CHAPTER XII

Absolute Values

§1. DEFINITIONS, DEPENDENCE, AND INDEPENDENCE

Let K be a field. An **absolute value** v on K is a real-valued function $x \mapsto |x|_v$ on K satisfying the following three properties:

AV 1. We have $|x|_v \geqq 0$ for all $x \in K$, and $|x|_v = 0$ if and only if $x = 0$.

AV 2. For all $x, y \in K$, we have $|xy|_v = |x|_v |y|_v$.

AV 3. For all $x, y \in K$, we have $|x + y|_v \leqq |x|_v + |y|_v$.

If instead of **AV 3** the absolute value satisfies the stronger condition

AV 4. $|x + y|_v \leqq \max(|x|_v, |y|_v)$

then we shall say that it is a **valuation**, or that it is non-archimedean.

The absolute value which is such that $|x|_v = 1$ for all $x \neq 0$ is called **trivial**.

We shall write $|x|$ instead of $|x|_v$ if we deal with just one fixed absolute value. We also refer to v as the absolute value.

An absolute value of K defines a metric. The distance between two elements x, y of K in this metric is $|x - y|$. Thus an absolute value defines a topology on K. Two absolute values are called **dependent** if they define the same topology. If they do not, they are called independent.

We observe that $|1| = |1^2| = |(-1)^2| = |1|^2$ whence

$$|1| = |-1| = 1.$$

Also, $|-x| = |x|$ for all $x \in K$, and $|x^{-1}| = |x|^{-1}$ for $x \neq 0$.

Proposition 1.1. *Let* $|\ |_1$ *and* $|\ |_2$ *be non-trivial absolute values on a field* K. *They are dependent if and only if the relation*

$$|x|_1 < 1$$

implies $|x|_2 < 1$. *If they are dependent, then there exists a number* $\lambda > 0$ *such that* $|x|_1 = |x|_2^{\lambda}$ *for all* $x \in K$.

Proof. If the two absolute values are dependent, then our condition is satisfied, because the set of $x \in K$ such that $|x|_1 < 1$ is the same as the set such that $\lim x^n = 0$ for $n \to \infty$. Conversely, assume the condition satisfied. Then $|x|_1 > 1$ implies $|x|_2 > 1$ since $|x^{-1}|_1 < 1$. By hypothesis, there exists an element $x_0 \in K$ such that $|x_0|_1 > 1$. Let $a = |x_0|_1$ and $b = |x_0|_2$. Let

$$\lambda = \frac{\log b}{\log a}.$$

Let $x \in K, x \neq 0$. Then $|x|_1 = |x_0|_1^{\alpha}$ for some number α. If m, n are integers such that $m/n > \alpha$ and $n > 0$, we have

$$|x|_1 > |x_0|_1^{m/n}$$

whence

$$|x^n/x_0^m|_1 < 1,$$

and thus

$$|x^n/x_0^m|_2 < 1.$$

This implies that $|x|_2 < |x_0|_2^{m/n}$. Hence

$$|x|_2 \leqq |x_0|_2^{\alpha}.$$

Similarly, one proves the reverse inequality, and thus one gets

$$|x|_2 = |x_0|_2^{\alpha}$$

for all $x \in K$, $x \neq 0$. The assertion of the proposition is now obvious, i.e. $|x|_2 = |x|_1^{\lambda}$.

We shall give some examples of absolute values.

Consider first the rational numbers. We have the ordinary absolute value such that $|m| = m$ for any positive integer m.

For each prime number p, we have the p-adic absolute value v_p, defined by the formula

$$|p^r m/n|_p = 1/p^r$$

where r is an integer, and m, n are integers $\neq 0$, not divisible by p. One sees at once that the p-adic absolute value is non-archimedean.

One can give a similar definition of a valuation for any field K which is the quotient field of a principal ring. For instance, let $K = k(t)$ where k is a field and t is a variable over k. We have a valuation v_p for each irreducible polynomial $p(t)$ in $k[t]$, defined as for the rational numbers, but there is no way of normalizing it in a natural way. Thus we select a number c with $0 < c < 1$ and for any rational function $p^r f/g$ where f, g are polynomials not divisible by p, we define

$$|p^r f/g|_p = c^r.$$

The various choices of the constant c give rise to dependent valuations.

Any subfield of the complex numbers (or real numbers) has an absolute value, induced by the ordinary absolute value on the complex numbers. We shall see later how to obtain absolute values on certain fields by embedding them into others which are already endowed with natural absolute values.

Suppose that we have an absolute value on a field which is bounded on the prime ring (i.e. the integers $\mathbf{Z}$ *if the characteristic is* 0, *or the integers* mod p *if the characteristic is* p). *Then the absolute value is necessarily non-archimedean.*

Proof. For any elements x, y and any positive integer n, we have

$$|(x + y)^n| \leqq \sum \left| \binom{n}{v} x^v y^{n-v} \right| \leqq nC \max(|x|, |y|)^n.$$

Taking n-th roots and letting n go to infinity proves our assertion. We note that this is always the case in characteristic > 0 because the prime ring is finite!

