1968

The topology of p-ADIC number fields

Ridgley E. Lange
Southern Illinois University Edwardsville

THE TOPOLOGY OF p-ADIC NUMBER FIELDS

A Thesis

Submitted to the Graduate Faculty of

Southern Illinois University

Edwardsville, Illinois

in partial fulfillment of the

requirements for the degree of

Master of Arts

in

The Faculty of Mathematical Studies

by

Ridgley E. Lange

A.B., Washington University

St. Louis, Missouri

August 1968

ACKNOWLEDGEMENT

Best thanks to De. George V. Poynor.

CONTENTS

ONE: PRELIMINARIES

In the first chapter we introduce the conceptual tools for the treatment of the topological properties of the p-adic number fields. We begin with the definition of valuation and give examples. Next we discuss the topology induced by a valuation. The last sections concern the p-adic completion of the rationals and certain consequences.

1.1 VALUATIONS

Definition 1. Let k be any field and let $|\cdot|:k \to R^+$, the nonnegative reals, be a mapping. Then one calls $|\cdot|$ a valuation on k iff for $a,b \in k$

V1. $|a| = 0$ iff $a = 0$,

V2. $|ab| = |a||b|$,

V3. $|a + b| \leq |a| + |b|$.

The ordinary absolute value on the real number field and the norm on the complex field both clearly satisfy V1-V3.

Suppose we now replace V3 in Definition 1 by the property:

V4. $|a + b| \leq \max\{|a|,|b|\}$, for all $a,b \in k$.

Certainly $|\cdot|$ is still a valuation, since $\max\{|a|,|b|\} \leq |a| + |b|$. A valuation satisfying V4 is nonarchimedean; otherwise archimedean.

It follows that $|m|_o^t \leq n(1 + t(\ln m/\ln n))\max\{1,|n|_o\}^{t(\ln m/\ln n)}$. Hence $|m|_o \leq [n(1 + t(\ln m/\ln n))]^{1/t}\max\{1,|n|_o\}^{(\ln m/\ln n)}$. In the limit, as $t \to \infty$, the number in brackets tends to 1; so

$$|m|_o \leq \max\{1,|n|_o\}^{(\ln m/\ln n)}. \tag{2}$$

We need to know that $|n|_o > 1$ if $n > 1$. Suppose there is a $k > 1$ such that $|k|_o \leq 1$. Then, by (2), $|m|_o \leq 1$ for all $m > 1$. Let a and b be two integers such that $|a|_o > |b|_o$. We then have, for any positive integer e,

$$\begin{aligned} |a + b|_o^e &= |(a + b)^e|_o, \quad \text{by V2,} \\ &\leq |\sum_{j=1}^{e}\binom{e}{j}a^j b^{e-j}|_o \leq (e+1)|a|_o^j|b|_o^{e-j} \\ &\leq (e + 1)|a|_o^e . \end{aligned}$$

Taking eth roots and letting $e \to \infty$, one again has $|a + b|_o \leq |a|_o \leq \max\{|a|_o,|b|_o\}$. This implies that $|\cdot|_o$ is nonarchimedean, a contradiction. Thus, $|n|_o > 1$ for $n > 1$. Hence, by (2),

$$|m|_o^{1/\ln m} \leq |n|_o^{1/\ln n} ; \tag{3}$$

and since m and n were arbitrary integers greater than 1, (3) can be reversed. We may then write for $n > 1$, $|n|_o^{1/\ln n} = \exp(r)$, for some $r > 0$. Therefore, $|n|_o = n^r = |n|^r$, if $n > 1$. For $n < -1$, $-n > 1$; so $|n|_o = |-n|_o = |-n|^r = |n|^r$. For $n = 1$, 0, or -1 the conclusion is evident. Thus, for all $x \in Q$, $|x|_o = |x|^r$.

1.2 METRIC SPACES

Definition 2. Let S be a set and let $d: S \times S \to R^+$. Then the pair (S,d) is a metric space with metric d iff for all $x, y, z \in S$

M1. $d(x,y) = 0$ iff $x = y$,

M2. $d(x,y) = d(x,y)$,

M3. $d(x,y) \leq d(x,z) + d(z,y)$.

Suppose S = k, the field of Definition 1, and $d(x,y) = |x-y|$ for $x,y \in k$. First, $x = y$ iff $|x-y| = 0$. Denote the identity element of k by 1. Then by V2, $|1| = |1 \cdot 1| = |1||1|$. Since $1 \neq 0$, $|1| = 1$ by V1. Again by V2, $1 = |(-1)^2| = |-1|^2$. Hence $|-1| = 1$. So we have $|x-y| = |-1(y-x)| = |-1||y-x| = |y - x|$. By V3 $|x-y| = |(x-z) + (z-y)| \leq |x-z| + |z-y|$. Hence M1, M2, and M3 hold for (k,d), where d is defined above. By Definition 2 we then have

Proposition 1. (k,) is a metric space.

This result enables us to construct a topological space in the ususal way. We shall denote $(k, |\cdot|)$ briefly by k, provided the meaning of the latter is clear.

Definition 3. An open sphere $S(r;x)$ in k with radius r and center x is $\{y \in k: |y - x| < r\}$. A set G in k is open iff for each $x \in G$ there is an $r > 0$ such that $S(r;x)$ is contained in G.

From this we derive the following facts:

Proposition 2. Let k be a metric space. Then

a. $\emptyset$ and k are open sets;

b. each open sphere is open;

c. G is open iff G is the union of open spheres;

d. arbitrary unions of open sets are open;

e. finite intersections of open sets are open.

Proof. The proof follows the usual line of reasoning. We show b. as a typical example.

Let $S(r;x)$ be an open sphere in the metric space k, and suppose $y \in S(r;x)$. By Definition 3, $|y-x| < r$. Let $|y-x| = r' \geq 0$. Set $t = r-r'$. Suppose $z \in S(t;y)$. Then, by Definition 3, $|z-y| < t$. Thus, by M3, $|z-x| \leq |z-y| + |y-x| < t + r' = r$. Again, by Definition 3, $S(r;x)$ is open.

The absolute value on the rationals gives rise to the usual topology. By Proposition 0, this topology is unique in the sense that any archimedean valuation on Q generates the same topology. In that topology we know that an open sphere has just one center. In the nonarchimedean case, however, each point in an open sphere is a center.

Proposition 3. Let $|\cdot|$ be nonarchimedean. Then, for each $z \in S(r;x)$, $S(r;z) = S(r;x)$.

Proof. Suppose $|\cdot|$ is a nonarchimedean valuation and $z \in S(r;x)$. Then, by definition, $|z-x| < r$, for any $y \in S(r;x)$, $|y-x| < r$. By V4, $|y-z| \leq \max\{|y-x|,|x-z|\} < r$. Hence $y \in S(r;z)$, and we have that $S(r;x)$ is contained in $S(r;z)$. By the same kind of argument, $S(r;z)$ is contained in $S(r;x)$. Thus $S(r;z) = S(r;x)$.

