of $|x-z|$ *equals* the greater of the lengths of the other two sides and so the triangle is indeed isosceles as claimed. □

We consider one last peculiar but important consequence of Theorem 1.4. For a fixed element $a \in k$ and $r \in \mathbb{R}$, $r > 0$, we define the *open ball of radius r centered about a* by

$$B(a, r) = \{x \in k : |x-a| < r\} \ .$$

Now let $b \in k$ be any other element in $B(a,r)$, that is, $b \in B(a,r)$. If $|\ |$ is a nonarchimedean absolute value on k, then it can be shown that

$$B(a,r) = B(b,r) \ .$$

That is, *every point in an open disk is the center of that open disk.* The proof of this strange assertion closely parallels the argument of Corollary 1.5 and is left as an instructive exercise for the reader.

2 Nonarchimedean Spaces and Basic p-adic Analysis

By the Fundamental Theorem of Arithmetic, every integer greater than 1 can be factored uniquely as a finite product of prime numbers (up to the order of the factors). Thus given a nonzero integer n, $n \neq 1$, we may express it uniquely as

$$n = \pm p_1^{t_1} p_2^{t_2} \cdots p_L^{t_L} \ ,$$

in which each p_l is a distinct prime number and t_l is a positive integer. This unique prime factorization extends to nonzero rational numbers r, $r \neq 1$, as

$$r = \pm p_1^{u_1} p_2^{u_2} \cdots p_M^{u_M} \ ,$$

where now the u_m's are nonzero *integers.* For example,

$$\frac{140}{297} = 2^2 \times 3^{-3} \times 5 \times 7 \times 11^{-1} \ .$$

Let p be a fixed prime number. We can always include this special prime p in the factorization of any such r as follows: If p does not already occur in the factorization of r, then we can express the factorization with our superfluous factor as:

$$r = \pm p^0 p_1^{u_1} p_2^{u_2} \cdots p_M^{u_M} \ .$$

Given the fixed prime p, this new factorization is also unique. We now define a map $|\ |_p : \mathbb{Q} \to [0, +\infty)$ as follows: $|0|_p = 0$, and for $r \in \mathbb{Q}$, $r \neq 0$,

$$|r|_p = p^{-t} ,$$

where t is the power of p occurring in this new factorization of r.
Examples. $|140/297|_3 = 3^3$, $|140/297|_2 = 1/2^2$, and $|140/297|_{23} = 1$.

We now discover that this peculiar prime reciprocal function possesses incredible structure.

Theorem 2.1. *Let p be a fixed prime number and let $|\ |_p : \mathbb{Q} \to [0, +\infty)$ be the map defined above. Then $|\ |_p$ is a nonarchimedean absolute value on $\mathbb{Q}$.*

The absolute value $|\ |_p$ is called the *p-adic absolute value.*

Proof. Clearly we have that $|x|_p \geq 0$ for all $x \in \mathbb{Q}$ and that $|x|_p = 0$ if and only if $x = 0$. Given arbitrary nonzero rational numbers x and y, we express them as:

$$x = p^t \frac{r_1}{s_1} \quad \text{and} \quad y = p^u \frac{r_2}{s_2} ,$$

where t and u are integers, and r_1, s_1, r_2, s_2 are integers each relatively prime to p. Thus we have

$$\begin{aligned} |xy|_p &= \left|p^{t+u}(r_1 r_2)/(s_1 s_2)\right|_p \\ &= \left|p^{t+u}\right|_p = p^{-(t+u)} \\ &= p^{-t} p^{-u} = |x|_p \, |y|_p \ . \end{aligned}$$

Hence for all rational x and y, $|xy|_p = |x|_p |y|_p$. It remains for us to establish the strong triangle inequality. Without loss of generality we may assume that $t \leq u$ so we have that $u - t$ is a nonnegative integer,

$|y|_p \leq |x|_p$, and $r_1 s_2 + p^{u-t} r_2 s_1$ is an integer. Hence

$$\begin{aligned} |x+y|_p &= \left| p^t \left(\frac{r_1}{s_1} + p^{u-t} \frac{r_2}{s_2} \right) \right|_p \\ &= |x|_p \left| \frac{r_1 s_2 + p^{u-t} r_2 s_1}{s_1 s_2} \right|_p \\ &= \max\{|x|_p, |y|_p\} \left| r_1 s_2 + p^{u-t} r_2 s_1 \right|_p \\ &\leq \max\{|x|_p, |y|_p\} , \end{aligned}$$

and therefore $|\ |_p$ is a nonarchimedean absolute value on $\mathbb{Q}$. □

In this context we have that

$$\mathcal{O} = \{x \in \mathbb{Q} : |x|_p \leq 1\} \quad \text{and} \quad \mathcal{P} = \{x \in \mathbb{Q} : |x|_p < 1\} ,$$

where, by Theorem 1.3, $\mathcal{O}$ is a ring and $\mathcal{P}$ the unique maximal ideal in $\mathcal{O}$. Here the residue class field, $\mathcal{O}/\mathcal{P}$, is isomorphic to the finite field of order p; that is, $\mathbb{Z}/p\mathbb{Z}$. To establish this assertion we first observe that, in view of unique factorization, $\mathcal{O}$ and $\mathcal{P}$ can be defined alternatively, but equivalently, as

$$\begin{aligned} \mathcal{O} &= \{x = r/s \in \mathbb{Q} : \gcd(r,s) = 1 \text{ and } \gcd(s,p) = 1\} \text{ and} \\ \mathcal{P} &= \{x = r/s \in \mathbb{Q} : \gcd(r,s) = 1 \text{ and } \gcd(r,p) > 1\} . \end{aligned}$$

It follows that for any $r/s \in \mathcal{O}$, the denominator s is not congruent to 0 modulo p and thus has a multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$, say s^{-1}. Let $t = t(r/s)$ be the element of $\mathbb{Z}/p\mathbb{Z}$ that is congruent to rs^{-1} modulo p. Then one can verify that the map $\eta : \mathcal{O}/\mathcal{P} \to \mathbb{Z}/p\mathbb{Z}$ defined by:

$$\eta(x + \mathcal{P}) = t(x) \bmod p$$

is a well-defined function and moreover is an isomorphism of fields. Thus from now on, we will represent $\mathcal{O}/\mathcal{P}$ as $\{0, 1, 2, \ldots, p-1\}$.

We now introduce some basic p-adic analysis. Suppose that $\{a_n\}_{n=T}^{\infty}$ is an infinite sequence of elements from $\mathcal{O}/\mathcal{P}$ (here we will allow T to

be an arbitrary *integer*). It is easy to see that $|a_n|_p$ equals either 0 or 1, depending upon whether $a_n = 0$ or $a_n \neq 0$, respectively. Let us now consider the following infinite sequence of rational numbers:

$$\left\{ \sum_{n=T}^{N} a_n p^n \right\}_{N=T}^{\infty} . \tag{2.1}$$

Note that by the strong triangle inequality, for $M > L$,

$$\left| \sum_{n=T}^{M} a_n p^n - \sum_{n=T}^{L} a_n p^n \right|_p$$

$$\leq \max \left\{ \left| a_{L+1} p^{L+1} \right|_p , \left| a_{L+2} p^{L+2} \right|_p , \ldots , \left| a_M p^M \right|_p \right\} = p^{-L-1} .$$

In view of this observation, one can establish that the sequence in (2.1) is a Cauchy sequence in $\mathbb{Q}$ with respect to the metric topology generated by the p-adic absolute value. Moreover, every Cauchy sequence in $\mathbb{Q}$ with respect to the p-adic absolute value can be expressed as a sequence of partial sums as above with a suitable choice of the coefficients $\{a_n\}_{n=T}^{\infty} \subseteq \mathcal{O}/\mathcal{P}$. Thus, in some sense, we can describe the general shape of all Cauchy sequences in this context.

If the sequence in (2.1) converges to a number $\alpha \in \mathbb{Q}$, then we write

$$\sum_{n=T}^{\infty} a_n p^n = \alpha ;$$

which leads to the question: Which of these Cauchy sequences converge in $\mathbb{Q}$? The answer, whose proof we do not include here, is analogous to its Euclidean (archimedean) counterpart. In fact, we could view this answer as its *arithmetical* analogue.

Theorem 2.2. *Let p be a fixed prime number. Then the infinite series*

$$\sum_{n=T}^{\infty} a_n p^n ,$$

where $a_n \in \mathcal{O}/\mathcal{P}$, converges to a rational number with respect to the p-adic absolute value if and only if the infinite sequence $\{a_n\}_{n=T}^{\infty}$ is eventually periodic.

Example. Evaluate $\sum_{n=0}^{\infty} 3^{2n}$ with respect to the 3-adic metric. If we write s for this sum then we have:

$$\begin{aligned} s &= 1 + 3^2 + 3^4 + 3^6 + \cdots \text{ and} \\ 3^2 s &= \quad 3^2 + 3^4 + 3^6 + \cdots . \end{aligned}$$

If we subtract these two identities, then we find $(1 - 3^2)s = 1$, and therefore discover that $s = -1/8$.

Exercise. Find an infinite series that converges to a *positive* rational number with respect to the 3-adic absolute value.

In view of Theorem 2.2, we see that not all Cauchy sequences in $\mathbb{Q}$ with respect to the p-adic absolute value converge in $\mathbb{Q}$. To construct such a non-convergent Cauchy sequence, we need only select a sequence $\{a_n\}_{n=T}^{\infty}$ that is not periodic. Thus $\mathbb{Q}$ is not a *complete* metric space with respect to the p-adic metric (the metric given by $d(x, y) = |x - y|_p$). We now define the set $\mathbb{Q}_p$ to be the *completion of* $\mathbb{Q}$ *with respect to the metric induced by the p-adic absolute value.* That is, $\mathbb{Q}_p$ is the smallest field that contains $\mathbb{Q}$ and for which every p-adic Cauchy sequence converges. The set $\mathbb{Q}_p$ is called the *field of p-adic numbers.* As we will discover in Section 3, every element of $\mathbb{Q}_p$ can be expressed as an infinite series of the form

$$\sum_{n=T}^{\infty} a_n p^n , \tag{2.2}$$

where $a_n \in \{0, 1, \ldots, p-1\}$, and in view of Theorem 2.2, we see that (2.2) is the p-adic analogue of the decimal expansion of real numbers.