If the absolute value is archimedean, then we refer the reader to any other book in which there is a discussion of absolute values for a proof of the fact that it is dependent on the ordinary absolute value. This fact is essentially useless (and is never used in the sequel), because we always start with a concretely given set of absolute values on fields which interest us.

In Proposition 1.1 we derived a strong condition on dependent absolute values. We shall now derive a condition on independent ones.

Theorem 1.2. (Approximation Theorem). (Artin-Whaples). *Let K be a field and $|\ |_1, \ldots, |\ |_s$ non-trivial pairwise independent absolute values on K. Let $x_1, \ldots, x_s$ be elements of K, and $\epsilon > 0$. Then there exists $x \in K$ such that*

$$|x - x_i|_i < \epsilon$$

for all i.

Proof. Consider first two of our absolute values, say v_1 and v_2. By hypothesis we can find $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_s \geqq 1$. Similarly, we can find $\beta \in K$ such that $|\beta|_1 \geqq 1$ and $|\beta|_s < 1$. Put $y = \beta/\alpha$. Then $|y|_1 > 1$ and $|y|_s < 1$.

We shall now prove that there exists $z \in K$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, s$. We prove this by induction, the case $s = 2$ having just been proved. Suppose we have found $z \in K$ satisfying

$$|z|_1 > 1 \quad \text{and} \quad |z|_j < 1 \qquad \text{for} \quad j = 2, \ldots, s-1.$$

If $|z|_s \leqq 1$ then the element $z^n y$ for large n will satisfy our requirements.

If $|z|_s > 1$, then the sequence

$$t_n = \frac{z^n}{1 + z^n}$$

tends to 1 at v_1 and v_s, and tends to 0 at $v_j (j = 2, \ldots, s-1)$. For large n, it is then clear that $t_n y$ satisfies our requirements.

Using the element z that we have just constructed, we see that the sequence $z^n/(1 + z^n)$ tends to 1 at v_1 and to 0 at v_j for $j = 2, \ldots, s$. For each $i = 1, \ldots, s$ we can therefore construct an element z_i which is very close to 1 at v_i and very close to 0 at v_j $(j \neq i)$. The element

$$x = z_1 x_1 + \cdots + z_s x_s$$

then satisfies the requirement of the theorem.

§2. COMPLETIONS

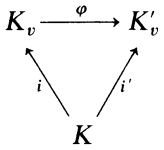
Let K be a field with a non-trivial absolute value v, which will remain fixed throughout this section. One can then define in the usual manner the notion of a Cauchy sequence. It is a sequence $\{x_n\}$ of elements in K such that, given $\epsilon > 0$, there exists an integer N such that for all $n, m > N$ we have

$$|x_n - x_m| < \epsilon.$$

We say that K is **complete** if every Cauchy sequence converges.

Proposition 2.1. *There exists a pair (K_v, i) consisting of a field K_v, complete under an absolute value, and an embedding $i : K \to K_v$ such that the absolute value on K is induced by that of K_v (i.e. $|x|_v = |ix|$ for $x \in K$), and such that iK is dense in K_v. If (K_v', i') is another such pair, then there exists a unique*

isomorphism $\varphi : K_v \to K'_v$ *preserving the absolute values, and making the following diagram commutative:*



Proof. The uniqueness is obvious. One proves the existence in the well-known manner, which we shall now recall briefly, leaving the details to the reader.

The Cauchy sequences form a ring, addition and multiplication being taken componentwise.

One defines a null sequence to be a sequence $\{x_n\}$ such that $\lim_{n\to\infty} x_n = 0$. The null sequences form an ideal in the ring of Cauchy sequences, and in fact form a maximal ideal. (If a Cauchy sequence is not a null sequence, then it stays away from 0 for all n sufficiently large, and one can then take the inverse of almost all its terms. Up to a finite number of terms, one then gets again a Cauchy sequence.)

The residue class field of Cauchy sequences modulo null sequences is the field K_v. We embed K in K_v "on the diagonal", i.e. send $x \in K$ on the sequence $(x, x, x, \ldots)$.

We extend the absolute value of K to K_v by continuity. If $\{x_n\}$ is a Cauchy sequence, representing an element ξ in K_v, we define $|\xi| = \lim |x_n|$. It is easily proved that this yields an absolute value (independent of the choice of representative sequence $\{x_n\}$ for ξ), and this absolute value induces the given one on K.

Finally, one proves that K_v is complete. Let $\{\xi_n\}$ be a Cauchy sequence in K_v. For each n, we can find an element $x_n \in K$ such that $|\xi_n - x_n| < 1/n$. Then one verifies immediately that $\{x_n\}$ is a Cauchy sequence in K. We let ξ be its limit in K_v. By a three-ϵ argument, one sees that $\{\xi_n\}$ converges to ξ, thus proving the completeness.

A pair (K_v, i) as in Proposition 2.1 may be called a **completion** of K. The standard pair obtained by the preceding construction could be called **the completion** of K.

Let K have a non-trivial archimedean absolute value v. If one knows that the restriction of v to the rationals is dependent on the ordinary absolute value, then the completion K_v is a complete field, containing the completion of $\mathbf{Q}$ as a closed subfield, i.e. containing the real numbers $\mathbf{R}$ as a closed subfield. It will be worthwhile to state the theorem of Gelfand-Mazur concerning the structure of such fields. First we define the notion of normed vector space.