Definition 4. Let S be a subset of the metric space k. A point $x \in k$ is an accumulation point of S iff for each $r > 0$, $S(r;x) \cap (S-\{x\}) \neq \emptyset$. S is closed iff each accumulation point of S is an element of S.

Proposition 4. Let k be a metric space. Then a subset S of k is closed iff the complement of S in k is open.

Proof. This is another result from general topology; the proof is omitted.

1.3 CONVERGENCE

In this section we define the concepts needed below in the construction of a complete field from the rational field.

Definition 5. A sequence in a set S is a mapping from the positive integers into S. We denote this kind of mapping in the usual way by $\{x_n\}$. Let $\{x_n\}$ be a sequence in the metric space k. Then $\{x_n\}$ converges iff there is an $x \in k$ such that, given $\varepsilon > 0$, there is an $N > 0$ such that $d(x_n,x) < \varepsilon$ for all $n > N$. We call x the limit of the sequence $\{x_n\}$ and write $x_n \to x$, as $n \to \infty$;

or $\lim_{n\to\infty} x_n = x$. We shall frequently shorten the notation to read: $|x_n - x| < \varepsilon$ for n sufficiently large.

Definition 6. In a metric space k the sequence $\{x_n\}$ is cauchy iff, given $\varepsilon > 0$, there is an $N > 0$ such that $d(x_m, x_n) < \varepsilon$ for all $m,n > N$. To specify that the sequence $\{x_n\}$ is cauchy with respect to the metric d, we say $\{x_n\}$ is d-cauchy.

For metric spaces we have the following result:

Proposition 5. Every sequence that converges is cauchy.

The kind of metric space that will interest us most in the remainder of this paper is that in which the converse of Proposition 5 is true; namely,

Definition 7. A metric space k is complete iff each cauchy sequence in k converges.

It is well known that the rational field Q is not complete under the usual topology; but there is a "larger" field, R, containing Q that is complete under this topology. It turns out, however, that there are many more completions of Q under the nonarchimedean valuations. In the next section we introduce the p-adic valuations on Q which enable us to see this.

1.4 THE p-ADIC VALUATIONS ON Q

From elementary number theory we know that every integer has a unique factorization into primes. Let Q be the rational field, Z the ring of integers. Then Q = $\{ab^{-1}: a,b \in Z;\ b \neq 0\}$. Each $x \in Q$ can then be written as

$$x = \pm \frac{p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}}{q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}} \tag{4}$$

where the p's and q's are all distinct primes and e_i, $f_j \geq 0$. Now fix one prime p. Then (4) can be rewritten as

$$x = \frac{a}{b} p^r , \tag{5}$$

where $a,b,r \in Z$ and $(a,p) = (b,p) = 1$ [(a,p) denotes the greatest common divisor of a and p.] Choose c such that $0 < c < 1$. Define a mapping $|\cdot|_p : Q \to R$ by setting for each $x \in Q$, represented in (5),

$$|x|_p = c^r, \text{ if } x \neq 0, \text{ and} \tag{6}$$

$$|x|_p = 0, \text{ if } x = 0. \tag{7}$$

Since (5) guarantees the uniqueness of r, $|x|_p$ is well-defined. But more can be said:

Proposition 6. $|\cdot|_p$ is a nonarchimedean valuation on Q.

Proof. Let $x \in Q$. By (7), $|x|_p = 0$ iff $x = 0$. Suppose $x \neq 0$. From (5) there exist $a,b,r \in Z$, a and b both relatively prime to p such that $x = (a/b)p^r$; and thus $|x|_p = c^r$, $0 < c < 1$.

Then, clearly, $|x|_p > 0$ for all $x \neq 0$. Now suppose $y \in Q$ and $y = \frac{a'}{b'}p^s$, a', b', and s as in (5). Then $xy = \frac{aa'}{bb'}p^{r+s}$ such that $(aa',p) = (bb',p) = 1$. By (6)

$$(8) \qquad |xy|_p = c^{r+s} = c^r c^s = |x|_p |y|_p .$$

Now assume $|x|_p > |y|_p$. Then $s > r$ and $x + y = p^r\left(\frac{a}{b} + \frac{a'}{b'}p^t\right)$, $t = s-r > 0$. Hence, by (8), $|x+y|_p = |p^r|_p\left|\frac{a}{b} + \frac{a'}{b'}p^t\right|_p$. But $\frac{a}{b} + \frac{a'}{b'}p^t = \frac{ab'+a'bp^t}{bb'}$. Since both numerator and denominator of the last fraction are prime to p, its image under $|\cdot|_p$ is $c^0 = 1$. So $|x+y|_p = |p^r|_p = c^r = |x|_p = \max\{|x|_p, |y|_p\}$. Suppose next $|x|_p = |y|_p$, i.e., $r = x$. Then $x+y = p^{r'}\frac{d}{bb'}$, where $r' \geq r$ and $(d,p)=1$. Then, by definition, $|x+y|_p = c^{r'} \leq c^r = |x|_p = \max\{|x|_p, |y|_p\}$. We see $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x,y \in Q$. Since $|\cdot|_p$ satisfies V1, V2, and V4, it is a nonarchimedean valuation.

We note that in the course of the proof we have shown that $|x|_p \neq |y|_p$ implies $|x+y|_p = \max\{|x|_p, |y|_p\}$. Now let $c = 1/p$ and write "$|\cdot|$" for "$|\cdot|_p$". Then $|\cdot|$ will be called the <u>normalized p-adic valuation</u> on Q.

1.5 THE p-ADIC COMPLETION OF Q

We want to point out first that, as in the case of the archimedean valuation, Q is <u>not</u> complete under the p-adic valuation. It is clear that for some integer $n > 1$, $(1+p)^{1/n} \notin Q$ [5; 75]. But

$$(9) \qquad (1+p)^{1/n} = 1 + \frac{1}{n}p + \frac{1}{n}\left(1 - \frac{1}{n}\right)\frac{p^2}{2} + \ldots$$

by the binomial expansion. Let s_r be the rth partial sum on the right of (9). Surely $s_r \to (1+p)^{1/n}$, as $r \to \infty$, and $s_r \in Q$ for each r. For $r>t$, $|s_r - s_t| = |\sum_{i=t+1}^{r} a_i p^i| \leq \max\{|a_i p^i|\}$, $t<i\leq r$, by Proposition 6. But $\max\{|a_i p^i|\} \leq |p^{t+1}| = (1/p)^{t+1}$. Then as $t\to\infty$, hence $r\to\infty$, $|s_r - s_t| \to 0$. Hence $\{s_r\}$ is a cauchy sequence in Q which does not converge; so Q is not complete.

Definition 8. The space (Y,d') is a completion of the space (X,d) iff

C1. Y is d'-complete,

C2. there is a subset Y' of Y such that X is isometric to Y' and Y' is dense in Y.