We define the sets $\mathbb{Z}_p$ and $p\mathbb{Z}_p$ by

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

and

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\} .$$

It is clear that $\mathcal{O}$ is a subset of $\mathbb{Z}_p$ and $\mathcal{P}$ is a subset of $p\mathbb{Z}_p$. In fact, following the proof of Theorem 1.3 we have that $\mathbb{Z}_p$ is a ring and $p\mathbb{Z}_p$ is the unique maximal ideal contained in $\mathbb{Z}_p$. The ring $\mathbb{Z}_p$ is called the *ring of p-adic integers.*

In order for us to include the Euclidean absolute value $|\ |$ on $\mathbb{Q}$ in our discussion of valuations, we adopt the following notation. We write $|\ |_\infty$ for the usual Euclidean absolute value on $\mathbb{Q}$ and $\mathcal{T}_\infty$ for the metric topology on $\mathbb{Q}$ generated by $|\ |_\infty$. Similarly, for a prime p we write $|\ |_p$ and $\mathcal{T}_p$ for the analogous p-adic objects. We note that $\mathbb{Q}_\infty$ is just another name for $\mathbb{R}$. We define the set $V_\mathbb{Q}$ by

$$V_\mathbb{Q} = \{\infty, 2, 3, 5, 7, 11, 13, \ldots\} .$$

We call $V_\mathbb{Q}$ the set of *places* of $\mathbb{Q}$. It is a straightforward, but worthwhile exercise to verify that for any two distinct elements q and p in $V_\mathbb{Q}$, $|\ |_p$ is *not equivalent* to $|\ |_q$. That is, $\mathcal{T}_p \neq \mathcal{T}_q$. It thus follows, perhaps not surprisingly, that $\mathbb{Q}_p \neq \mathbb{Q}_q$. Thus we have constructed a countably infinite collection of distinct absolute values on $\mathbb{Q}$. The following very important theorem of Alexander Ostrowski from 1934—whose proof we only sketch below—tells us that there are no other (non-equivalent) nontrivial absolute values on $\mathbb{Q}$.

Theorem 2.3. *Suppose that $\|\ \|$ is a nontrivial absolute value on $\mathbb{Q}$. Then $\|\ \|$ is equivalent to $|\ |_p$ for some $p \in V_\mathbb{Q}$.*

Outline of the proof. Let $\|\ \|$ be a nontrivial absolute value on $\mathbb{Q}$. We first claim that $\|\ \|$ is nonarchimedean if and only if $\|n\| \leq 1$ for all $n \in \mathbb{Z}$. To establish this assertion, we first note that if $\|\ \|$ is nonarchimedean, then for any $n \in \mathbb{Z}$ (without loss of generality, we assume that $n > 0$), we have

$$\|n\| = \|1 + 1 + \cdots + 1\| \leq \max\{\|1\|, \|1\|, \ldots, \|1\|\} = 1 .$$

Conversely, if we now assume that $\|n\| \leq 1$ for all $n \in \mathbb{Z}$, then for any integer $M \geq 1$ and any integer m, $0 \leq m \leq M$, we have $\left\|\binom{M}{m}\right\| \leq 1$. Thus it follows that for any $x, y \in \mathbb{Q}$,

$$\begin{aligned}
\|x+y\| &= \left\|(x+y)^M\right\|^{1/M} = \left\|\sum_{m=0}^{M} \binom{M}{m} x^m y^{M-m}\right\|^{1/M} \\
&\leq \left(\sum_{m=0}^{M} \left\|\binom{M}{m}\right\| \|x^m y^{M-m}\|\right)^{1/M} \\
&\leq \left((M+1)\max\{\|x\|, \|y\|\}^M\right)^{1/M} \\
&= (M+1)^{1/M} \max\{\|x\|, \|y\|\} \ .
\end{aligned}$$

If we now let $M \to \infty$, then the previous inequality shows that $\| \ \|$ is nonarchimedean, thus establishing our claim.

If $\| \ \|$ is archimedean, then we can find a positive integer n satisfying $\|n\| > 1$. We define the positive real number τ by $\|n\| = |n|_\infty^\tau$. Using base-n expansions and a "power trick" similar to the one in the previous paragraph, it can be shown that this special τ satisfies an even greater condition: For *any* rational number α, we have $\|\alpha\| = |\alpha|_\infty^\tau$. Given this identity, it follows that $\| \ \|$ is equivalent to $| \ |_\infty$.

If $\| \ \|$ is nonarchimedean, then we can find the smallest positive integer n satisfying $\|n\| < 1$. It can now be shown that n must be prime, which we will rename p. Using Corollary 1.5 and the Euclidean algorithm, one can craft an argument to deduce that for any rational number α, if $|\alpha|_p = p^{-t}$, then $\|\alpha\| = \|p\|^t$. This assertion allows us to show that $\| \ \|$ is equivalent to $| \ |_p$. □

Therefore (up to equivalence) the set of places $V_{\mathbb{Q}}$ corresponds to a *complete* list of distinct nontrivial absolute values on $\mathbb{Q}$. So any nontrivial

absolute value on $\mathbb{Q}$ is (essentially) either the usual Euclidean absolute value or a p-adic absolute value for some prime p.

Is it possible that all the absolute values on $\mathbb{Q}$ are somehow connected to each other?

A positive answer may initially appear hopeless since these absolute values are so apparently different and independent. However they *are* connected in the following simple but fundamentally deep and beautiful theorem, commonly known as the *product formula.* Recall that we denoted the trivial absolute value on a field by $|\ |_0$.

Theorem 2.4. (The Product Formula) *Let α be a rational number. Then*

$$\prod_{p \in V_{\mathbb{Q}}} |\alpha|_p = |\alpha|_0 \ .$$

That is, for $\alpha \neq 0$, $\prod_{p \in V_{\mathbb{Q}}} |\alpha|_p = 1$.

Remark. Upon first inspection, it appears that the above product is an infinite product and thus issues of convergence need to be considered. However we recall that α has only finitely many prime factors. Thus for any prime p that is *not* a factor of α we have $|\alpha|_p = 1$. Therefore the product in Theorem 2.4 is only formally infinite and, in fact, is finite.

Proof of Theorem 2.4. If $\alpha = 0$, then the identity trivially holds. Thus we need only consider the case in which $\alpha \neq 0$ (and so $|\alpha|_0 = 1$). Without loss of generality we assume that $\alpha > 0$. We factor α into its unique finite product of distinct primes

$$\alpha = p_1^{n_1} p_2^{n_2} \cdots p_L^{n_L} \ ,$$

in which $n_l > 0$ is an integer for each l. Therefore we have

$$\begin{aligned}\prod_{p \in V_{\mathbb{Q}}} |\alpha|_p &= |\alpha|_\infty \prod_{p \text{ a prime}} |\alpha|_p \\ &= |\alpha|_\infty \prod_{l=1}^{L} |\alpha|_{p_l} = |\alpha|_\infty \prod_{l=1}^{L} p_l^{-n_l} \\ &= p_1^{n_1} p_2^{n_2} \cdots p_L^{n_L} p_1^{-n_1} p_2^{-n_2} \cdots p_L^{-n_L} \\ &= 1 = |\alpha|_0 \ .\end{aligned}$$

Thus the product formula holds for all rational α. □

Though the proof of this result is straightforward, the product formula is at the very heart of the subject. Notice that it illustrates, among other things, that if we know the value of $|\alpha|_p$ for each $p \in V_{\mathbb{Q}}$ except for one place, say q, then we automatically know $|\alpha|_q$. Also, in some sense, it is equivalent to the "fundamental principle of number theory"; namely that "there are no integers between 0 and 1." The product formula plays an important role in algebraic number theory and, as we will mention in Section 8, allows us to extend this fundamental principle to arbitrary number fields.

3 Topological Properties of $\mathbb{Q}_p$

Let p be a fixed prime and consider the infinite series

$$\sum_{n=0}^{\infty} a_n \ ,$$

where $a_n \in \mathbb{Q}_p$ for each n. It is easy to see that if this series converges in $\mathbb{Q}_p$, then

$$\lim_{n \to \infty} |a_n|_p = 0 \ .$$

Suppose now that we are given the infinite series and we wish to determine whether or not it converges in $\mathbb{Q}_p$. In the archimedean setting

(in $\mathbb{Q}_\infty = \mathbb{R}$) we recall from calculus that there are a variety of "tests" we emply in order to determine convergence. Here we show that in the nonarchimedean case, the situation is much simpler.

Theorem 3.1. *Let $\sum_{n=0}^{\infty} a_n$ be an infinite series with $a_n \in \mathbb{Q}_p$ for each n. Then the series converges in $\mathbb{Q}_p$ if and only if $\lim_{n\to\infty} |a_n|_p = 0$.*

Proof. If the series converges in $\mathbb{Q}_p$, then the terms must p-adically approach 0. Suppose now that

$$\lim_{n\to\infty} |a_n|_p = 0 \ .$$

Thus for any given $\varepsilon > 0$, there exists an index T such that for all $t \geq T$,

$$|a_t|_p < \varepsilon \ . \tag{3.1}$$

For $N \geq 0$, we write S_N for the Nth parial sum:

$$S_N = \sum_{n=0}^{N} a_n \ .$$

To establish that the series converges we need to show that the sequence of partial sums converges. Given that $\mathbb{Q}_p$ is a complete field, we need only show that $\{S_N\}_{N=0}^{\infty}$ is a Cauchy sequence in $\mathbb{Q}_p$. Suppose that $M > N \geq T$. Then by the strong triangle inequality and (3.1) we have

$$\begin{aligned} |S_M - S_N|_p &= |a_{N+1} + a_{N+2} + \cdots + a_M|_p \\ &\leq \max\{|a_{N+1}|_p, |a_{N+2}|_p, \ldots, |a_M|_p\} < \varepsilon \ . \end{aligned}$$

Hence the sequence of partial sums is a Cauchy and therefore the corresponding infinite series converges in $\mathbb{Q}_p$. □

Of course Theorem 3.1 is false in the archimedean case. Thus although we can transcribe all the results from real analysis to the p-adic setting, we see that sometimes the nonarchimedean analogues are strikingly different.