Let K be a field with a non-trivial absolute value, and let E be a vector space over K. By a **norm** on E (compatible with the absolute value of K) we shall mean a function $\xi \to |\xi|$ of E into the real numbers such that:

NO 1. $|\xi| \geqq 0$ for all $\xi \in E$, and $= 0$ if and only if $\xi = 0$.

NO 2. For all $x \in K$ and $\xi \in E$ we have $|x\xi| = |x||\xi|$.

NO 3. If $\xi, \xi' \in E$ then $|\xi + \xi'| \leqq |\xi| + |\xi'|$.

Two norms $|\ |_1$ and $|\ |_2$ are called **equivalent** if there exist numbers $C_1, C_2 > 0$ such that for all $\xi \in E$ we have

$$C_1|\xi|_1 \leqq |\xi|_2 \leqq C_2|\xi|_1.$$

Suppose that E is finite dimensional, and let $\omega_1, \ldots, \omega_n$ be a basis of E over K. If we write an element

$$\xi = x_1\omega_1 + \cdots + x_n\omega_n$$

in terms of this basis, with $x_i \in K$, then we can define a norm by putting

$$|\xi| = \max_i |x_i|.$$

The three properties defining a norm are trivially satisfied.

Proposition 2.2. *Let K be a complete field under a non-trivial absolute value, and let E be a finite-dimensional space over K. Then any two norms on E (compatible with the given absolute value on K) are equivalent.*

Proof. We shall first prove that the topology on E is that of a product space, i.e. if $\omega_1, \ldots, \omega_n$ is a basis of E over K, then a sequence

$$\xi^{(v)} = x_1^{(v)}\omega_1 + \cdots + x_n^{(v)}\omega_n, \qquad x_i^{(v)} \in K,$$

is a Cauchy sequence in E only if each one of the n sequences $x_i^{(v)}$ is a Cauchy sequence in K. We do this by induction on n. It is obvious for $n = 1$. Assume $n \geqq 2$. We consider a sequence as above, and without loss of generality, we may assume that it converges to 0. (If necessary, consider $\xi^{(v)} - \xi^{(\mu)}$ for $v, \mu \to \infty$.) We must then show that the sequences of the coefficients converge to 0 also. If this is not the case, then there exists a number $a > 0$ such that we have for some j, say $j = 1$,

$$|x_1^{(v)}| > a$$

for arbitrarily large v. Thus for a subsequence of (v), $\xi^{(v)}/x_1^{(v)}$ converges to 0, and we can write

$$\frac{\xi^{(v)}}{x_1^{(v)}} - \omega_1 = \frac{x_2^{(v)}}{x_1^{(v)}}\omega_2 + \cdots + \frac{x_n^{(v)}}{x_1^{(v)}}\omega_n.$$

We let $\eta^{(v)}$ be the right-hand side of this equation. Then the subsequence $\eta^{(v)}$ converges (according to the left-hand side of our equation). By induction, we

conclude that its coefficients in terms of $\omega_2, \ldots, \omega_n$ also converge in K, say to $y_2, \ldots, y_n$. Taking the limit, we get

$$\omega_1 = y_2\omega_2 + \cdots + y_n\omega_n,$$

contradicting the linear independence of the ω_i.

We must finally see that two norms inducing the same topology are equivalent. Let $|\ |_1$ and $|\ |_2$ be these norms. There exists a number $C > 0$ such that for any $\xi \in E$ we have

$$|\xi|_1 \leqq C \quad \text{implies} \quad |\xi|_2 \leqq 1.$$

Let $a \in K$ be such that $0 < |a| < 1$. For every $\xi \in E$ there exists a unique integer s such that

$$C|a| < |a^s\xi|_1 \leqq C.$$

Hence $|a^s\xi|_2 \leqq 1$ whence we get at once

$$|\xi|_2 \leqq C^{-1}|a|^{-1}|\xi|_1.$$

The other inequality follows by symmetry, with a similar constant.

Theorem 2.3. (Gelfand-Mazur). *Let A be a commutative algebra over the real numbers, and assume that A contains an element j such that $j^2 = -1$. Let $\mathbf{C} = \mathbf{R} + \mathbf{R}j$. Assume that A is normed (as a vector space over $\mathbf{R}$), and that $|xy| \leqq |x|\,|y|$ for all $x, y \in A$. Given $x_0 \in A$, $x_0 \neq 0$, there exists an element $c \in \mathbf{C}$ such that $x_0 - c$ is not invertible in A.*

Proof. (Tornheim). Assume that $x_0 - z$ is invertible for all $z \in \mathbf{C}$. Consider the mapping $f : \mathbf{C} \to A$ defined by

$$f(z) = (x_0 - z)^{-1}.$$

It is easily verified (as usual) that taking inverses is a continuous operation. Hence f is continuous, and for $z \neq 0$ we have

$$f(z) = z^{-1}(x_0 z^{-1} - 1)^{-1} = \frac{1}{z}\left(\frac{1}{\dfrac{x_0}{z} - 1}\right).$$

From this we see that $f(z)$ approaches 0 when z goes to infinity (in $\mathbf{C}$). Hence the map $z \mapsto |f(z)|$ is a continuous map of $\mathbf{C}$ into the real numbers $\geqq 0$, is bounded, and is small outside some large circle. Hence it has a maximum, say M. Let D

be the set of elements $z \in \mathbf{C}$ such that $|f(z)| = M$. Then D is not empty; D is bounded and closed. We shall prove that D is open, hence a contradiction.