We have observed that the real field R is a completion of Q under the ordinary absolute value. We now outline the construction of a p-adic completion of Q. This is done in a standard way. Let C be the set of all $|\cdot|$-cauchy sequences in Q. Define addition and multiplication in C as follows:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} \text{ and}$$

$$\{a_n\}\cdot\{b_n\} = \{a_n b_n\},$$

where $\{a_n\}$ and $\{b_n\}$ are $|\cdot|$-cauchy sequences in Q. It is evident that the element $\{1,1,1,\ldots\}$ in C is a multiplicative identity. We then have:

Lemma 1. C is a ring with identity.

The sequence $\{a_n\}$ is <u>null</u> iff $a_n \to 0$, as $n \to \infty$, or $|a_n| \to 0$, as $n \to \infty$. Every null sequence is cauchy since $|a_n| \to 0$ implies $|a_m - a_n| \leq \max\{|a_m|, |a_n|\} \to 0$, as $m,n \to \infty$. Let N be the set of all null sequences in Q. Then N is contained in C. Moreover, we state without proof

<u>Lemma 2</u>. N is a maximal ideal in C.

Thus, we know that the quotient ring C/N is a field. Let $\hat{Q} = C/N$.

<u>Proposition 7</u>. $\hat{Q}$ is a completion of Q.

Proof. By the definition of $\hat{Q}$, for each $x \in \hat{Q}$, $x = \{a_n\}+N$, where $\{a_n\}$ is cauchy in Q. Since V4 implies V3, $|a_m| = |a_n+(a_m-a_n)| \leq |a_n|+|a_m-a_n|$. So $|a_m|-|a_n| \leq |a_m-a_n|$. By similar reasoning, $|a_n|-|a_m| \leq |a_m-a_n|$. Hence $||a_m|-|a_n|| \leq |a_m-a_n|$, where the outer vertical bars on the left denote the usual absolute value on R. Hence $\{|a_n|\}$ is a cauchy sequence of real numbers. By the completeness of the real field, $\{|a_n|\}$ converges to a real number $\lim_{n\to\infty}|a_n|$. We define $v(x) = \lim_{n\to\infty}|a_n|$. Because of the uniqueness of this limit v is well defined. We claim that it is actually a valuation on $\hat{Q}$. Suppose x=0. Then $\{a_n\} \in N$ and $v(x) = \lim_{n\to\infty}|a_n| = 0$. Conversely, $v(x) = 0$ implies $\{a_n\}$ is a null sequence. Hence $x = 0$. Thus v satisfies V1. Let $y \in Q$ be $y = \{b_n\}+N$. Then $v(xy) = \lim_{n\to\infty}|a_nb_n| = \lim_{n\to\infty}|a_n||b_n| = \lim_{n\to\infty}|a_n| \cdot \lim_{n\to\infty}|b_n| = v(x)v(y)$ by V2 and limit properties. Thus V2 holds for V. Now

$v(x+y) = \lim_{n\to\infty}|a_n+b_n| \le \lim_{n\to\infty} \max\{|a_n|,|b_n|\} \le \max\{\lim_{n\to\infty}|a_n|, \lim_{n\to\infty}|b_n|\}$ $= \max v(x), v(y)$, by V4 and limit properties. So v satisfies V4 and is therefore a nonarchimedean valuation on Q.

Imbed Q in $\hat{Q}$ by $f: Q\to\hat{Q}$ such that for $a\varepsilon Q$ $f(a) = \{a\}+N$, $\{a\}$ the constant sequence in a. Let $Q' = f(Q)$, the image of Q under f. Then each $x\varepsilon Q'$ can be written as $\{a\}+N$, $a\varepsilon Q$. So $v(x) = v(f(a)) = \lim_{n\to\infty}|a| = |a|$. Hence f is an isometry from Q onto Q'.

Let x be any element of $\hat{Q}$. Then $x = \{a_n\}+N$, $a_n \varepsilon Q$. Since $\{a_n\}$ is cauchy, given $\varepsilon>0$, there is an $n_o>0$ such that $|a_n-a_m|<\varepsilon$ if $m,n>n_o$. Suppose $m>n_o$ and fixed, and let $y = \{a_m, a_m, \ldots\}+N$. Thus $y\varepsilon Q'$. By definition, $v(x-y) = \lim_{n\to\infty}|a_n-a_m|<\varepsilon$. This shows that Q' is dense in Q.

Finally, we prove Q is complete. Let $\{a_n'\}$ be cauchy in Q', where $a_n' = \{a_n, a_n, \ldots\}+N$, $a_n \varepsilon Q$. We have $v(a_n') = \lim_{n\to\infty}|a_n| = |a_n|$, which implies that $|a_n-a_m| = v(a_n'-a_m')$, since Q and Q' are isometric. Hence $\{a_n\}$ is cauchy in Q. Set $x = \{a_n\}+N$. Then $\lim_{n\to\infty} v(x-a_n') = \lim_{n\to\infty}\lim_{m\to\infty}|a_n-a_m| = 0$. Hence $\lim_{n\to\infty} a_n' = x$. Now suppose $\{x_n\}$ is any cauchy sequence in $\hat{Q}$. By the density of Q' in $\hat{Q}$, for each n there is a b_n in Q' such that $v(b_n-x_n)<\frac{1}{n}$. By V3 then,

(10) $v(b_n-b_m) \le v(b_n-x_n)+v(x_n-x_m)+v(x_m-b_m)$.

As $m,n\to\infty$, each term on the right of (10) approaches 0. So $\{b_n\}$ is cauchy. By the discussion above, $b_n\to b\varepsilon\hat{Q}$, as $n\to\infty$. Hence $v(b-x_n) \le v(b-b_n)+v(b_n-x_n)$. Since the limit of the

terms on the right of the last inequality is 0, we get $\lim_{n\to\infty} x_n = b$.

We have shown that $\hat{Q}$ satisfies C1 and C2 of Definition 8 and so is a completion of Q.

We note here without proof that $\hat{Q}$ is unique up to isomorphism. Furthermore, since Q is isomorphic to Q', we will say that Q is contained in $\hat{Q}$ and v extends $|\cdot|$ from Q to $\hat{Q}$. (This notion will be formalized later in section 2.3). For the present we write $v(x) = |x|$ for all $x \in \hat{Q}$.

For any field k denote the image of k under the valuation $|\cdot|$ by $|k|$. We then have

Proposition 8. $|\hat{Q}| = |Q|$.

Proof. We need only show that for any $x \in Q$ there is an $a \in Q$ such that $|x| = |a|$. The case $x = 0$ is clear enough. Hence, suppose $x \neq 0$. By Proposition 7, there is a sequence $\{a_n\}$ in Q such that $a_n \to x$. Thus, for sufficiently large n, $|x| = |a_n+(x-a_n)| = \max\{|a_n|,|x-a_n|\} = |a_n|$. This shows $|\hat{Q}| = |Q|$.

From Proposition 7 and the definition of a separable topological space, we see easily

Proposition 9. Considered as a topological space, $\hat{Q}$ is separable.