We now turn our attention to topological properties of $\mathbb{Q}_p$ by first recalling the ring of p-adic integers:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

and, in order to develop some intuition into the structure of this ring, considering the following:

Theorem 3.2. *The ring $\mathbb{Z}$ is a dense subset of $\mathbb{Z}_p$.*

Proof. For an integer x, we have that $|x|_p \leq 1$ and thus clearly $\mathbb{Z} \subseteq \mathbb{Z}_p$. We now demonstrate that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Let $\alpha \in \mathbb{Z}_p$ and $0 < \varepsilon < 1$. We must show that there exists an integer m such that $|m - \alpha|_p < \varepsilon$. We recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. That is, $\mathbb{Q}_p$ is the smallest field containing $\mathbb{Q}$ such that all p-adic Cauchy sequences converge. It follows that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Therefore we may find a *rational number* r/s such that $|r/s - \alpha|_p < \varepsilon$. By the strong triangle inequality we have that

$$\left|\frac{r}{s}\right|_p = \left|\frac{r}{s} - \alpha + \alpha\right|_p \leq \max\{\varepsilon, 1\} = 1 \ .$$

Thus we conclude that $r/s \in \mathbb{Z}_p$.

We now write r/s as

$$\frac{r}{s} = p^l \left(\frac{u}{v}\right) \ ,$$

where $l \geq 0$ and u, v, and p are pairwise relatively prime. Next we select an integer $i > 0$ so large that $p^{-i} < \varepsilon$. Plainly since p and v are relatively prime, it follows that p^i and v are also relatively prime. Thus there exist integers a and b satisfying

$$av + bp^i = 1 \quad \text{or equivalently} \quad bp^i = 1 - av \ . \tag{3.2}$$

Now define the integer m by $m = aup^l$. In view of (3.2) we have

$$\left|\frac{r}{s} - m\right|_p \quad = \quad \left|p^l \left(\frac{u}{v}\right) - p^l au\right|_p$$

$$\begin{aligned} &= \left|p^l \left(\frac{u}{v}\right)\right|_p |1 - av|_p \\ &= p^{-l} |1 - av|_p \leq |bp^i|_p \leq p^{-i} < \varepsilon \ . \end{aligned}$$

Therefore we have $|r/s - m|_p < \varepsilon$. Hence, by another application of the strong triangle inequality we conclude that

$$\begin{aligned} |m - \alpha|_p &= \left|m - \frac{r}{s} + \frac{r}{s} - \alpha\right|_p \\ &\leq \max\{|r/s - m|_p, |r/s - \alpha|_p\} < \varepsilon \ . \end{aligned}$$

Thus $\mathbb{Z}$ is a dense subring of $\mathbb{Z}_p$. □

Theorem 3.2 provides yet another example of the dramatic difference between p-adic and real analysis. The set of points in $\mathbb{R}$ that have absolute value less than or equal to 1 is the closed interval $[-1, 1]$, which has no particularly attractive algebraic structure. In the nonarchimedean setting, the analogous set, $\mathbb{Z}_p$, forms a *ring*. Moreover, we observe that in the archimedean case,

$$[-1, 1] \cap \mathbb{Z} = \{-1, 1\} \ ,$$

while in the nonarchimedean case

$$\mathbb{Z}_p \cap \mathbb{Z} = \mathbb{Z} \ .$$

Thus, the collection of integers in $\mathbb{Q}_p$ is a *bounded* subset that is dense in $\mathbb{Z}_p$.

Recall that a topological space $(X, \mathcal{T})$ is *locally compact* if for every point $x \in X$, there exists an open set $U \in \mathcal{T}$ such that $x \in U$ and the closure of U is compact. In the archimedean setting, we note that the interval $(-1, 1)$ in $\mathbb{R}$ is an open set whose closure is compact. This fact allows us to deduce that $\mathbb{R}$ is locally compact.

In fact the same strategy will allow us to prove that $\mathbb{Q}_p$ is also a locally compact field (thus, local compactness is a property enjoyed

by both archimedean and nonarchimedean completions). In the nonarchimedean analysis, perhaps not surprisingly, we will replace the set $[-1,1]$ with $\mathbb{Z}_p$. However in this case, we will not have to consider an analogue to the real open interval $(-1,1)$. For as we will now discover, $\mathbb{Z}_p$ is *both open and closed.*

Theorem 3.3. *The ring of p-adic integers, $\mathbb{Z}_p$, is both open and closed and moreover is a compact subset of $\mathbb{Q}_p$.*

Proof. It is a straightforward exercise to verify that

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 2\} .$$

Given this identity and our metric topology, we conclude that $\mathbb{Z}_p$ is an open set. Clearly, in view of the definition of $\mathbb{Z}_p$, we have that it is also closed.

To show that $\mathbb{Z}_p$ is compact, we begin by claiming that

$$\mathbb{Z}_p = \bigcup_{a=0}^{p-1} (a + p\mathbb{Z}_p) . \tag{3.3}$$

To establish this assertion, we first observe that any element in the union of (3.4) has p-adic absolute value less than or equal to 1. Thus we have that $\bigcup_{a=0}^{p-1}(a + p\mathbb{Z}_p) \subseteq \mathbb{Z}_p$.

Suppose now that $\alpha \in \mathbb{Z}_p$. By Theorem 3.2 we have that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Hence there must exist an integer $m \in \mathbb{Z}$ such that $|\alpha - m|_p < 1/p$. Let $\tilde{m} \in \{0, 1, 2, \ldots, p-1\}$ be the unique element satisfying $m \equiv \tilde{m} \mod p$. It follows that $|m - \tilde{m}|_p \leq 1/p$. An application of the strong triangle inequality yields

$$|\alpha - \tilde{m}|_p = |\alpha - m + m - \tilde{m}|_p \leq \max\{|\alpha - m|_p, |m - \tilde{m}|_p\} = \frac{1}{p} .$$

Thus we conclude that given an $\alpha \in \mathbb{Z}_p$, there exists an integer a, $0 \leq a \leq p-1$, such that $\alpha \in a + p\mathbb{Z}_p$ and so $\mathbb{Z}_p \subseteq \bigcup_{a=0}^{p-1}(a + p\mathbb{Z}_p)$. Hence

identity (3.3) holds and, moreover, one can verify that the sets within the union are all pairwise disjoint.

We now prove that $\mathbb{Z}_p$ is compact by contradiction: We assume that $\mathbb{Z}_p$ is not compact. Then there must exist an infinite open cover $\{\mathcal{U}_\lambda\}_{\lambda\in\Lambda}$ of $\mathbb{Z}_p$ with the property that there is no finite subcollection of $\{\mathcal{U}_\lambda\}_{\lambda\in\Lambda}$ that also covers $\mathbb{Z}_p$. From identity (3.3) it follows that there must exist an a_0, $0 \leq a_0 \leq p-1$, such that the set

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

is *not* covered by finitely many of the $\mathcal{U}_\lambda$'s (for otherwise, we would be able to find a finite subcover). We now apply identity (3.3) again and notice that

$$a_0 + p\mathbb{Z}_p = a_0 + p\left(\bigcup_{a=0}^{p-1}(a + p\mathbb{Z}_p)\right) .$$

Thus, repeating our previous argument, there must exist an a_1, $0 \leq a_1 \leq p-1$, such that the set

$$a_0 + a_1 p + p^2\mathbb{Z}_p$$

is not covered by finitely many $\mathcal{U}_\lambda$'s. We continue this process and generate an infinite series

$$\sum_{n=0}^{\infty} a_n p^n$$

with the property that for any $N \geq 0$,

$$\left(\sum_{n=0}^{N} a_n p^n\right) + p^{N+1}\mathbb{Z}_p \tag{3.4}$$

is not covered by finitely many $\mathcal{U}_\lambda$'s. This infinite series converges to a point, let us call it α, in $\mathbb{Z}_p$. That is,

$$\alpha = \sum_{n=0}^{\infty} a_n p^n \ \in \mathbb{Z}_p \ .$$

Since $\{\mathcal{U}_\lambda\}_{\lambda\in\Lambda}$ is an open cover of $\mathbb{Z}_p$, there must exist an element of this collection, say $\mathcal{U}_{\lambda_0}$, such that $\alpha \in \mathcal{U}_{\lambda_0}$. Of course $\mathcal{U}_{\lambda_0}$ is an open set and the topology here is generated by open p-adic balls. Therefore there must exist an integer $N > 0$ so that the open ball centered at α of radius $1/p^N$.

$$B\left(\alpha, \frac{1}{p^N}\right) = \left\{x \in \mathbb{Z}_p : |\alpha - x|_p < \frac{1}{p^N}\right\} ,$$

is contained in $\mathcal{U}_{\lambda_0}$. We note that the ball $B\left(\alpha, 1/p^N\right)$ could have been defined by the following equivalent description:

$$B\left(\alpha, 1/p^N\right) = \alpha + p^{N+1}\mathbb{Z}_p \ . \tag{3.5}$$

We now observe that

$$\sum_{n=0}^{N} a_n p^n \in B\left(\alpha, 1/p^N\right)$$

because

$$\begin{aligned}
\left|\alpha - \sum_{n=0}^{N} a_n p^n\right|_p &= \left|\sum_{n=N+1}^{\infty} a_n p^n\right|_p \\
&= \left|p^{N+1}\right|_p \left|\sum_{n=N+1}^{\infty} a_n p^{n-(N+1)}\right|_p \\
&\leq p^{-(N+1)} < \frac{1}{p^N} \ .
\end{aligned}$$

Therefore, since every element within an open p-adic ball is the center of the ball, identity (3.5) reveals that

$$\left(\sum_{n=0}^{N} a_n p^n\right) + p^{N+1}\mathbb{Z}_p \subseteq \mathcal{U}_{\lambda_0} \ .$$

However this containment contradicts the defining property (3.4) of the series. Thus there must exist a finite subcover and hence $\mathbb{Z}_p$ is compact. □

Let α be an arbitrary element of $\mathbb{Q}_p$. Then the set $\alpha + \mathbb{Z}_p$ is, by the previous proof, an open set containing α that is compact. Therefore Theorem 3.3 immediately implies

Corollary 3.4. *The field of p-adic numbers, $\mathbb{Q}_p$, is locally compact.*

Moreover, the algorithm used in the proof of Theorem 3.3 provides a method for finding the p-adic "digits", $a_n \in \{0, 1, \ldots, p-1\}$, of an arbitrary $\alpha \in \mathbb{Q}_p$ in its p-adic expansion

$$\alpha = \sum_{n=T}^{\infty} a_n p^n \ .$$

The proof of Theorem 3.3 also highlights the fact that p-adic absolute values are, in reality, the generalizations of congruences. As we noted, $x \equiv y \bmod p$ if and only if $|x - y|_p < 1$. Thus the p-adic absolute value measures an *arithmetic distance* that is exactly captured by congruences. However notice that congruences are always studied in the context of *integers*, while the p-adic absolute value is able to handle arithmetic analysis of *rational numbers* and, as we have seen, irrational numbers from the completion $\mathbb{Q}_p$. Thus we have come upon the "right" tool to consider arithmetic issues: Traditionally working with the arithmetic via congruences is complicated and delicate. However now we can apply all the powerful machinery of analysis and topology to attempt to answer difficult arithmetic questions. In fact, these types of applications are what inspired Kurt Hensel to develop this theory in 1897. Thus we see that these ideas are not only beautiful and potentially powerful, but relatively new.