Let c_0 be a point of D, which, after a translation, we may assume to be the origin. We shall see that if r is real > 0 and small, then all points on the circle of radius r lie in D. Indeed, consider the sum

$$S(n) = \frac{1}{n} \sum_{k=1}^{n} \frac{1}{x_0 - \omega^k r}$$

where ω is a primitive n-th root of unity. Taking formally the logarithmic derivative of $X^n - r^n = \prod_{k=1}^{n} (X - \omega^k r)$ shows that

$$\frac{nX^{n-1}}{X^n - r^n} = \sum_{k=1}^{n} \frac{1}{X - \omega^k r},$$

and hence, dividing by n, and by X^{n-1}, and substituting x_0 for X, we obtain

$$S(n) = \frac{1}{x_0 - r(r/x_0)^{n-1}}.$$

If r is small (say $|r/x_0| < 1$), then we see that

$$\lim_{n \to \infty} |S(n)| = \left| \frac{1}{x_0} \right| = M.$$

Suppose that there exists a complex number λ of absolute value 1 such that

$$\left| \frac{1}{x_0 - \lambda r} \right| < M.$$

Then there exists an interval on the unit circle near λ, and there exists $\epsilon > 0$ such that for all roots of unity ζ lying in this interval, we have

$$\left| \frac{1}{x_0 - \zeta r} \right| < M - \epsilon.$$

(This is true by continuity.) Let us take n very large. Let b_n be the number of n-th roots of unity lying in our interval. Then b_n/n is approximately equal to the length of the interval (times 2π): We can express $S(n)$ as a sum

$$S(n) = \frac{1}{n} \left[\sum_{\mathrm{I}} \frac{1}{x_0 - \omega^k r} + \sum_{\mathrm{II}} \frac{1}{x_0 - \omega^k r} \right],$$

the first sum $\sum_{\text{I}}$ being taken over those roots of unity ω^k lying in our interval, and the second sum being taken over the others. Each term in the second sum has norm $\leqq M$ because M is a maximum. Hence we obtain the estimate

$$|S(n)| \leqq \frac{1}{n}[|\sum_{\text{I}}| + |\sum_{\text{II}}|]$$

$$\leqq \frac{1}{n}(b_n(M - \epsilon) + (n - b_n)M)$$

$$\leqq M - \frac{b_n}{n}\epsilon.$$

This contradicts the fact that the limit of $|S(n)|$ is equal to M.

Corollary 2.4. *Let K be a field, which is an extension of $\mathbf{R}$, and has an absolute value extending the ordinary absolute value on $\mathbf{R}$. Then $K = \mathbf{R}$ or $K = \mathbf{C}$.*

Proof. Assume first that K contains $\mathbf{C}$. Then the assumption that K is a field and Theorem 2.3 imply that $K = \mathbf{C}$.

If K does not contain $\mathbf{C}$, in other words, does not contain a square root of -1, we let $L = K(j)$ where $j^2 = -1$. We define a norm on L (as an $\mathbf{R}$-space) by putting

$$|x + yj| = |x| + |y|$$

for $x, y \in K$. This clearly makes L into a normed $\mathbf{R}$-space. Furthermore, if $z = x + yj$ and $z' = x' + y'j$ are in L, then

$$\begin{aligned} |zz'| &= |xx' - yy'| + |xy' + x'y| \\ &\leqq |xx'| + |yy'| + |xy'| + |x'y| \\ &\leqq |x||x'| + |y||y'| + |x||y'| + |x'||y| \\ &\leqq (|x| + |y|)(|x'| + |y'|) \\ &\leqq |z||z'|, \end{aligned}$$

and we can therefore apply Theorem 2.3 again to conclude the proof.

As an important application of Proposition 2.2, we have:

Proposition 2.5. *Let K be complete with respect to a nontrivial absolute value v. If E is any algebraic extension of K, then v has a unique extension to E. If E is finite over K, then E is complete.*

Proof. In the archimedean case, the existence is obvious since we deal with the real and complex numbers. In the non-archimedean case, we postpone

the existence proof to a later section. It uses entirely different ideas from the present ones. As to uniqueness, we may assume that E is finite over K. By Proposition 2.2, an extension of v to E defines the same topology as the max norm obtained in terms of a basis as above. Given a Cauchy sequence $\xi^{(\nu)}$ in E,

$$\xi^{(\nu)} = x_{\nu 1}\omega_1 + \cdots + x_{\nu n}\omega_n,$$

the n sequences $\{x_{\nu i}\}(i = 1, \ldots, n)$ must be Cauchy sequences in K by the definition of the max norm. If $\{x_{\nu i}\}$ converges to an element z_i in K, then it is clear that the sequence $\xi^{(\nu)}$ converges to $z_1\omega_1 + \cdots + z_n\omega_n$. Hence E is complete. Furthermore, since any two extensions of v to E are equivalent, we can apply Proposition 1.1, and we see that we must have $\lambda = 1$, since the extensions induce the same absolute value v on K. This proves what we want.