Proposition 10. The sequence $\{a_n\}$ converges in Q iff $\lim_{n\to\infty}|a_n-a_{n+1}| = 0$.

Proof. Suppose first that $\{a_n\}$ converges in $\hat{Q}$. Then, by Proposition 5, $\{a_n\}$ is cauchy. Hence $|a_n-a_m|\to 0$, as $m,n\to\infty$. In particular, $|a_n-a_{n+1}|\to 0$, an $n\to\infty$.

Suppose, conversely, that $|a_n-a_{n+1}|\to 0$, as $n\to\infty$, and suppose $m>n$. Then $|a_n-a_m|\leq \max\{|a_i-a_{i+1}|\}$, $n\leq i<m$. The last expression tends to 0, as $n\to\infty$. Hence $\{a_n\}$ is a cauchy sequence. By Proposition 7, $\{a_n\}$ converges.

Corollary. The series $\sum_{n=1}^{\infty} a_n$ converges iff $|a_n| \to 0$.

Proof. Let s_n be the nth partial sum of the series $\sum a_n$. By Proposition 10, the sequence $\{s_n\}$ converges iff $|a_n| = |s_{n-1}-s_n| \to 0$. Thus $\sum a_n$ converges iff $|a_n| \to 0$.

1.6 VALUATION RINGS

Proposition 11. Let k be a field with nonarchimedean valuation $|\cdot|$. Let $V = \{x\in k: |x| \leq 1\}$ and let $P = \{y\in k: |y| < 1\}$. Then V is a ring with unique maximal ideal P.

Proof. Suppose $x,y \in V$. Then by definition $|x|\leq 1$ and $|y|\leq 1$. Hence $|xy| = |x||y|\leq 1\cdot 1 = 1$. Thus $xy \in V$. Further $|x-y|\leq \max\{|x|,|y|\}\leq 1$. So $x-y\in V$. It follows that V is a ring in k.

Suppose next $x,y\in P$. Then $|x|<1$, $|y|<1$. Hence $|x-y|<1$. P is thus an additive subgroup of V. Let z be any element in V. Then $|xz| = |x||z| \leq |x| < 1$. Therefore, P is an ideal in V.

We show, moreover, that P is a maximal ideal in V. Suppose I is an ideal in V such that P is properly contained in I. Choose $a \in I-P$. Then, by the definition of P and V, $|a| = 1$. But $|a^{-1}| = |a|^{-1} = 1$. Hence $a^{-1} \in V$. In that case $1 = aa^{-1} \in I$, which implies $I = V$. Thus P is maximal; its uniqueness is obvious.

We shall call V the <u>valuation ring</u> of k <u>associated with</u> $|\cdot|$. Since P is a maximal ideal, it is prime. We observe that Q and $\hat{Q}$ both have respective valuation rings V and $\hat{V}$ associated with a p-adic valuation. V and $\hat{V}$ each have unique maximal ideals P and $\hat{P}$. It is easy to verify that $V = Q \cap \hat{V}$ and $P = Q \cap \hat{P}$. We observe also that an integer $a \in P$ iff $a \equiv 0(p)$. For if $a \in P$, then $|a| < 1$. Thus $a = bp^r$ for some $r > 0$. Hence $a \equiv 0(p)$. Conversely, $a \equiv 0(p)$ implies $|a| < 1$, or $a \in P$. We can thus write $a \equiv 0 \pmod{P}$ for $a \equiv 0(p)$. We need these remarks to establish

<u>Proposition 12</u>. Let x be any element in $\hat{Q}$. Then x has a unique representation in the form

$$x = \sum_{i=r}^{\infty} a_i p^i, \tag{11}$$

where a_i and r are integers and $0 \leq a_i \leq p-1$.

Proof. We first suppose that $x=0$ and x has the expansion (11). Let $r \in Z$ be the smallest integer such that $a_r \neq 0$. For a Z such that $0 \leq a \leq p-1$, $|a| = 1$ because $(a,p) = 1$. Also for integers m and n such that $m < n$, $|p^m| = (1/p)^m > (1/p)^n = |p^n|$.

Hence $0 = |x| = |\sum_{i=r}^{\infty} a_i p^i| \leq \max_{i \geq r}\{|p^i|\} = p^{-r}$. But $p^{-r} \neq 0$ for all $r \in Z$. Hence $a_r = 0$ and so $a_i = 0$ for all i.

Now suppose $x \neq 0$. Then $x \in \hat{Q}^*$, the multiplicative group of $\hat{Q}$. By Proposition 8, we have $|\hat{Q}^*| = |Q^*| = \{|p^n|: n \in Z\}$. Hence $|x| = |p^r|$ for some $r \in Z$. Set $y = xp^{-r}$. Then $|y| = 1$. By the above remarks, $y \in \hat{V}$. By Proposition 7, there is a sequence $\{c_n\}$ in Q such that $c_n \to y$. That is, there is an s sufficiently large so that $|c_s - y| < 1$. Then $|c_s| = |y+(c_s-y)| \leq \max\{|y|, |c_s-y|\} = 1$. Thus $c_s \in V$. Set $c_s = b_r$. We now have $y - b_r \in P$. We may also write $b_r = e/d$, $e, d \in Z$ and $(e,p) = (d,p) = 1$. Then there exist $u, v \in Z$ such that $ud+vp = 1$. Hence $ud \equiv 1 (p)$ or, by the remark above, $ud \equiv 1 (\text{mod } P)$. Now $b_r - eu = \frac{e}{d} - eu = \frac{e(1-du)}{d} \equiv 0 (\text{mod } P)$. Thus $b_r - eu \in P$ or $b_r - eu \in \hat{P}$. Let $a_r = eu \in Z$. Then $|a_r - y| \leq \max\{|a_r - b_r|, |b_r - y|\} < 1$. So $|a_r p^r - yp^r| = |p^r||a_r - y| < |p^r|$. We then get $x = yp^r = a_r p^r + g_1$, $|g_1| < |p^r|$. But then $|g_1| = |p^m|$, some $m > r$. Reiterating the above construction, we find $g_1 = a_m p^m + g_2$, $|g_2| < |p^m|$. Continuing in this way, after the kth step one has

$$(12) \quad x = a_r p^r + a_{r+1} p^{r+1} + \ldots + a_{r+k} p^{r+k} + g_{k+1},$$

where $a_i \in Z$ with the "gaps" being filled by setting some of the a's = 0 if necessary and $|g_{k+1}| < |p^{r+k+1}|$. But as $k \to \infty$, $|p^{r+k+1}| \to 0$. Hence by the corollary to Proposition 10, the partial sums (12) converge with limit x. That is, $x = \sum_{i=r}^{\infty} a_i p^i$, $a_i \in Z$. Suppose $a_r \geq p$. Then $a_r = a_r' + p^t$, $a_r \leq p-1$, $t \geq 0$.

It is clear that we can do this inductively, so that we may write x in the form (11).