4 Restricted Topological Products: An Introduction to the Adèle Ring

Let $\{X_\lambda\}_{\lambda \in \Lambda}$ be a family of topological spaces. For almost all $\lambda \in \Lambda$ (that is, all but possibly a finite number of λ) let O_λ be a specified open set in X_λ. Let $\mathcal{X}$ be the space whose points are $\alpha = (\alpha_\lambda)_{\lambda \in \Lambda}$ where

$\alpha_\lambda \in X_\lambda$ for all $\lambda \in \Lambda$ and $\alpha_\lambda \in O_\lambda$ for almost all $\lambda \in \Lambda$. That is, the points of $\mathcal{X}$ are "vectors" with one component for each $\lambda \in \Lambda$ such that the element in the λth coordinate α_λ is an element of X_λ and more restrictively, for almost all components, the λth coordinate α_λ is not only in X_λ but in the specified open set O_λ in X_λ.

We give $\mathcal{X}$ a topology $\mathcal{T}$ generated by open sets of the form:

$$\Gamma = \prod_{\lambda \in \Lambda} \Gamma_\lambda \ ,$$

where Γ_λ is open in X_λ for all $\lambda \in \Lambda$ and $\Gamma_\lambda = O_\lambda$ for almost all $\lambda \in \Lambda$. We call the topological space $(\mathcal{X}, \mathcal{T})$ the *restricted topological product of the* $\{X_\lambda\}_{\lambda \in \Lambda}$ *with respect to* $\{O_\lambda\}$. To apply this topological construct to our setting, we recall that the collection of places of $\mathbb{Q}$ is defined by

$$V_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, 11, 13, \ldots\}$$

and corresponds to all the non-equivalent, nontrivial absolute values on $\mathbb{Q}$. Moreover, for each place $p \in V_{\mathbb{Q}}$, $\mathbb{Q}_p$ is a topological space with the metric topology induced by the absolute value $|\ |_p$. We now consider the family of topological spaces $\{\mathbb{Q}_p\}_{p \in V_{\mathbb{Q}}}$ and recall that for each prime number p, the ring of p-adic integers,

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \ ,$$

is an open set in the field of p-adic numbers $\mathbb{Q}_p$. Plainly almost all $p \in V_{\mathbb{Q}}$ are primes (in fact there is only one element in $V_{\mathbb{Q}}$, namely ∞, that is not a prime). Therefore for almost all $p \in V_{\mathbb{Q}}$ (all p except $p = \infty$), $\mathbb{Z}_p$ is an open set in $\mathbb{Q}_p$.

We write $(\mathbb{Q}_{\mathbb{A}}, \mathcal{T})$ for the restricted topological product of $\{\mathbb{Q}_p\}_{p \in V_{\mathbb{Q}}}$ with respect to $\{\mathbb{Z}_p\}_{p \text{ a prime}}$. That is, elements in the set $\mathbb{Q}_{\mathbb{A}}$ have the form: $\alpha = (\alpha_p)_{p \in V_{\mathbb{Q}}}$ with $\alpha_p \in \mathbb{Q}_p$ for all $p \in V_{\mathbb{Q}}$, and for almost all p, $\alpha_p \in \mathbb{Z}_p$. So α may be viewed as a "vector" with infinitely many components, the pth component α_p coming from the completion $\mathbb{Q}_p$ and

almost all of the components are, in fact, p-adic integers. We abbreviate $(\alpha_p)_{p \in V_{\mathbb{Q}}}$ as simply (α_p).

We now define the binary operations *addition* and *multiplication* on $\mathbb{Q}_{\mathbb{A}}$ as follows: If $\alpha = (\alpha_p)$ and $\beta = (\beta_p)$ are two elements of $\mathbb{Q}_{\mathbb{A}}$, then

$$\alpha + \beta = (\alpha_p + \beta_p) \quad \text{and} \quad \alpha\beta = (\alpha_p \beta_p) \ .$$

Here the addition $\alpha_p + \beta_p$ and multiplication $\alpha_p \beta_p$ correspond to the addition and multiplication in the field $\mathbb{Q}_p$ for the appropriate $p \in V_{\mathbb{Q}}$. Thus, we have defined addition and multiplication on $\mathbb{Q}_{\mathbb{A}}$ by componentwise addition and multiplication.

Theorem 4.1. *The set $\mathbb{Q}_{\mathbb{A}}$ with componentwise addition and multiplication forms a commutative topological ring with unity.*

Proof. We observe that $0 = (0)$ (here we mean that every component is 0) is an element of $\mathbb{Q}_{\mathbb{A}}$ and is the additive identity element in $\mathbb{Q}_{\mathbb{A}}$ and similarly $1 = (1)$ is in $\mathbb{Q}_{\mathbb{A}}$ and is the multiplicative identity element. The fact that the addition and multiplication are commutative follow immediately from the fact that $+$ and $\times$ defined on each completion $\mathbb{Q}_p$ are commutative.

Suppose now that $a = (a_p)$ is an element of $\mathbb{Q}_{\mathbb{A}}$. Then $a_p \in \mathbb{Q}_p$ for all p and for almost all p, $a_p \in \mathbb{Z}_p$ (that is, for almost all p, $|a_p|_p \leq 1$). Thus $-a_p$ is in $\mathbb{Q}_p$ for all p and for almost all p, $-a_p \in \mathbb{Z}_p$. Hence $-a = (-a_p)$ is another element of $\mathbb{Q}_{\mathbb{A}}$ and is plainly the additive inverse of a in $\mathbb{Q}_{\mathbb{A}}$. Suppose that $b = (b_p)$ is another element of $\mathbb{Q}_{\mathbb{A}}$. We again note that $b_p \in \mathbb{Z}_p$ for all but finitely many places p. Of course the set of primes p for which $b_p \in \mathbb{Z}_p$ need not be the same set for which $a_p \in \mathbb{Z}_p$. However the collection of primes p for which *either* a_p or b_p is *not* in $\mathbb{Z}_p$ is a finite set. Therefore, for all primes p not in this new finite set, both a_p and b_p are in $\mathbb{Z}_p$. That is, for almost all primes, a_p and b_p are both in $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a ring $a_p + b_p \in \mathbb{Z}_p$, we have that

$$a + b = (a_p) + (b_p) = (a_p + b_p)$$

is an element of $\mathbb{Q}_{\mathbb{A}}$, and thus $\mathbb{Q}_{\mathbb{A}}$ is closed under addition. A similar argument shows that $\mathbb{Q}_{\mathbb{A}}$ is closed under multiplication. All other conditions required for $\mathbb{Q}_{\mathbb{A}}$ to be a ring follow immediately from the fact that $\mathbb{Q}_p$ is a field (in particular, a ring) for each $p \in V_{\mathbb{Q}}$. □

The topological ring $\mathbb{Q}_{\mathbb{A}}$ is called the *adèle ring* (*associated with* $\mathbb{Q}$) and, in some sense, it empowers us to analyze arithmetic issues with respect to all primes simultaneously. We recall that a topological space $(X, \mathcal{T})$ is called a *Hausdorff space* if for any two distinct elements x and y in X, there exists disjoint open sets U_x, U_y so that $x \in U_x$ and $y \in U_y$. Recall that every metric space is a Hausdorff space.

Theorem 4.2. *The adèle ring* $\mathbb{Q}_{\mathbb{A}}$ *is a Hausdorff space.*

Proof. Let $a = (a_p)$ and $b = (b_p)$ be two distinct elements of $\mathbb{Q}_{\mathbb{A}}$. Since they are distinct, there must exist a place, say q, for which $a_q \neq b_q$; that is, there must exist a component for which the "vectors" a and b differ, otherwise $a = b$. Therefore we have found two distinct points, a_q and b_q in the metric space $\mathbb{Q}_q$, and since $\mathbb{Q}_q$ is a Hausdorff space, there exist two disjoint open sets U_q and V_q in $\mathbb{Q}_q$ such that $a_q \in U_q$ and $b_q \in V_q$. We now define two subsets $\mathcal{U}$ and $\mathcal{V}$ of $\mathbb{Q}_{\mathbb{A}}$ by:

$$\mathcal{U} = \prod_{\substack{p \neq q \\ a_p \notin \mathbb{Z}_p}} \mathbb{Q}_p \times \prod_{\substack{p \neq q \\ a_p \in \mathbb{Z}_p}} \mathbb{Z}_p \times U_q$$

and

$$\mathcal{V} = \prod_{\substack{p \neq q \\ b_p \notin \mathbb{Z}_p}} \mathbb{Q}_p \times \prod_{\substack{p \neq q \\ b_p \in \mathbb{Z}_p}} \mathbb{Z}_p \times V_q \, .$$

We now claim that both $\mathcal{U}$ and $\mathcal{V}$ are open sets in $\mathbb{Q}_{\mathbb{A}}$. This follows from the fact that at each component p the subsets defined there are open in $\mathbb{Q}_p$ and for almost all places p, the subsets are $\mathbb{Z}_p$. We note that $a \in \mathcal{U}$ and $b \in \mathcal{V}$. Finally, we claim that $\mathcal{U}$ and $\mathcal{V}$ are disjoint open sets. Suppose not, that is, suppose there exists an element $\zeta = (\zeta_p) \in \mathbb{Q}_{\mathbb{A}}$ such that $\zeta \in \mathcal{U}$ and $\zeta \in \mathcal{V}$. This assumption implies that the qth component

of ζ, ζ_q, is in both the qth components of $\mathcal{U}$ and $\mathcal{V}$. Thus,

$$\zeta_q \in U_q \quad \text{and} \quad \zeta_q \in V_q \ .$$

However the sets U_q and V_q are *disjoint sets*, which is a contradiction. Therefore $\mathcal{U}$ and $\mathcal{V}$ are disjoint and hence $\mathbb{Q}_{\mathbf{A}}$ is Hausdorff. □

Theorem 4.3. *The adèle ring $\mathbb{Q}_{\mathbf{A}}$ is a locally compact space.*