From the uniqueness we can get an explicit determination of the absolute value on an algebraic extension of K. Observe first that if E is a normal extension of K, and σ is an automorphism of E over K, then the function

$$x \mapsto |\sigma x|$$

is an absolute value on E extending that of K. Hence we must have

$$|\sigma x| = |x|$$

for all $x \in E$. If E is algebraic over K, and σ is an embedding of E over K in K^a, then the same conclusion remains valid, as one sees immediately by embedding E in a normal extension of K. In particular, if α is algebraic over K, of degree n, and if $\alpha_1, \ldots, \alpha_n$ are its conjugates (counting multiplicities, equal to the degree of inseparability), then all the absolute values $|\alpha_i|$ are equal. Denoting by N the norm from $K(\alpha)$ to K, we see that

$$|N(\alpha)| = |\alpha|^n,$$

and taking the n-th root, we get:

Proposition 2.6. *Let K be complete with respect to a non-trivial absolute value. Let α be algebraic over K, and let N be the norm from $K(\alpha)$ to K. Let $n = [K(\alpha) : K]$. Then*

$$|\alpha| = |N(\alpha)|^{1/n}.$$

In the special case of the complex numbers over the real numbers, we can write $\alpha = a + bi$ with $a, b \in \mathbf{R}$, and we see that the formula of Proposition 2.6 is a generalization of the formula for the absolute value of a complex number,

$$\alpha = (a^2 + b^2)^{1/2},$$

since $a^2 + b^2$ is none other than the norm of α from $\mathbf{C}$ to $\mathbf{R}$.

Comments and examples. The process of completion is widespread in mathematics. The first example occurs in getting the real numbers from the rational numbers, with the added property of ordering. I carry this process out in full in [La 90a], Chapter IX, §3. In all other examples I know, the ordering property does not intervene. We have seen examples of completions of fields in this chapter, especially with the p-adic absolute values which are far away from ordering the field. But the real numbers are nevertheless needed as the range of values of absolute values, or more generally norms.

In analysis, one completes various spaces with various norms. Let V be a vector space over the complex numbers, say. For many applications, one must also deal with a seminorm, which satisfies the same conditions except that in **NO 1** we require only that $\|\xi\| \geqq 0$. We allow $\|\xi\| = 0$ even if $\xi \neq 0$.

One may then form the space of Cauchy sequences, the subspace of null sequences, and the factor space $\overline{V}$. The seminorm can be extended to a seminorm on $\overline{V}$ by continuity, and this extension actually turns out to be a norm. It is a general fact that $\overline{V}$ is then complete under this extension. A **Banach space** is a complete normed vector space.

Example. Let V be the vector space of step functions on $\mathbf{R}$, a step function being a complex valued function which is a finite sum of characteristic functions of intervals (closed, open, or semiclosed, i.e. the intervals may or may not contain their endpoints). For $f \in V$ we define the **L^1-seminorm** by

$$\|f\|_1 = \int_{\mathbf{R}} |f(x)|\, dx.$$

The completion of V with respect to this seminorm is defined to be $L^1(\mathbf{R})$. One then wants to get a better idea of what elements of $L^1(\mathbf{R})$ look like. It is a simple lemma that given an L^1-Cauchy sequence in V, and given $\varepsilon > 0$, there exists a subsequence which converges uniformly except on a set of measure less than ε. Thus elements of $L^1(\mathbf{R})$ can be identified with pointwise limits of L^1-Cauchy sequences in V. The reader will find details carried out in [La 85].

Analysts use other norms or seminorms, of course, and other spaces, such as the space of C^∞ functions on $\mathbf{R}$ with compact support, and norms which may bound the derivatives. There is no end to the possible variations.

Theorem 2.3 and Corollary 2.4 are also used in the theory of Banach algebras, representing a certain type of Banach algebra as the algebra of continuous functions on a compact space, with the Gelfand-Mazur and Gelfand-Naimark theorems. Cf. [Ri 60] and [Ru 73].

Arithmetic example. For p-adic Banach spaces in connection with the number theoretic work of Dwork, see for instance Serre [Se 62], or also [La 90b], Chapter 15.

In this book we limit ourselves to complete fields and their finite extensions.

Bibliography

[La 85] S. LANG, *Real and Functional Analysis*, Springer Verlag, 1993

[La 90a] S. LANG, *Undergraduate Algebra*, Second Edition, Springer Verlag, 1990

[La 90b] S. LANG, *Cyclotomic Fields* I *and* II, Springer Verlag 1990 (combined from the first editions, 1978 and 1980)

[Ri 60] C. RICKART, *Banach Algebras*, Van Nostrand (1960), Theorems 1.7.1 and 4.2.2.