To show the uniqueness of (11), we suppose there are two such expressions, $x = \sum_{i=r}^{\infty} a_i p^i = \sum_{i=s}^{\infty} a_i p^i$. Let q be the smallest integer for which $a_i \neq b_i$. Then $\sum_{i=q}^{\infty} (a_i - b_i)p^i = 0$. By paragraph one of this proof, we have $a_i - b_i = 0$ for all i. Hence $a_i = b_i$ for each i. This completes the proof.

We shall call (11) the <u>canonical representation</u> of x. It enables us to deduce

<u>Proposition 13</u>. $\hat{Q}$ is uncountably infinite.

Proof. First, $\hat{Q}$ is at least countably infinite, since $\hat{Q}$ contains the rational field, By Proposition 12, each $x \in \hat{Q}$ has unique representation (11). We shorten this to the p-ary notation:

(13) $\quad x = a_r a_{r+1} a_{r+2} \ldots, \quad 0 \leq a_i \leq p-1.$

Suppose $r \geq 0$. Then $|x| = |p^r| \leq 1$, and thus $x \in \hat{V}$. Conversely, $x \in V$ implies $r \geq 0$. Thus every element in V can be expressed as in (13) by $a_0 a_1 a_2 \ldots$

We now show $\hat{V}$ is uncountable. Suppose $\hat{V}$ is countable and its elements have been listed as a sequence $x_1, x_2, x_3, \ldots$ Let $x_i = a_0^i a_1^i a_2^i \ldots$, where the superscripts denote the sequential position. If $a_0^1 \neq 0$, let $a_0^* = 0$; otherwise, let $a_0^* = 1$. If $a_1^2 \neq 0$, let $a_1^* = 0$; otherwise, let $a_1^* = 1$. Continuing indefinitely in this fashion, we get an element $y = a_0^* a_1^* a_2^* \ldots$ that is not in the list $x_1, x_2, \ldots$ But clearly $y \in \hat{V}$. Hence $\hat{V}$ and also $\hat{Q}$ are uncountable.

TWO: TOPOLOGICAL STRUCTURE OF $\hat{Q}$

In this chapter we discuss some of the topological properties of certain subsets of the metric space Q constructed in section 1.5. Section 2.1 contains results concerning the valuation ring of $\hat{Q}$. Later we discuss more general sets in $\hat{Q}$.

2.1 STRUCTURE OF $\hat{V}$.

As before, we let $\hat{V}$ be the valuation ring of $\hat{Q}$, defined in 1.6. If S is a set in a topological space T, we denote by $\bar{S}$, the <u>closure</u> of S in T, the set S together with the set of all its accumulation points. We then have

<u>Lemma 1</u>. Let V be the valuation ring of Q. Then $\bar{V} = \hat{V}$.

Proof. By the remarks in section 1.6, V is contained in $\hat{V}$. Suppose $x \in \bar{V}-V$. Then x is an accumulation point of V. Hence there is a sequence $\{x_n\}$ in V such that $x_n \to x$. Thus $|x| = |x_n+(x-x_n)| \leq \max\{|x_n|, |x-x_n|\} = x_n$ for large enough n. But $|x_n| \leq 1$ for all n. Hence $|x| \leq 1$. It follows that $x \in \hat{V}$, and so $\bar{V}$ is contained in $\hat{V}$.

Suppose next that $x \in \hat{V}$. Then there is a sequence $\{x_n\}$ in Q such that $x_n \to x$. Suppose $|x_n| > 1$ for just finitely many n. Then for n sufficiently large $|x_n| \leq 1$. Hence for sufficently large n, $x_n \in V$. Thux $x \in \bar{V}$. Now suppose $|x_n| > 1$ for infinitely many n. Then $\{x_n\}$ has a subsequence $\{x_{n_i}\}$ such that $|x_{n_i}| > 1$ for eac i. But also $x_{n_i} \to x$.

Hence for i sufficiently large, $|x_{n_i}-x| < 1$. Since $|x| \leq 1$, $|x| < |x_{n_i}|$, for all i. Thus, for each i, $|x_{n_i}-x| = \max\{|x|, |x_{n_i}|\} > 1$. This is a contradiction of a previous statement. Hence $|x_n| > 1$ for just finitely many n. By the first part of this paragraph, we conclude $x \in \hat{V}$. Thus, $\bar{V} = \hat{V}$.

Definition 9. A set S in a metric space M is totally bounded iff, given $\varepsilon>0$, there is a finite set $\{a_1, a_2, \ldots, a_n\}$ in S such that for each $x \in S$ $|x-a_i| < \varepsilon$ for some a_i. The set $\{a_i: i=1,2,\ldots,m\}$ is an ε-net for S.

Lemma 2. $\hat{V}$ is totally bounded.

Proof. We claim first that, with the notation of 1.5, $|\hat{V}| = |V|$. By Lemma 1, V is dense in $\hat{V}$. Let $x \in \hat{V}$. Then there is a sequence $\{a_n\}$ in V such that $a_n \to x$. Hence $|x| \leq \max\{|x-a_n|, |a_n|\} = |a_n|$ for sufficiently large n. Thus $|\hat{V}| = |V|$. The total boundedness of V therefore implies that of $\hat{V}$.

We now show V is totally bounded. Let $\varepsilon>0$ be given. Then there exists an N>0 such that $\left(\frac{1}{p}\right)^n < \varepsilon$ for all n>N. By Proposition 13, each element of V can be expressed uniquely as $\sum_{i=0}^{\infty} a_i p^i$, $0 \leq a_i \leq p-1$. Consider the set of all such sums such that $a_i = 0$ for i>N. There are no more than p^{N+1} such sums. Denote this set of elements by $B = \{b_s: s = 1,2,\ldots,p^{N+1}\}$. Let y be any point in V, and suppose

$|y| \leq \left(\frac{1}{p}\right)^{N+1}$. Then $|y-0| = |y| < \varepsilon$. Next suppose $|y| > (1/p)^{N+1}$. Then $y = b_s + \sum_{i \geq N+1}^{\infty} a_i p^i$, for some $b_s \varepsilon B$. Hence $|y-b_s| = |\sum_{i=N} a_i p^i| = (1/p)^{N+1} < \varepsilon$. Let $b_0 = 0$. Then the set $\{b_s : s = 0,1,2,\ldots,p^{N+1}\}$ is an ε-net for V. Thus V, and hence $\hat{V}$, is totally bounded.

Theorem 1. $\hat{V}$ is compact.

Proof. By Lemma 2, $\hat{V}$ is totally bounded. By Lemma 1, $\hat{V}$ is closed. Since $\hat{Q}$ is complete, $\hat{V}$ is complete by A2. [A1, A , etc., refer to results cited in the Appendix.] Thus, by A3, $\hat{V}$ is compact.

Definition 10. A set A is totally disconned iff for each pair $x,y \varepsilon A$, $x \neq y$, there exist open sets S and T such that $x \varepsilon S$, $y \varepsilon T$; $S,T \neq \emptyset$; $S \cap T = \emptyset$; and A is contained in $S \cup T$.