Proof. We must show that for any point in $\mathbb{Q}_{\mathbf{A}}$, there exists an open set containing the point whose closure is compact. Let $\alpha = (\alpha_p)$ be a element of $\mathbb{Q}_{\mathbf{A}}$. Define the set S as

$$S = \{p \in V_{\mathbb{Q}} : \alpha_p \notin \mathbb{Z}_p\} \ .$$

We note that since α is in $\mathbb{Q}_{\mathbf{A}}$, for almost all primes p, $\alpha_p \in \mathbb{Z}_p$. Thus the set S is a finite set. We have already seen that for any p, $\mathbb{Q}_p$ is locally compact. Therefore for each $p \in S$, there must exist an open set U_p in $\mathbb{Q}_p$ such that $\alpha_p \in U_p$ and the closure $\overline{U_p}$ of U_p is compact. We now define the subset $\mathcal{U}$ of $\mathbb{Q}_{\mathbf{A}}$ by

$$\mathcal{U} = \prod_{p \in S} U_p \times \prod_{p \notin S} \mathbb{Z}_p \ .$$

It follows that $\mathcal{U}$ is an open set in $\mathbb{Q}_{\mathbf{A}}$ and $\alpha \in \mathcal{U}$. Also its closure, $\overline{\mathcal{U}}$,

$$\overline{\mathcal{U}} = \prod_{p \in S} \overline{U_p} \times \prod_{p \notin S} \mathbb{Z}_p \ ,$$

is compact (recall that the $\mathbb{Z}_p$ are open, closed, and compact). Therefore $\mathbb{Q}_{\mathbf{A}}$ is locally compact. □

5 The Topology and Algebra of the Adèle Ring

We open our discussion by observing that we may embed the rational numbers $\mathbb{Q}$ into $\mathbb{Q}_{\mathbf{A}}$ in a natural way. If $a \in \mathbb{Q}$, then for almost all prime numbers p, $|a|_p = 1$. Consider the element $(a, a, a, a, \ldots)$.

From our previous remark, for almost all p, $a \in \mathbb{Z}_p$ and thus the vector $(a, a, a, a, \ldots)$ is an element of $\mathbb{Q}_{\mathbf{A}}$. We define the *natural diagonal map* $\eta : \mathbb{Q} \to \mathbb{Q}_{\mathbf{A}}$ by:

$$\eta(a) = (a, a, a, a, \ldots) \, .$$

The map η is easily seen to be one-to-one and therefore we may view η as an embedding of $\mathbb{Q}$ into $\mathbb{Q}_{\mathbf{A}}$. So we may view the rational numbers as being a subset of the adèles. Thus, for now on, whenever we view $\mathbb{Q} \subseteq \mathbb{Q}_{\mathbf{A}}$, we formally are considering $\mathbb{Q} \hookrightarrow \mathbb{Q}_{\mathbf{A}}$; that is, the image of the diagonal map $\eta(\mathbb{Q}) \subseteq \mathbb{Q}_{\mathbf{A}}$. We now consider how the rational numbers "sit inside" the adèles.

Recall that given a topological space $(X, \mathcal{T})$ and a subset S in X we say that set S is a *discrete subset* of X if given any element $s \in S$, there exists an open set $U \in \mathcal{T}$ such that $S \cap U = \{s\}$. That is, there exists an open set so that s is the only element of S in the open set. A subset D of X is said to be a *dense* subset of X if for every open set $U \in \mathcal{T}$, $D \cap U \neq \emptyset$. That is, D is dense if it intersects every open set.

We are about to demonstrate that the adèle ring is so vast that the set of rational numbers is a discrete subset. It is worth noting that the following proof contains only two fundamental ideas: First, the strange fact that every element of a p-adic open ball is its center and, second, the product formula:

$$\prod_{p \in V_{\mathbb{Q}}} |a|_p = 1 \text{ for all } a \in \mathbb{Q} \, , a \neq 0 \, .$$

Theorem 5.1. *The field of rational numbers $\mathbb{Q}$ is a discrete subset of the adèle ring $\mathbb{Q}_{\mathbf{A}}$.*

Proof. Suppose that $a \in \mathbb{Q} \subseteq \mathbb{Q}_{\mathbf{A}}$, that is, $a = (a, a, a, a, \ldots)$. We now define the subset $\mathcal{U}$ by

$$\mathcal{U} = \mathcal{U}_\infty \times \prod_{p \text{ prime}} \mathcal{U}_p \, ,$$

where

$$\mathcal{U}_\infty = \{x \in \mathbb{Q}_\infty \ : \ |x - a|_\infty < 1\}$$

and

$$\mathcal{U}_p = \{x \in \mathbb{Q}_p \ : \ |x - a|_p \leq 1\}$$

for p a prime. Clearly $\mathcal{U}_\infty$ is an open subset of $\mathbb{Q}_\infty (= \mathbb{R})$ and $\mathcal{U}_p$ is an open subset of $\mathbb{Q}_p$ for p prime. We now claim that for almost all p (that is, all but possibly finitely many p's), $\mathcal{U}_p = \mathbb{Z}_p$. We note that if $a = 0$, then this is trivially true since $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ |x - 0|_p \leq 1\}$. Thus we now assume that $a \neq 0$. Then for almost all primes p, $|a|_p = 1$. For all primes p for which $|a|_p = 1$, it follows that $0 \in \mathcal{U}_p$. Since 0 is an element of the p-adic open ball $\mathcal{U}_p$, we have that 0 can be viewed as the center of the ball. Therefore

$$\mathcal{U}_p = \{x \in \mathbb{Q}_p \ : \ |x - 0|_p \leq 1\} = \mathbb{Z}_p \ .$$

That is, for almost all p, $\mathcal{U}_p = \mathbb{Z}_p$, which establishes our claim. Thus we conclude that $\mathcal{U}$ is an open set in $\mathbb{Q}_\mathbb{A}$ containing a.

Suppose now that $b \in \mathbb{Q} \cap \mathcal{U}$. Then we have $|b - a|_\infty < 1$ and for all primes p, $|b - a|_p \leq 1$. Therefore we conclude

$$\begin{aligned} \prod_{p \in V_\mathbb{Q}} |b - a|_p &= |b - a|_\infty \prod_{p \text{ prime}} |b - a|_p \\ &\leq |b - a|_\infty \prod_{p \text{ prime}} 1 \\ &= |b - a|_\infty < 1 \ . \end{aligned}$$

That is, $\prod_{p \in V_\mathbb{Q}} |b - a|_p < 1$. However, $b - a \in \mathbb{Q}$. Hence by the product formula we must have $b - a = 0$, which implies that the only rational number contained in the open set $\mathcal{U}$ is a. Hence $\mathbb{Q}$ is a discrete subset of $\mathbb{Q}_\mathbb{A}$. □

To further explore the structure of $\mathbb{Q}$ as a subset of $\mathbb{Q}_\mathbb{A}$, we turn our attention to some algebraic considerations. Since $\mathbb{Q}$ is a field and $\mathbb{Q}_\mathbb{A}$

is a ring we trivially have that $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{\mathbf{A}}, +)$ are additive abelian groups. If we wish to consider $\mathbb{Q}$ and $\mathbb{Q}_{\mathbf{A}}$ as mearly groups under addition, then we denote these groups as $\mathbb{Q}^+$ and $\mathbb{Q}_{\mathbf{A}}^+$. We note that $\mathbb{Q}^+$ is a subgroup of $\mathbb{Q}_{\mathbf{A}}^+$ and quotient space $\mathbb{Q}_{\mathbf{A}}^+/\mathbb{Q}^+$ is another abelian group.

Theorem 5.2. *Let $\gamma : \mathbb{Q}_{\mathbf{A}}^+ \to \mathbb{Q}_{\mathbf{A}}^+/\mathbb{Q}^+$ be the natural homomorphism defined by $\gamma(\alpha) = \alpha + \mathbb{Q}^+$, and give $\mathbb{Q}_{\mathbf{A}}^+/\mathbb{Q}^+$ the quotient topology generated by γ. Then $\mathbb{Q}_{\mathbf{A}}^+/\mathbb{Q}^+$ is compact.*

Before proving this theorem we make an important observation. The previous two theorems imply that the set $\mathbb{Q}$ is a *lattice* in $\mathbb{Q}_{\mathbf{A}}$. That is, the subset $\mathbb{Q}$ sits inside $\mathbb{Q}_{\mathbf{A}}$ in the same way that $\mathbb{Z}$ sits inside of $\mathbb{R}$: $\mathbb{Z}$ is discrete in $\mathbb{R}$ and $\mathbb{R}/\mathbb{Z}$ is isomorphic to the circle group, which is compact. There is a significant distinction between these two examples: The roles of ring and field have been transposed. The discrete set $\mathbb{Z}$ is a ring that is contained in the field $\mathbb{R}$ whose quotient is compact. On the other hand, the *field* $\mathbb{Q}$ is the discrete subset contained in the *ring* $\mathbb{Q}_{\mathbf{A}}$ whose quotient is compact. In particular, we see that the nonzero elements of the *lattice* $\mathbb{Q}$ in $\mathbb{Q}_{\mathbf{A}}$ have multiplicative inverses. This insight highlights some of the rich algebraic structure within $\mathbb{Q}_{\mathbf{A}}$. We prove the theorem by first establishing the following lemma that, in some sense, defines a fundamental domain in $\mathbb{Q}_{\mathbf{A}}$.