[Ru 73] W. RUDIN, *Functional Analysis*, McGraw Hill (1973) Theorems 10.14 and 11.18.

[Se 62] J. P. SERRE, Endomorphismes complêtement continus des espaces de Banach p-adiques, *Pub. Math. IHES* **12** (1962), pp. 69–85

§3. FINITE EXTENSIONS

Throughout this section we shall deal with a field K having a non-trivial absolute value v.

We wish to describe how this absolute value extends to finite extensions of K. If E is an extension of K and w is an absolute value on E extending v, then we shall write $w|v$.

If we let K_v be the completion, we know that v can be extended to K_v, and then uniquely to its algebraic closure K_v^a. If E is a finite extension of K, or even an algebraic one, then we can extend v to E by embedding E in K_v^a by an isomorphism over K, and taking the induced absolute value on E. We shall now prove that every extension of v can be obtained in this manner.

Proposition 3.1. *Let E be a finite extension of K. Let w be an absolute value on E extending v, and let E_w be the completion. Let K_w be the closure of K in E_w and identify E in E_w. Then $E_w = EK_w$ (the composite field).*

Proof. We observe that K_w is a completion of K, and that the composite field EK_w is algebraic over K_w and therefore complete by Proposition 2.5. Since it contains E, it follows that E is dense in it, and hence that $E_w = EK_w$.

If we start with an embedding $\sigma : E \to K_v^a$ (always assumed to be over K), then we know again by Proposition 2.5 that $\sigma E \cdot K_v$ is complete. Thus this construction and the construction of the proposition are essentially the same, up to an isomorphism. In the future, we take the embedding point of view. We must now determine when two embeddings give us the same absolute value on E.

Given two embeddings $\sigma, \tau : E \to K_v^a$, we shall say that they are **conjugate over K_v** if there exists an automorphism λ of K_v^a over K_v such that $\sigma = \lambda\tau$. We see that actually λ is determined by its effect on τE, or $\tau E \cdot K_v$.

Proposition 3.2. *Let E be an algebraic extension of K. Two embeddings $\sigma, \tau : E \to K_v^a$ give rise to the same absolute value on E if and only if they are conjugate over K_v.*

Proof. Suppose they are conjugate over K_v. Then the uniqueness of the extension of the absolute value from K_v to K_v^a guarantees that the induced absolute values on E are equal. Conversely, suppose this is the case. Let $\lambda : \tau E \to \sigma E$ be an isomorphism over K. We shall prove that λ extends to an isomorphism of $\tau E \cdot K_v$ onto $\sigma E \cdot K_v$ over K_v. Since τE is dense in $\tau E \cdot K_v$, an element $x \in \tau E \cdot K_v$ can be written

$$x = \lim \tau x_n$$

with $x_n \in E$. Since the absolute values induced by σ and τ on E coincide, it follows that the sequence $\lambda \tau x_n = \sigma x_n$ converges to an element of $\sigma E \cdot K_v$ which we denote by λx. One then verifies immediately that λx is independent of the particular sequence τx_n used, and that the map $\lambda : \tau E \cdot K_v \to \sigma E \cdot K_v$ is an isomorphism, which clearly leaves K_v fixed. This proves our proposition.

In view of the previous two propositions, if w is an extension of v to a finite extension E of K, then we may identify E_w and a composite extension EK_v of E and K_v. If $N = [E : K]$ is finite, then we shall call

$$N_w = [E_w : K_v]$$

the **local degree**.

Proposition 3.3. *Let E be a finite separable extension of K, of degree N. Then*

$$N = \sum_{w|v} N_w.$$

Proof. We can write $E = K(\alpha)$ for a single element α. Let $f(X)$ be its irreducible polynomial over K. Then over K_v, we have a decomposition

$$f(X) = f_1(X) \cdots f_r(X)$$

into irreducible factors $f_i(X)$. They all appear with multiplicity 1 according to our hypothesis of separability. The embeddings of E into K_v^a correspond to the maps of α onto the roots of the f_i. Two embeddings are conjugate if and only if they map α onto roots of the same polynomial f_i. On the other hand, it is clear that the local degree in each case is precisely the degree of f_i. This proves our proposition.

Proposition 3.4. *Let E be a finite extension of K. Then*

$$\sum_{w|v} [E_w : K_v] \leqq [E : K].$$

If E is purely inseparable over K, then there exists only one absolute value w on E extending v.

Proof. Let us first prove the second statement. If E is purely inseparable over K, and p^r is its inseparable degree, then $\alpha^{p^r} \in K$ for every α in E. Hence v has a unique extension to E. Consider now the general case of a finite extension, and let $F = E^{p^r}K$. Then F is separable over K and E is purely inseparable over F. By the preceding proposition,

$$\sum_{w|v} [F_w : K_v] = [F : K],$$

and for each w, we have $[E_w : F_w] \leqq [E : F]$. From this our inequality in the statement of the proposition is obvious.