Theorem 2. V is totally disconnected.

Proof. Suppose $x,y \varepsilon V$ and $x \neq y$. Since $\hat{V}$ is clearly a subspace of $\hat{Q}$, $\hat{V}$ is a Hausdorff space. Hence, by definition, there are open spheres $S(r;x)$ and $S(q;y)$ such that $S(r;x) \cap S(q;y) = \emptyset$. Suppose $r<q$. Then it is evident that $S(r;x) \cap S(r;y) = \emptyset$. By Theorem 1, there are a finite number of distinct open spheres S_i of radius r covering $\hat{V}$. By Proposition 3, we may assume $S_1 = S(r;x)$. Suppose $S_i \cap S_j$ is not empty for $i \neq j$. Let z be in this intersection. Then, again by Proposition 3, $S_i = S(r;z) = S_j$. Hence $i = j$, contrary to assumption. The spheres S_i

are thus pairwise disjoint and $y \in \bigcup_{i \neq 1} S_i$. Write $S=S_1$ and $T = \bigcup_{i>1} S_i$. Then, by Proposition 2, S and T are both open. By the above remarks $S \cap T = \emptyset$. Also $\hat{V}$ is contained in $S \cup T$. Since x and y were arbitrary in $\hat{V}$, $\hat{V}$ is totally disconnected by Definition 2.

2.2 MORE GENERAL SETS

Theorem 3. Any open sphere in $\hat{Q}$ is also closed.

Proof. Let $S = S(r;a)$ be any open sphere in Q. Let x be an accumulation point of S. Then we can find a sequence $\{a_n\}$ in S such that $a_n \to x$. For all n, $|a-a_n|<r$; so we have $|x-a| \leq \max\{|x-a_n|, |a_n-a|\} = |a_n-a|<r$ for large enough n. Thus $x \in S$. By Definition 4, S is closed.

From Theorem 3 we obtain

Theorem 4. $\hat{Q}$ is totally disconnected.

Proof. Let x and y be any two distinct points in $\hat{Q}$. Then there exists an open sphere $S(r;x)$ in $\hat{Q}$ such that $y \notin S(r;x)$. By Theorem 3, $S(r;x)$ is closed. Hence $S(r;x)^c$, the complement of $S(r;x)$ in $\hat{Q}$, is open by A6. But $S(r;x)^c \cap S(r;x) = \emptyset$; both of these sets are nonempty, since $y \in S(r;x)^c$; and Q is contained in their union. Hence, by Definition 10, $\hat{Q}$ is totally disconnected.

Theorem 5. Let $\{O_n\}$ be a descending sequence of open sets in $\hat{Q}$, $O_n \neq \emptyset$; that is, for each n, O_n contains O_{n+1}. Suppose that the diameter of the nth term tends to 0, an $n \to \infty$. Then there exists just one $x \in \bigcap_{n=1}^{\infty} O_n$.

Proof. Let $\{O_n\}$ be a descending sequence of open sets in $\hat{Q}$ such that the diameter of the nth set tends to 0. By Proposition 2d., $G_n = \bigcap_{i=1}^{n} O_i$ is an open set for each n. Then, for each n, there is an open sphere S_n contained in G_n. The S_n clearly form a descending sequence such that their diameters satisfy the same condition as the O_n. But by Theorem 3, for each n, S_n is closed. Hence, by Cantor's lemma for complete metric spaces (A7), there is a unique element $x \in S_n$ for all n. Hence $x \in O_n$ for all n. Thus $x \in \bigcap_{i=1}^{\infty} O_i$.

Lemma 3. Every open sphere in $\hat{Q}$ is totally bounded.

Proof. Let $S(r;a)$ be an open sphere in $\hat{Q}$ and suppose $|a| = d$. Let $d' = r+d$. Suppose also that $x \in S(r;a)$. Then $|x-a|<r$. Assume $|x|>|a|$. Then $|x| = \max\{|x|,|a|\} = |x-a|<r\leq d'$. Thus $x \in S(d';0)$. Also, $|x| \leq |a|$ implies $|x| < d'$, and so $x \in S(d';0)$. This shows that $S(r;a)$ is contained in $S(d';0)$.

It is easy to see that, with the same procedure as in the proof of Lemma 2, one can show $S(d';0)$ is totally bounded. It is then clear that $S(r;a)$ itself is totally bounded.

Definition 11. A space T is locally compact iff for each $x \in T$ there is an open sphere S containing x such that $\bar{S}$ is compact.

Theorem 6. $\hat{Q}$ is locally compact.

Proof. Let x be any point in $\hat{Q}$. Then, surely, there is an $r > 0$ such that $S(r;x)$ is contained in $\hat{Q}$. By Lemma 3, $S(r;x)$ is totally bounded. By Theorem 3, $S(r;x)$ is closed. Hence, from A2 and the fact that Q is complete, $S(r;x)$ is complete. Thus, by A3, $S(r;x)$ is compact. Definition 11 implies that $\hat{Q}$ is locally compact.

We can see that $\hat{Q}$ itself is not compact as follows. Suppose $\hat{Q}$ were compact. Then every sequence in $\hat{Q}$ would converge. Consider the sequence $\{p^{-n}\}$. Then $p^{-(n+1)}-p^{-n} = p^{-n}(1-p^{-1})$, and so $|p^{-n-1}-p^{-n}| = |p^{-n}| = p^{+n}$, which does not tend to 0, as $n \to \infty$. By Proposition 10, $\{p^{-n}\}$ does not converge. Hence $\hat{Q}$ is not compact.

On the other hand, we have an analogue in $\hat{Q}$ for a compactness criterion in euclidean space. First we need

Definition 12. A set B in a metric space is bounded iff there is an open sphere $S(r;0)$ containing B.

Lemma 4. A set S in $\hat{Q}$ is complete and totally bounded iff it is closed and bounded.

Proof. Suppose the set S in $\hat{Q}$ is complete and totally bounded. Let x and y be any two elements of S. Then, given $\varepsilon > 0$, there is an ε-net $\{a_i\}$ for S. Hence,

$$|x-y| \leq \max\{|x-a_i|, |a_i-a_j|, |a_j-y|\}, \text{ for } i \neq j,$$

$$\leq 2\varepsilon + \max\{|a_i-a_j|\}$$

$$\leq 2\varepsilon + \max\{|a_i|\}, \text{ for all } i.$$

Setting $r=2\varepsilon+\max\{|a_i|\}$, we see that S is contained in $S(r;0)$. Hence by Definition 12, S is bounded. Now let y be an accumulation point of S. Then there is a sequence $\{x_n\}$ in S such that $x_n \to y$. By Proposition 5, $\{x_n\}$ is cauchy. Hence, by the definition of completeness, $y \in S$. Thus S is closed.

For the converse, suppose S is closed and bounded. Then, by A2, S is complete. By Definition 12, there is an $r>0$ such that $S(r;0)$ contains S. But by the proof of Lemma 3, $S(r;0)$ is totally bounded. Hence, so is S.