Lemma 5.3. *Let $\mathcal{F} \subseteq \mathbb{Q}_{\mathbf{A}}$ be the subset defined by*

$$\mathcal{F} = \prod_{p \in V_{\mathbb{Q}}} \mathcal{F}_p \ ,$$

in which

$$\mathcal{F}_\infty = \{x \in \mathbb{Q}_\infty : |x|_\infty \leq \tfrac{1}{2}\}$$

and, for p prime,

$$\mathcal{F}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \ .$$

Then for every $\alpha = (\alpha_p) \in \mathbb{Q}_{\mathbf{A}}$ there exists elements $\omega \in \mathcal{F}$ and $\zeta \in \mathbb{Q}$ such that α can be decomposed as

$$\alpha = \omega + \zeta \ .$$

Proof. Let $\alpha = (\alpha_p)$ be an element of $\mathbb{Q}_{\mathbf{A}}$. We must show that there exists $\omega \in \mathcal{F}$ and $\zeta \in \mathbb{Q}$ such that $\alpha = \omega + \zeta$. We claim that for each prime p, there exists a rational number, r_p, of the form $r_p = n_p/p^{m_p}$, where $n_p, m_p \in \mathbb{Z}$, $m_p \geq 0$, satisfying $|\alpha_p - r_p|_p \leq 1$. To establish this assertion we first observe that since (α_p) is an element of the adèles, for almost all primes p, $|\alpha_p|_p \leq 1$. Hence for all such primes p, r_p may be taken to be 0. We now consider the (finite) collection of primes p for which $|\alpha_p|_p > 1$ and recall from Section 2 that since $\alpha_p \in \mathbb{Q}_p$, α_p has a p-adic expansion of the form

$$\alpha_p = \sum_{n=T}^{\infty} a_n p^n \ ,$$

where $a_n \in \{0, 1, \ldots, p-1\}$ for all n. Thus, selecting the integer N large enough, the rational number

$$\sum_{n=T}^{N} a_n p^n$$

could be chosen for r_p. That is, the previous finite sum can be expressed as n_p/p^{m_p} and is p-adically within 1 unit of α_p. Since $r_p \neq 0$ for only finitely many primes, we have that

$$r = \sum_{p \text{ prime}} r_p$$

converges (it is, in fact, a *finite* sum) to a rational number. We observe that for any fixed prime number q,

$$\begin{aligned} |\alpha_q - r|_q &= \left| (\alpha_q - r_q) - \sum_{p \neq q} r_p \right|_q \\ &\leq \max\{|\alpha_q - r_q|_q, |r_{p_1}|_q, |r_{p_2}|_q, \ldots, |r_{p_t}|_q\} \\ &\leq 1 \ . \end{aligned}$$

Next we select an integer s so that

$$|\alpha_\infty - r - s|_\infty \leq \frac{1}{2} \ .$$

We now define $\omega = (\omega_p) = (\alpha_p - r - s)$. We note that

$$|\omega_\infty|_\infty = |\alpha_\infty - r - s|_\infty \leq \frac{1}{2} ,$$

and for p prime,

$$|\omega_p|_p = |\alpha_p - r - s|_p \leq \max\{|\alpha_p - r|_p, |s|_p\} \leq 1 .$$

Therefore $\omega = (\omega_p) \in \mathcal{F}$. If we define $\zeta = r + s$ $(\in \mathbb{Q})$, then clearly $\alpha = \omega + \zeta$, which completes the proof. □

Proof of Theorem 5.2. Let $\mathcal{F}$ be the fundamental domain as defined in Lemma 5.3. By Tychonoff's Theorem, $\mathcal{F}$ is compact in $\mathbb{Q}_{\mathbb{A}}$ since it is the topological product of compact sets. If we define the map

$$\gamma\Big|_{\mathcal{F}} : \mathcal{F} \to \mathbb{Q}_{\mathbb{A}}^+/\mathbb{Q}^+$$

to be the restriction of the natural homomorphism γ on $\mathbb{Q}_{\mathbb{A}}^+$ to the subset $\mathcal{F}$, then by the definition of the quotient topology on $\mathbb{Q}_{\mathbb{A}}^+/\mathbb{Q}^+$, we have that $\gamma\Big|_{\mathcal{F}}$ is a continuous function. We now claim that $\gamma\Big|_{\mathcal{F}}$ is surjective. Suppose that $\alpha + \mathbb{Q}^+ \in \mathbb{Q}_{\mathbb{A}}^+/\mathbb{Q}^+$ is an arbitrary element in the quotient space (so $\alpha \in \mathbb{Q}_{\mathbb{A}}^+$). From Lemma 5.3 there exist $\omega \in \mathcal{F}$ and $\zeta \in \mathbb{Q}$ such that $\alpha = \omega + \zeta$. Thus, $\omega = \alpha - \zeta \in \mathcal{F}$ and

$$\gamma\Big|_{\mathcal{F}}(\omega) = \omega + \mathbb{Q}^+ = \alpha - \zeta + \mathbb{Q}^+ = \alpha + \mathbb{Q}^+ .$$

Hence $\mathbb{Q}_{\mathbb{A}}^+/\mathbb{Q}^+$ is the continous image of a compact set and therefore is compact. □

6 Geometry of Numbers over the Adèle Ring

The subject of "Geometry of Numbers" was first studied by Hermann Minkowski in 1896. At the most basic level, the subject answers the following question. Suppose that K is a convex, symmetric set in Euclidean N-space $(\mathbb{R}^N)$. How big does the set K have to be in order to

insure that K contains a nonzero integer lattice point? In this question, we measure "how big K is" by computing its N-dimensional volume; this is, its Lebesgue measure in $\mathbb{R}^N$. We recall that Lebesgue measure (or volume) satisfies two fundamental properties: First, the volume of any compact (measurable) set is finite and the volume of any nontrivial open (measurable) set is positive. And second, volume is translation invariant. If we write $\mathrm{Vol}_N(K)$ for the N-dimensional Lebesgue measure of K, then we could state Minkowski's Convex Body Theorem as follows:

Minkowski's Convex Body Theorem. *Let K be a convex, symmetric set in $\mathbb{R}^N$. If $\mathrm{Vol}_N(K) > 2^N$, then $K \cap \mathbb{Z}^N \neq \{\vec{0}\}$. That is, K contains a nonzero integer lattice point.*

We now wish to study the analogous issue over the adèle ring associated with $\mathbb{Q}$. That is, given a "convex, symmetric" subset of $\mathbb{Q}_{\mathbf{A}}$, how large does it have to be so that it contains a nonzero lattice point? Here the lattice in $\mathbb{Q}_{\mathbf{A}}$ is the field $\mathbb{Q}$. This generalized theory will involve a translation invariant measure on $\mathbb{Q}_{\mathbf{A}}$.

Let G be a locally compact abelian group. Thus, we have an abelian group G that can be viewed as a topological space, and as such is locally compact and Hausdorff. In Section 5 we established that $\mathbb{Q}_{\mathbf{A}}^+$ is an example of such an object.

A collection of subsets $\mathcal{S}$ of G is called a *σ-algebra in G* if the following are satisfied:

(1) $G \in \mathcal{S}$.

(2) If $S \in \mathcal{S}$, then $\mathrm{comp}(S) \in \mathcal{S}$, where $\mathrm{comp}(S)$ is the complement of S in G.

(3) The (countable) union of elements of $\mathcal{S}$ is an element of $\mathcal{S}$.

Let $\mathcal{B}$ be the smallest σ-algebra in G that contains all the open sets of G. The elements of $\mathcal{B}$ are called the *Borel sets of G*. We now state

an important theorem of Alfred Haar from 1932 that states that there exists a way to measure "volume" in any locally compact abelian group.

Theorem 6.1. *If G is a locally compact abelian group, then there exists a (positive) regular measure μ on the Borel sets $\mathcal{B}$ in G such that:*

(1) $\mu(K) < \infty$ for all compact sets $K \in \mathcal{B}$.

(2) $\mu(U) > 0$ for all nontrivial open sets $U \in \mathcal{B}$.

(3) $\mu(g + E) = \mu(E)$ for all $g \in G$ and $E \in \mathcal{B}$; that is, μ is translation invariant.

Moreover, μ is unique upto a multiplicative constant.

The measure μ from Theorem 6.1 is called *Haar measure on G*. So for example, Lebesgue measure is a Haar measure on $\mathbb{R}$. We will normalize a Haar measure, μ, on $\mathbb{Q}_{\mathbf{A}}$ as follows. We first let μ_∞ be the usual (Lebesgue) measure on $\mathbb{Q}_\infty = \mathbb{R}$. Then for each prime p, since $\mathbb{Q}_p$ is a locally compact abelian group, there is a Haar measure on it. We normalize the Haar measure, μ_p, on $\mathbb{Q}_p$ so that $\mu_p(\mathbb{Z}_p) = 1$. That is, we normalize so that the measure of the compact ring of p-adic integers is equal to 1. Then, informally, we define the Haar measure μ on $\mathbb{Q}_{\mathbf{A}}$ to be the product measure associated with the local measures defined above. That is,

$$\mu = \prod_{p \in V_{\mathbb{Q}}} \mu_p \ .$$

So if $\mathcal{U} = \prod_p \mathcal{U}_p$ is a measurable subset in $\mathbb{Q}_{\mathbf{A}}$ then

$$\mu(\mathcal{U}) = \prod_{p \in V_{\mathbb{Q}}} \mu_p(\mathcal{U}_p) \ .$$

We are now able to offer the (one-dimensional) adelic convex body theorem.

Theorem 6.2. *If $\alpha = (\alpha_p) \in \mathbb{Q}_{\mathbf{A}}$ satisfies*

$$\prod_{p \in V_{\mathbb{Q}}} |\alpha_p|_p > 1 \ ,$$

then there exists a rational number $\beta \in \mathbb{Q} \subseteq \mathbb{Q}_{\mathbb{A}}$ *such that*

(i) $\beta \neq 0$.

(ii) For all $p \in V_{\mathbb{Q}}$, $|\beta|_p \leq |\alpha_p|_p$.

We can reformulate Theorem 6.2 as follows. Given $\alpha = (\alpha_p) \in \mathbb{Q}_{\mathbb{A}}$ as in the theorem, we define the set $K = \prod_p K_p \subseteq \mathbb{Q}_{\mathbb{A}}$ by

$$K_p = \{x \in \mathbb{Q}_p : |x|_p \leq |\alpha_p|_p\} ,$$

for all $p \in V_{\mathbb{Q}}$. In some sense K is a convex, symmetric subset of the adèle ring. Then Theorem 6.2 asserts that if $\mu(K) > 2$ then $K \cap \mathbb{Q} \neq \{0\}$. That is, K contains a nonzero (rational) lattice point β.