Whenever v is an absolute value on K such that for any finite extension E of K we have $[E : K] = \sum_{w|v} [E_w : K_v]$ we shall say that v is **well behaved**. Suppose we have a tower of finite extensions, $L \supset E \supset K$. Let w range over the absolute values of E extending v, and u over those of L extending v. If $u|w$ then L_u contains E_w. Thus we have:

$$\begin{aligned}
\sum_{u|v} [L_u : K_v] &= \sum_{w|v} \sum_{u|w} [L_u : E_w][E_w : K_v] \\
&= \sum_{w|v} [E_w : K_v] \sum_{u|w} [L_u : E_w] \\
&\leqq \sum_{w|v} [E_w : K_v][L : E] \\
&\leqq [E : K][L : E].
\end{aligned}$$

From this we immediately see that if v is well behaved, E finite over K, and w extends v on E, then w is well behaved (we must have an equality everywhere).

Let E be a finite extension of K. Let p^r be its inseparable degree. We recall that the norm of an element $\alpha \in K$ is given by the formula

$$N_K^E(\alpha) = \prod_\sigma \sigma\alpha^{p^r}$$

where σ ranges over all distinct isomorphisms of E over K (into a given algebraic closure).

If w is an absolute value extending v on E, then the norm from E_w to K_v will be called the **local norm**.

Replacing the above product by a sum, we get the trace, and the local trace. We abbreviate the trace by Tr.

Proposition 3.8. *Let E be a finite extension of K, and assume that v is well*

behaved. Let $\alpha \in E$. *Then*:

$$N_K^E(\alpha) = \prod_{w|v} N_{K_v}^{E_w}(\alpha)$$

$$\mathrm{Tr}_K^E(\alpha) = \sum_{w|v} \mathrm{Tr}_{K_v}^{E_w}(\alpha)$$

Proof. Suppose first that $E = K(\alpha)$, and let $f(X)$ be the irreducible polynomial of α over K. If we factor $f(X)$ into irreducible terms over K_v, then

$$f(X) = f_1(X) \cdots f_r(X)$$

where each $f_i(X)$ is irreducible, and the f_i are distinct because of our hypothesis that v is well behaved. The norm $N_K^E(\alpha)$ is equal to $(-1)^{\deg f}$ times the constant term of f, and similarly for each f_i. Since the constant term of f is equal to the product of the constant terms of the f_i, we get the first part of the proposition. The statement for the trace follows by looking at the penultimate coefficient of f and each f_i.

If E is not equal to $K(\alpha)$, then we simply use the transitivity of the norm and trace. We leave the details to the reader.

One can also argue directly on the embeddings. Let $\sigma_1, \ldots, \sigma_m$ be the distinct embeddings of E into K_v^a over K, and let p^r be the inseparable degree of E over K. The inseparable degree of $\sigma E \cdot K_v$ over K_v for any σ is at most equal to p^r. If we separate $\sigma_1, \ldots, \sigma_m$ into distinct conjugacy classes over K_v, then from our hypothesis that v is well behaved, we conclude at once that the inseparable degree of $\sigma_i E \cdot K_v$ over K_v must be equal to p^r also, for each i. Thus the formula giving the norm as a product over conjugates with multiplicity p^r breaks up into a product of factors corresponding to the conjugacy classes over K_v.

Taking into account Proposition 2.6, we have:

Proposition 3.6. *Let* K *have a well-behaved absolute value* v. *Let* E *be a finite extension of* K, *and* $\alpha \in E$. *Let*

$$N_w = [E_w : K_v]$$

for each absolute value w *on* E *extending* v. *Then*

$$\prod_{w|v} |\alpha|_w^{N_w} = |N_K^E(\alpha)|_v.$$

§4. VALUATIONS

In this section, we shall obtain, among other things, the existence theorem concerning the possibility of extending non-archimedean absolute values to algebraic extensions. We introduce first a generalization of the notion of non-archimedean absolute value.

Let Γ be a multiplicative commutative group. We shall say that an **ordering** is defined in Γ if we are given a subset S of Γ closed under multiplication such that Γ is the disjoint union of S, the unit element 1, and the set S^{-1} consisting of all inverses of elements of S.

If $\alpha, \beta \in \Gamma$ we define $\alpha < \beta$ to mean $\alpha\beta^{-1} \in S$. We have $\alpha < 1$ if and only if $\alpha \in S$. One easily verifies the following properties of the relation $<$:

1. For $\alpha, \beta \in \Gamma$ we have $\alpha < \beta$, or $\alpha = \beta$, or $\beta < \alpha$, and these possibilities are mutually exclusive.
2. $\alpha < \beta$ implies $\alpha\gamma < \beta\gamma$ for any $\gamma \in \Gamma$.
3. $\alpha < \beta$ and $\beta < \gamma$ implies $\alpha < \gamma$.

(Conversely, a relation satisfying the three properties gives rise to a subset S consisting of all elements < 1. However, we don't need this fact in the sequel.)

It is convenient to attach to an ordered group formally an extra element 0, such that $0\alpha = 0$, and $0 < \alpha$ for all $\alpha \in \Gamma$. The ordered group is then analogous to the multiplicative group of positive reals, except that there may be non-archimedean ordering.