We can now derive

Theorem 7. A set A in $\hat{Q}$ is compact iff A is closed and bounded.

Proof. Let A be a subset of $\hat{Q}$. Then, by A3, A is compact iff A is complete and totally bounded. Thus, by Lemma 4, A is compact iff it is closed and bounded.

It is evident that the proof of Theorem 1 could have been deferred until now and Lemma 1 is redundant. But the force of Theorem 7 may be used to show the following

Corollary. Let $\hat{U}$ and $\hat{P}$ denote, respectively, the group of units and the maximal ideal of $\hat{V}$, the valuation ring of $\hat{Q}$. Then $\hat{U}$ and $\hat{P}$ are compact.

Proof. By the same kind of argument as the proof of Lemma 1, $\hat{U}$ and $\hat{P}$ are closed. Since $x\varepsilon P$ iff $|x|<1$, $\hat{P}$ is bounded. Thus $\hat{P}$ is compact by Theorem 7. Also $x\varepsilon\hat{U}$ iff $|x| = 1$. So $\hat{U}$ is bounded, and hence compact, again by Theorem 7.

2.3 EXTENSIONS

In this section we want to extend our results to finite field extensions of $\hat{Q}$. For this we need

Definition 13. Let V be a linear space over the field k, and $|\cdot|$ a valuation on k. Let $N: V\to R^{+}$. Then V is called a normed linear space over k iff for all $x,y\varepsilon V$ and $a \varepsilon k$

N1. $N(x) = 0$ iff $x = 0$.

N2. $N(x+y) \leq N(x) + N(y)$.

N3. $N(ax) = |a|N(x)$.

For $x \varepsilon V$, $N(x)$ is called the norm of x.

We want to point out first that any linear space V over a field k having valuation $|\cdot|$ can be normed. Given a fixed basis $x_1,x_2,\ldots,x_n$ for V, each $x \varepsilon V$ can be uniquely written

$$x = a_1x_1 + a_2x_2 + \ldots + a_nx_n, \quad a_i \varepsilon k. \tag{1}$$

We set $N_o(x) = \max_i\{|a_i|\}$. It is obvious that N_o satisfies N1 of Definition 13. Suppose $y\varepsilon V$ and $y = \sum_i b_ix_i$. Then $N_o(x+y) = \max_i\{|a_i+b_i|\}\leq\max_i\{|a_i|+|b_i|\}=\max_i\{|a_i|\}+ \max_i\{|b_i|\}=$

$N_o(x) + N_o(y)$. Hence N2 holds for N_o. Let $c \in k$. Then $N_o(cx) = \max_i\{|ca_i|\} = \max_i\{|c||a_i|\} = |c|\max_i\{|a_i|\} = |c|N_o(x)$. Thus N3 holds and N_o is a norm on V. We shall call N_o the canonical norm on V, although N_o depends on the basis $\{x_i\}$. We note also that V is a metric space with metric

$$d(x,y) = N_o(x-y), \quad x,y \in V. \tag{2}$$

We then have

Theorem 8. Let V be a normed linear space over the field k. Let $|\cdot|$ be a valuation on k such that k is $|\cdot|$-complete Then V is N_o-complete.

Proof. We must show that every d-cauchy sequence in V converges (where d is defined in (2)). Let $x_1, x_2, \ldots, x_m$ be a basis for V over k. When each $x \in V$ can be written in the form (1). Let $\{y_n\}$ be a d-cauchy sequence in V. Then, by definition, $d(y_r, y_s) \to 0$, as $r,s \to \infty$. Suppose for each j, $y_j = \sum_{i=1}^{m} a_{ji}x_i$, $a_{ji} \in k$. Then $d(y_r,y_s) = \max_i\{|a_{ri}-a_{si}|\}$, $1 \leq i \leq m$. Hence, for each i, $|a_{ri}-a_{si}| \to 0$, $r,s \to \infty$. That is, the sequence $\{a_{ji}\}$ is cauchy for each i, $1 \leq i \leq m$. Since k is complete, $a_{ji} \to a_i \in k$, as $j \to \infty$, for each i. Set $y = \sum_{i=1}^{m} a_i x_i$. Then $d(y,y_j) = \max\{|a_i - a_{ji}|\} \to 0$, as $j \to \infty$. Thus $y_j \to y$, as $j \to \infty$, and V is N_o-complete.

Definition 14. Two norms N_1 and N_2 on the linear space V are equivalent iff there exist constants $A,B > 0$ such that, for each $x \in V$,

$$AN_1(x) \leq N_2(x) \leq BN_1(x). \tag{3}$$

It is easy to see that, if (3) is satisfied, N_1 and N_2 induce the same topology, for then every sequence in V is N_1-cauchy iff it is N_2-cauchy.

Theorem 9. Let N and N' be norms on V over k, k complete with respect to the valuation $|\cdot|$. Then N and N' are equivalent.

Proof. We show that the norm N is equivalent to the canonical norm N_o. In that case it is clear that any two norms are equivalent.

Let N be any norm on V over k. Choose a basis $x_1,x_2,\ldots,x_n$ for V over k, $|\cdot|$-complete. Each $x \in V$ can be expressed in the form (1). Hence

$$\begin{aligned} N(x) &= N\left(\sum_{i=1}^{n} a_i x_i\right) \\ &\leq \sum_{i=1}^{n} |a_i| N(x_i), \text{ by N1 and N2,} \\ &\leq \max_i\{|a_i|\} \sum_{i=1}^{n} N(x_i) = BN_o(x), \end{aligned}$$

where $B = \sum_i N(x_i)$. Clearly, $B>0$, since $x_i \neq 0$ for at least one i. Thus, for all $x \in V$, $N(x) \leq BN_o(x)$. This shows half the inequality (3).

To prove the other part we proceed by induction on n. Suppose first that the dimension of V over k is n=1 with basis x_1. Then $N(x) = N(ax_1) = |a|N(x_1) = AN_o(x)$, where $A = N(x_1) > 0$. In this case, then, (3) is completely satisfied. Next suppose (3) holds for all subspaces of V of dimension n-1. Hence, by Definition 14, N and N_o are equivalent on the subspaces V_i spanned by the set of n-1 basis elements obtained by deleting the ith element. The V_i are clearly normed linear spaces over k. By Theorem 8, each V_i is complete under both N_o and N. Thus, by A2, for each i, V_i is closed under both norms, since V itself is complete. Now let $T_i = x_i + V_i$, the set of elements in V_i translated by the vector x_i. For each i, the sets T_i and V_i, considered as metric spaces, are obviously isometric. Hence, for each i, T_i is closed.

Now assume that, for some i, $0 \in T_i$. Then there are scalars $a_j \in k$, $j \neq i$, such that $0 = x_i + \sum_{j \neq i} a_j x_j$. This, however, contradicts the linear independence of the basis elements. Hence, for all i, $0 \notin T_i$. So $0 \notin \bigcup_{i=1}^{n} T_i$. Write $T = \bigcup_i T_i$. Then, by A4, T is closed. Further, $\{0\}$ is closed. Thus, by A5, there is an $A>0$ such that A is the distance between $\{0\}$ and T, where distance is taken with respect to N. Thus, for all $y \in T$, $N(y) \geq A$.