Proof of Theorem 6.2. For almost all p, $|\alpha_p|_p \leq 1$. Since $\prod_p |\alpha_p|_p > 1$, we conclude that $|\alpha_p|_p = 1$ for almost all p. We now define the set $\mathcal{F} = \prod_p \mathcal{F}_p$ in $\mathbb{Q}_{\mathbb{A}}^+$ by

$$\mathcal{F}_\infty = \{x \in \mathbb{Q}_\infty : |x|_\infty \leq \tfrac{1}{2}\} ,$$

and for prime p

$$\mathcal{F}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \quad (= \mathbb{Z}_p) .$$

By Theorem 5.2, $\mathbb{Q}_{\mathbb{A}}^+ / \mathbb{Q}^+$ is compact and thus it has finite measure (technically the Haar measure on the quotient space is the measure induced by the measure μ on $\mathbb{Q}_{\mathbb{A}}$). Moreover, it turns out that the measure of the compact set $\mathbb{Q}_{\mathbb{A}}^+ / \mathbb{Q}^+$ is equal to $\mu(\mathcal{F})$. We now compute $\mu(\mathcal{F})$:

$$\mu(\mathcal{F}) = \prod_p \mu_p(\mathcal{F}_p) = \mu_\infty(\mathcal{F}_\infty) \prod_{p \text{ prime}} \mu_p(\mathbb{Z}_p) = 1 .$$

We now define the set $S = S(\alpha) = \prod_p S_p \subseteq \mathbb{Q}_{\mathbb{A}}$ by

$$S_\infty = \{w \in \mathbb{Q}_\infty : |w|_\infty \leq \tfrac{1}{2}|\alpha_\infty|_\infty\} ,$$

and for prime p

$$S_p = \{w \in \mathbb{Q}_p : |w|_p \leq |\alpha_p|_p\} .$$

In view of our hypothesis, we observe that

$$\mu(S) = \prod_p \mu_p(S_p) = \prod_p |\alpha_p|_p \; \mu(\mathcal{F}) > 1 \; .$$

Since $\mathbb{Q}_{\mathbb{A}}^+/\mathbb{Q}^+$ has measure 1 and the measure of S is greater than 1, we conclude that the map

$$\gamma\Big|_S : S \to \mathbb{Q}_{\mathbb{A}}^+/\mathbb{Q}^+$$

is *not* injective. As this map is not injective, there must exist two distinct elements in S, say w_1 and w_2, satisfying $w_1 + \mathbb{Q}^+ = w_2 + \mathbb{Q}^+$. Alternatively, we have $\gamma(w_1) = \gamma(w_2)$; that is,

$$w_1 - w_2 \in \mathbb{Q}^+ \; .$$

If we let $\beta = w_1 - w_2$, then it follows that $\beta \in \mathbb{Q}$ and since w_1 and w_2 are distinct, $\beta \neq 0$. Since w_1 and w_2 are elements of S we note that

$$|\beta|_\infty = |w_1 - w_2|_\infty \leq |w_1|_\infty + |w_2|_\infty \leq \frac{1}{2}|\alpha_\infty|_\infty + \frac{1}{2}|\alpha_\infty|_\infty = |\alpha_\infty|_\infty \; ,$$

and for prime p, by the strong triangle inequality,

$$|\beta|_p = |w_1 - w_2|_p \leq \max\{|w_1|_p, |w_2|_p\} \leq |\alpha_p|_p \; .$$

Thus for all $p \in V_{\mathbb{Q}}$, $|\beta|_p \leq |\alpha_p|_p$. □

We close this section with the following interesting corollary.

Corollary 6.3. *Suppose that $\tilde{p}$ is a fixed place of $\mathbb{Q}$. For each place $p \in V_{\mathbb{Q}}$ not equal to $\tilde{p}$, suppose that $\delta_p \in \mathbb{Q}_p$ with $|\delta_p|_p = 1$ for almost all $p \neq \tilde{p}$. Then there exists a rational number β, $\beta \neq 0$ satisfying*

$$|\beta|_p \leq |\delta_p|_p \; ,$$

for all $p \neq \tilde{p}$.

Proof. Select an element $\alpha_{\tilde{p}} \in \mathbb{Q}_{\tilde{p}}$ such that $|\alpha_{\tilde{p}}|_{\tilde{p}}$ is so large that

$$\prod_{\text{All } p \in V_{\mathbb{Q}}} |\alpha_p|_p > 1 \, .$$

By Theorem 6.2 there is a nonzero rational number β such that

$$|\beta|_p \leq |\alpha_p|_p$$

for all $p \in V_{\mathbb{Q}}$. □

As we will discover in the next section, Corollary 6.3 has an interesting geometric interpretation. We will prove that the field $\mathbb{Q}$ delicately sits in the ring $\mathbb{Q}_{\mathbb{A}}$: $\mathbb{Q}$ is discrete in $\mathbb{Q}_{\mathbb{A}}$, however, if we were to remove any *one* completion $\mathbb{Q}_{\tilde{p}}$ from the adèle ring, then $\mathbb{Q}$ would be a *dense* subset in the resulting new restricted topological product.

7 Approximation Theorems in Algebraic Number Theory

In view of Corollary 6.3, we are now in a position to prove an important result from classical algebraic number theory known as the Strong Approximation Theorem.

Theorem 7.1. (Strong Approximation Theorem) *Suppose that $\tilde{p}$ is a fixed place. Let S be a finite set of places of $\mathbb{Q}$, with $\tilde{p} \notin S$. Suppose that $\alpha_p \in \mathbb{Q}_p$, for each $p \in S$, and $\varepsilon > 0$ is a real number. Then there exists a $\beta \in \mathbb{Q}$ satisfying*

$$|\alpha_p - \beta|_p < \varepsilon \ , \ \textit{for all } p \in S \ ,$$

and

$$|\beta|_p \leq 1 \ , \ \textit{for all } \ p \notin S \cup \{\tilde{p}\} \ .$$

Proof. By Lemma 5.3, we know there exists a set

$$\mathcal{F} = \{x = (x_p) \in \mathbb{Q}_{\mathbb{A}} : |x_p|_p \leq b_p\} \subseteq \mathbb{Q}_{\mathbb{A}} \ ,$$

in which $b_\infty = \frac{1}{2}$, and $b_p = 1$, for all primes p, with the property that every $\varphi = (\varphi_p) \in \mathbb{Q}_{\mathbb{A}}$ can be expressed as

$$\varphi = \omega + \zeta \ ,$$

where $\omega \in \mathcal{F}$ and $\zeta \in \mathbb{Q}$. By Corollary 6.3, we can find a nonzero $\gamma \in \mathbb{Q}$ such that $|\gamma|_p \leq |\delta_p|_p$ for all $p \neq \tilde{p}$, where $|\delta_p|_p < b_p^{-1}\varepsilon$, for $p \in S$, and $|\delta_p|_p = b_p^{-1}$, for all $p \notin S \cup \{\tilde{p}\}$. Thus,

$$\begin{aligned} |\gamma|_p &< b_p^{-1}\varepsilon \quad \text{for all } p \in S \ , \\ |\gamma|_p &\leq b_p^{-1} \quad \text{for all } p \notin S \cup \{\tilde{p}\} \ . \end{aligned}$$

Since $\gamma\varphi = \gamma\omega + \gamma\zeta$, we conclude that for any $a \in \mathbb{Q}_{\mathbb{A}}$, $a = \psi + \beta$ where $\psi \in \gamma\mathcal{F}$ and $\beta \in \mathbb{Q}$. We now define $a = (a_p) \in \mathbb{Q}_{\mathbb{A}}$ by $a_p = \alpha_p$ for all $p \in S$ and $a_p = 0$ otherwise. Hence there must exist a $\psi \in \gamma\mathcal{F}$ and $\beta \in \mathbb{Q}$ satisfying $a = \psi + \beta$; or equivalently $\beta = a - \psi$. We now claim that β satisfies the inequalities of the theorem. If $p \in S$, then

$$\begin{aligned} |\alpha_p - \beta|_p &= |\alpha_p - (a_p - \gamma\omega_p)|_p \\ &= |\alpha_p - \alpha_p + \gamma\omega_p|_p \\ &= |\gamma\omega_p|_p = |\gamma|_p \, |\omega_p|_p < b_p^{-1}\varepsilon b_p = \varepsilon \ . \end{aligned}$$

If $p \notin S \cup \{\tilde{p}\}$ then

$$|\beta|_p = |0 - \gamma\omega_p|_p \leq b_p^{-1}b_p = 1 \ ,$$

which completes the proof. □

There are other formulations of the Strong Approximation Theorem. We offer a geometric version below that was foreshadowed at the end of Section 6.

Theorem 7.2. *Suppose that $\tilde{p}$ is a fixed place. Let $\mathbb{Q}_{\mathbb{A}}(\tilde{p})$ be the restricted topological product of $\{\mathbb{Q}_p\}_{p \neq \tilde{p}}$ with respect to $\{\mathbb{Z}_p\}_{p \neq \tilde{p}}$. Then if $\mathbb{Q}$ is identified with its image in $\mathbb{Q}_{\mathbb{A}}(\tilde{p})$ by the usual diagonal embedding, then $\mathbb{Q}$ is a* dense *subset of $\mathbb{Q}_{\mathbb{A}}(\tilde{p})$.*

In the Strong Approximation Theorem, we have a bound for β at every place except for $\tilde{p}$. In some sense, we loss control over $|\beta|_{\tilde{p}}$; that is, in most situations, there will be a very high power of $\tilde{p}$ in the denominator of β. Furthermore, the Strong Approximation Theorem asserts that for all $p \notin S \cup \{\tilde{p}\}$, $|\beta|_p \leq 1$. Of course we know that for almost all p, $|\beta|_p = 1$. These observations lead us to the following question: How many places $p \notin S \cup \{\tilde{p}\}$ satisfy $|\beta|_p < 1$? That is, how many prime factors not in $S \cup \{\tilde{p}\}$ must occur in the factorization of β? Here we state a new result of the author asserting that only *one* additional prime is needed.

To avoid complications, we assume that S is a finite collection of places containing the place ∞. The (multiplicative) group of *S-units* is defined by

$$\mathcal{U}_S = \{\alpha \in \mathbb{Q} \ : \ |\alpha|_p = 1 \text{ for all } p \notin S\} \ .$$

Thus the Strong Approximation Theorem may be phrased as follows: There exists a finite collection of places S', $S \subseteq S'$, so that the nonzero rational number β that satisfies the inequalities of the Strong Approximation Theorem also satisfies: $\beta \in \mathcal{U}_{S'}$ and $|\beta|_p < 1$ for all primes $p \in S' \setminus S$, $p \neq \tilde{p}$. In fact, there need be only *one* prime $p \notin S \cup \{\tilde{p}\}$ satisfying $|\beta|_p < 1$ and moreover $|\beta|_p = p^{-1}$ for that prime. Furthermore, the prime p may be selected from any specified arithmetic progression. For relatively prime integers a and $b > 0$, we write $\mathcal{A}(a, b)$ for the arithmetic progression

$$\mathcal{A}(a, b) = \{a + bn \ : \ n = 0, 1, 2, \ldots\} \ .$$

We now state our new formulation of the Strong Approximation Theorem.

Theorem 7.3. *Let S be a finite collection of places of $\mathbb{Q}$ containing the infinite place. Let $\mathcal{A} = \mathcal{A}(a, b)$ be an arithmetic progression with $gcd(a, b) = 1$ and b relatively prime to each prime in S. Let $\tilde{p} \notin S$ be a fixed prime. For each place $p \in S$, let $\alpha_p \in \mathbb{Q}_p$ and $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$. Then there exists an S-unit u, an integer $k > 0$, and a prime $\tilde{q} \in \mathcal{A}$, $\tilde{q} \notin S$,*

satisfying

$$|\alpha_p - \tilde{p}^{-k}\tilde{q}u|_p < \varepsilon \ ,$$

for all $p \in S$.

We conclude with a modern proof of the ancient Chinese Remainder Theorem.

Theorem 7.4. (Chinese Remainder Theorem) *Let* $m_1, m_2, \ldots, m_N$ *be pairwise relatively prime integers, each greater than 1. If* $a_1, a_2, \ldots, a_N$ *are integers, then there exists an integer* x *satisfying the system of simultaneous congruences:*

$$x \equiv a_n \bmod m_n \ , \ \textit{for all } n = 1, 2, \ldots, N \ .$$

Proof. By unique factorization, without loss of generality, we may assume that $m_n = P_n^{t_n}$, where $P_1, P_2, \ldots, P_N$ are distinct primes, and $t_1, t_2, \ldots, t_N$ are positive integers. We now apply the Strong Approximation Theorem with $S = \{P_1, P_2, \ldots, P_N\}$ and with the fixed prime $\tilde{p} = \infty$. For each $P_n \in S$, we set $\alpha_{P_n} = a_n$ and we select a positive real number ε so small that

$$0 < \varepsilon \leq \min\left\{P_1^{-t_1}, P_2^{-t_2}, \ldots, P_N^{-t_N}\right\} \ .$$

Thus there exists a $\beta \in \mathbb{Q}$ such that

$$|a_n - \beta|_{P_n} < \varepsilon \ , \ \text{for } n = 1, 2, \ldots, N \ ,$$

and

$$|\beta|_p \leq 1 \ , \ \text{for all primes } p \notin S \ (p \neq \infty) \ .$$

We note that a_n is an integer, thus $|a_n|_p \leq 1$ for all prime numbers p. Hence we conclude that

$$|\beta|_{P_n} = |\beta - a_n + a_n|_{P_n} \leq \max\{|a_n - \beta|_{P_n}, |a_n|_{P_n}\} \leq 1 \ .$$

Therefore for *all* primes p, $|\beta|_p \leq 1$. It follows then that $\beta \in \mathbb{Z}$. Finally we observe that for each $n = 1, 2, \ldots, N$,

$$|a_n - \beta|_{P_n} < \varepsilon \leq P_n^{t_n} \ .$$

Thus $P_n^{t_n}$ must divide $\beta - a_n$, which is equivalent to

$$\beta - a_n \equiv 0 \bmod P_n^{t_n} \ , \quad \text{for } n = 1, 2, \ldots, N \ ,$$

and completes our proof. □

We discover that the Chinese Remainder Theorem is, in fact, a special case of the much more general Strong Approximation Theorem—for in the Strong Approximation Theorem, the α_p need not be integers (or even rational). Also, in the Chinese Remainder Theorem the fixed place is the infinite place. An interesting number theory exercise is to rework our proof of the Chinese Remainder Theorem with the fixed place being a prime, say 5, for example. One would produce a new variation of the Chinese Remainder Theorem. What would it imply? What would it say about the arithmetic structure of β?

8 Beyond the Field of Rational Numbers

A field k is called an *algebraic number field* if it is a finite field extension of $\mathbb{Q}$. Let V_k be the set of all places of k, that is, the set of all non-equivalent nontrivial absolute values on k. If $v \in V_k$, then we write $\| \ \|_v$ for the corresponding valuation. If we restrict the map $\| \ \|_v$ to $\mathbb{Q}$, then we will have a nontrivial absolute value on $\mathbb{Q}$. Thus, it will equivalent to $| \ |_p$ for some $p \in V_{\mathbb{Q}}$. In this case, we say that *the place v lies over the place p* and write $v|p$.

Conversely, we can select a place $p \in V_{\mathbb{Q}}$ and wonder many places $v \in V_k$ lie over p. To answer this question we first recall that since k is a finite (separable) extension of $\mathbb{Q}$, it follows that k is a simple extension

of $\mathbb{Q}$; that is, there exists an algebraic number α satisfying $k = \mathbb{Q}(\alpha)$. We write $F(x) \in \mathbb{Q}[x]$ for the minimal polynomial of α over $\mathbb{Q}$. Now given a place $p \in V_{\mathbb{Q}}$, we factor $F(x)$ in the polynomial ring $\mathbb{Q}_p[x]$:

$$F(x) = \prod_{m=1}^{M} f_m(x) \ ,$$

where each $f_m(x)$ is an irreducible polynomial in $\mathbb{Q}_p[x]$. In view of this factorization, it can be shown that the number of distinct places v that lie over p equals M.

All the valuation theory we developed in the previous sections can be extended to the setting of an algebraic number field k and its valuations V_k. In particular, once appropriately normalized, the absolute values satisfy the product formula:

Theorem 8.1. *For any nonzero $\alpha \in k$, it follows that*

$$\prod_{v \in V_k} \|\alpha\|_v = 1 \ .$$

In addition, the basic facts we established for $\mathbb{Q}_{\mathbb{A}}$ extend to the adèle ring $k_{\mathbb{A}}$ associated with k, including the strong approximate theorem.

Unlike the ring of integers $\mathbb{Z}$ in the field $\mathbb{Q}$, the ring of integers $\mathcal{O}_k$ in the field k might not enjoy the property of the unique factorization into primes. Through classical algebraic number theory we find that the *ideals* in any ring of integers $\mathcal{O}_k$ can always be factored uniquely into prime ideals. This investigation can be further refined to study how "far" the ring of integers is from being a unique factorization domain. In this setting, the ring of integers is a unique factorization domain precisely when it is a principal ideal domain. We recall that a principal ideal domain is a domain in which each ideal is generated by one element. Thus we can measure how far the ring of integers $\mathcal{O}_k$ is from being a unique factorization domain by measuring, in some sense, the ratio of ideals to principal ideals.

Given an algebraic number field k having ring of integers $\mathcal{O}_k$, we let $\mathcal{I}$ denote the set of all ideals contained in $\mathcal{O}_k$ and $\mathcal{I}^*$ the set of all principal ideals in $\mathcal{O}_k$. Plainly $\mathcal{I}^* \subseteq \mathcal{I}$. If we expand our collection of ideals to include fractional ideals, then we can endow these objects with a binary operation so that $\mathcal{I}$ is an abelian group with $\mathcal{I}^*$ as a subgroup. One considers related objects that are known as *divisors* and the *divisor group* however as we wish to convey only the underlying ideas, we consider the quotient group $\mathcal{I}/\mathcal{I}^*$. The associated quotient of divisors modulo the principal divisors is called the *class group* and the cardinality of the group is called the *class number of* k, denoted by $h = h_k$. We note that if $h = 1$, then $\mathcal{I} = \mathcal{I}^*$ and thus all ideals are principal and so $\mathcal{O}_k$ is a unique factorization domain. Thus we have:

Theorem 8.2. *The class number of an algebraic number field is 1 if and only if its ring of integers is a unique factorization domain.*

So the class number is the measure of how far $\mathcal{O}_k$ is from a unique factorization domain. It turns out that $\mathcal{O}_k$ is never "too far" from a unique factorization domain. We state this important result here:

Theorem 8.3. *The class number of any algebraic number field is finite.*

The proof of this deep theorem requires an application of the strong approximation theorem over k and involves the *idèle group*—the multiplicative group of units of the adèle ring. That is, the idèle group, $(k_{\mathbf{A}})^*$, is the set of elements $\alpha = (\alpha_v) \in k_{\mathbf{A}}$, for which $\alpha_v \neq 0$ for all $v \in V_k$ and for almost all $v \in V_k$, $|\alpha_v|_v = 1$. However instead of delving into this rich world of algebraic number theory, we will close here. Hopefully this journey provided some insights into how the theory of valuations and the adèle ring allow us to develop a deeper and more expansive notion of number and, indirectly, a greater appreciation for the beautiful way in which mathematics fits together.

"Arithmetic is the Queen of Mathematics" – Carl Friedrich Gauss

References

[1] E.B. Burger. *Exploring the Number Jungle: A Journey into Diophantine Analysis,* Student Mathematical Library **8**, American Mathematical Society, Providence, 2000.

[2] E.B. Burger. *Homogeneous Diophantine Approximation in S-integers,* Pacific J. Math. **152** (1992), 211–253.

[3] E.B. Burger. *Inhomogeneous inequalities over number fields,* Illinois J. Math. **38** (1994), 452–470.

[4] E.B. Burger. *On Mahler's compound bodies,* J. Austral. Math. Society (Series A) **55** (1993), 183–215.

[5] E.B. Burger and T. Struppeck. *Does* $\sum 1/n!$ *really converge? Infinite series and p-adic analysis,* The American Mathematical Monthly **103** (1996), 565–577.

[6] E.B. Burger and J.D. Vaaler. *On the decomposition of vectors over number fields,* J. reine angew. Math. **435** (1993), 197–219.

[7] J.W.S. Cassels. *Local Fields,* Cambridge University Press Cambridge, 1986.

[8] J.W.S. Cassels and A. Frohlich (Editors). *Algebraic Number Theory: Proceedings of an Instructional Conference by the London Mathematical Society,* Academic Press, Boston, 1986.

[9] F.Q. Gouvêa. *p-adic Numbers: An Introduction,* Springer-Verlag, Berlin-Heidelberg-New York, 2000.

[10] A. Weil. *Basic Number Theory,* Springer-Verlag, Berlin-Heidelberg-New York, 1995.

[11] EE. Weiss. *Algebraic Number Theory,* McGraw-Hill, New York, 1963.

Resumen

Aquí presentamos una introducción al anillo de adèles sobre el campo $\mathbb{Q}$ de los números racionales y destacamos algunas de sus bellas estructuras algebraicas y topológicas. Luego, aplicamos esta rica estructura en la revisión de algunos antiguos resultados de la teoría de números que colocamos dentro de este contexto moderno, y también hacemos algunas nuevas observaciones. Concluimos indicando cómo esta teoría nos permite ampliar la aritmética básica de $\mathbb{Q}$ a un más sutil, complejo e interesante ajuste de un campo arbitrario de números.

Palabras clave: Anillo de adèles, Análisis no arquimediano, Números p-ádicos

Edward B. Burger
Department of Mathematics
Williams College, Williamstown
Massachusetts 01267

eburger@williams.edu