Now let x be any nonzero element in V and suppose $x = \sum_i a_i x_i$, $a_i \in k$. Suppose $|a_r| = \max_i\{|a_i|\} = N_o(x)$. Then $a_r^{-1}x = a_r^{-1}a_1x_1 + a_r^{-1}a_2x_2 + \ldots + x_r + \ldots + a_r^{-1}a_nx_n$, so

$a_r^{-1}x \in T$. Hence, $N(a_r^{-1}x) \geq A$, and so, by N3, $N(x) \geq |a_r|A = N_o(x)A$. This completes the proof.

Definition 15. Let E be an extension field of the field k, having valuation v. Then v' is an extension of v to E iff v' is a valuation on E such that $v'(a) = v(a)$ for all $a \in k$.

Theorem 10. Let E be a finite extension field of the field k, complete under the valuation v. Let v' be an extension of v to E. Then

(4) E is complete under v' and

(5) v' is unique on E.

Proof. Let E be a finite extension of the field k. Then E may be considered as a vector space over k. Denote the degree of E over k by m. Let v' be a valuation on E which extends v. Let $x \in E$ and $a \in k$. Then $ax \in E$ and $v'(ax) = v'(a)v'(x) = v(a)v'(x)$. Thus N3 holds for v'. Since v' is a valuation, N1 and N2 are also satisfied. Hence v' is a norm on E. Hence, by Theorem 8, E is v'-complete.

For (5) we introduce the norm mapping from E into k: if $x \in E$, we let $N_{E\to k}(x) = n(x)$. Again, each $x \in E$ has the representation (1). Also, for $r \in Z$, $x^r = \sum_i a_{ri}x_i$, $a_{ri} \in k$. Suppose $v'(x) < 1$. Then $v'(x^r) = v'(x)^r \to 0$, as $r\to\infty$. So $x^r \to 0$, as $r\to\infty$. Since $n(x)$ is the product of all conjugates of x in E, $n(x)$ is a continuous mapping. Thus, as $r\to\infty$, $n(x^r)\to 0$. Clearly, then, $v(n(x^r))\to 0$. By the multiplicative properties of v and n, $v(n(x))^r \to 0$, as $r\to\infty$.

Thus $v(n(x)) < 1$.

Suppose next that $v'(x) > 1$. Then $1 > v'(x)^{-1} = v'(x^{-1})$. Hence, by the above remarks, $v(n(x^{-1})) < 1$, and so $v(n(x)) > 1$. From this and the last paragraph, we deduce

(6) $\qquad v'(x) = 1$ iff $v(n(x)) = 1$.

Now suppose $x \in E$ and $x \neq 0$. Set $y = n(x)/x^m$. Clearly, $y \in E$. Thus, by the properties of n, $n(y) = n(n(x)x^{-m}) = n(n(x))n(x)^{-m} = 1$. Hence, since v is a valuation, $v(n(y)) = 1$. By (6), $v'(y) = 1$. We then have $v'(x)^m = v'(n(x)) = v(n(x))$. Taking mth roots, $v'(x) = \sqrt[m]{v(n(x))}$. This shows v' is unique on E.

Remark. We note here that v' is unique only if the ground field k is complete. In the general case the number of extensions of the valuation on k is bounded by the degree of the extension [E:k]. The existence of such extensions can be established in various ways. In the situation where the ground field is complete, one may proceed via Hensel's Lemma [6;47]. In the more general case, one can use the theory of places [2;119]. It should be further remarked that an extension of an archimedean valuation is always unique since the only "archimedean" extension fields are isomorphic to subfields of the complex field [6]. These developments are beyond the scope of this paper.

Now let K be a finite extension of the field $\hat{Q}$, and let $|\cdot|_1$ be an extension to K of the p-adic valuation $|\cdot|$

on $\hat{Q}$. Then $|\cdot|_1$ must be nonarchimedean; for, if $|\cdot|_1$ were archimedean, then $|\cdot|$ would be archimedean on $\hat{Q}$, which is nonsense. Thus K has a valuation ring V' and V' has maximal ideal P'. We claim that $\hat{V}$, the valuation ring of $\hat{Q}$, is $V' \cap Q$. Suppose $x \in \hat{V}$. Then $x \in \hat{Q}$ and surely $x \in V'$, so $x \in V' \cap Q$. Conversely, $x \in V' \cap \hat{Q}$ implies $x \in \hat{Q}$ and $|x|_1 = |x| \leq 1$. Hence $x \in \hat{V}$. We have for ideals the analogous equation $P = P' \cap Q$. In this case we say P' lies above $\hat{P}$. Furthermore,

Theorem 11. Let K be a finite extension of Q such that $|\cdot|_1$ extends $|\cdot|$ to K. Then

(7) K is locally compact and

(8) Any set S in K is compact iff S is closed and bounded.

Proof. By Theorem 10, K is complete under the valuation $|\cdot|_1$. Hence (7) and (8) are clear from the development in 2.2.

2.4 TOPOLOGIES INDUCED BY DISTINCT PRIMES

In this last section we show that each prime p induces a distinct topology. We suppose that p and q are distinct primes and denote the p-adic valuation induced by each $|\cdot|_p$ and $|\cdot|_q$ respectively. By Proposition 7, we have the existence of completions Q_p and Q_q under $|\cdot|_p$ and $|\cdot|_q$ respectively.

Theorem 12. The topologies on Q_p and Q_q are distinct, provided $p \neq q$.

Proof. Let p and q be distinct primes. Then, by the

construction in section 1.5, Q_p and Q_q exist. Both contain Q as rational subfield. Consider the sequence $\{p^n\}$ in Q. Thus $\{p^n\}$ is in Q_p and Q_q. Hence $|p^n|_p = |p|_p^n \to 0$, as $n \to \infty$. Since q does not divide p, $|p|_q = 1$. Hence, for all n, $|p|_q^n = |p^n|_q = 1$. Thus Q_p and Q_q are topologically distinct.

We conclude then, that for each prime p there exists a distinct completion of the rationals under the p-adic valuation $|\cdot|_p$.

REFERENCES

1. Ahlfors, Lars V., Complex Analysis, McGraw-Hill, New York, 1966.
2. Bachman, George, Introduction to p-Adic Numbers and Valuation Theory, Academic Press, New York, 1964.
3. Lang, Serge, Algebraic Numbers, Addison-Wesley, Reading, Mass., 1964.
4. Simmons, George F., Introduction to Topology and Modern Analysis, McGraw-Hill, New York, 1963.
5. Van der Waerden, B. L., Modern Algebra, vol. I, Frederick Ungar, New York, 1953.
6. Weiss, Edwin, Algebraic Number Theory, McGraw-Hill, New York, 1963.