If $\alpha \in \Gamma$ and n is an integer $\neq 0$, such that $\alpha^n = 1$, then $\alpha = 1$. This follows at once from the assumption that S is closed under multiplication and does not contain 1. In particular, the map $\alpha \mapsto \alpha^n$ is injective.

Let K be a field. By a **valuation** of K we shall mean a map $x \mapsto |x|$ of K into an ordered group Γ, together with the extra element 0, such that:

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

VAL 2. $|xy| = |x||y|$ for all $x, y \in K$.

VAL 3. $|x + y| \leqq \max(|x|, |y|)$.

We see that a valuation gives rise to a homomorphism of the multiplicative group K^* into Γ. The valuation is called **trivial** if it maps K^* on 1. If the map giving the valuation is not surjective, then its image is an ordered subgroup of Γ, and by taking its restriction to this image, we obtain a valuation onto an ordered group, called the **value group**.

We shall denote valuations also by v. If v_1, v_2 are two valuations of K, we shall say that they are **equivalent** if there exists an order-preserving isomorphism λ of the image of v_1 onto the image of v_2 such that

$$|x|_2 = \lambda|x|_1$$

for all $x \in K$. (We agree that $\lambda(0) = 0$.)

Valuations have additional properties, like absolute values. For instance, $|1| = 1$ because $|1| = |1|^2$. Furthermore,

$$|\pm x| = |x|$$

for all $x \in K$. Proof obvious. Also, if $|x| < |y|$ then

$$|x + y| = |y|.$$

To see this, note that under our hypothesis, we have

$$|y| = |y + x - x| \leqq \max(|y + x|, |x|) = |x + y| \leqq \max(|x|, |y|) = |y|.$$

Finally, in a sum

$$x_1 + \cdots + x_n = 0,$$

at least two elements of the sum have the same value. This is an immediate consequence of the preceding remark.

Let K be a field. A subring $\mathfrak{o}$ of K is called a **valuation ring** if it has the property that for any $x \in K$ we have $x \in \mathfrak{o}$ or $x^{-1} \in \mathfrak{o}$.

We shall now see that valuation rings give rise to valuations. Let $\mathfrak{o}$ be a valuation ring of K and let U be the group of units of $\mathfrak{o}$. We contend that $\mathfrak{o}$ is a local ring. Indeed suppose that $x, y \in \mathfrak{o}$ are not units. Say $x/y \in \mathfrak{o}$. Then

$$1 + x/y = (x + y)/y \in \mathfrak{o}.$$

If $x + y$ were a unit then $1/y \in \mathfrak{o}$, contradicting the assumption that y is not a unit. Hence $x + y$ is not a unit. One sees trivially that for $z \in \mathfrak{o}$, zx is not a unit. Hence the nonunits form an ideal, which must therefore be the unique maximal ideal of $\mathfrak{o}$.

Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$ and let $\mathfrak{m}^*$ be the multiplicative system of nonzero elements of $\mathfrak{m}$. Then

$$K^* = \mathfrak{m}^* \cup U \cup \mathfrak{m}^{*-1}$$

is the disjoint union of $\mathfrak{m}^*$, U, and $\mathfrak{m}^{*-1}$. The factor group K^*/U can now be given an ordering. If $x \in K^*$, we denote the coset xU by $|x|$. We put $|0| = 0$. We define $|x| < 1$ (i.e. $|x| \in S$) if and only if $x \in \mathfrak{m}^*$. Our set S is clearly closed under multiplication, and if we let $\Gamma = K^*/U$ then Γ is the disjoint union of S, 1, S^{-1}. In this way we obtain a valuation of K.

We note that if $x, y \in K$ and $x, y \neq 0$, then

$$|x| < |y| \Leftrightarrow |x/y| < 1 \Leftrightarrow x/y \in \mathfrak{m}^*.$$

Conversely, given a valuation of K into an ordered group we let $\mathfrak{o}$ be the subset of K consisting of all x such that $|x| < 1$. It follows at once from the

axioms of a valuation that $\mathfrak{o}$ is a ring. If $|x| < 1$ then $|x^{-1}| > 1$ so that x^{-1} is not in $\mathfrak{o}$. If $|x| = 1$ then $|x^{-1}| = 1$. We see that $\mathfrak{o}$ is a valuation ring, whose maximal ideal consists of those elements x with $|x| < 1$ and whose units consist of those elements x with $|x| = 1$. The reader will immediately verify that there is a bijection between valuation rings of K and equivalence classes of valuations.

The extension theorem for places and valuation rings in Chapter VII now gives us immediately the extension theorem for valuations.

Theorem 4.1. *Let K be a subfield of a field L. Then a valuation on K has an extension to a valuation on L.*

Proof. Let $\mathfrak{o}$ be the valuation ring on K corresponding to the given valuation. Let $\varphi : \mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ be the canonical homomorphism on the residue class field, and extend φ to a homomorphism of a valuation ring $\mathfrak{O}$ of L as in §3 of Chapter VII. Let $\mathfrak{M}$ be the maximal ideal of $\mathfrak{O}$. Since $\mathfrak{M} \cap \mathfrak{o}$ contains $\mathfrak{m}$ but does not contain 1, it follows that $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. Let U' be the group of units of $\mathfrak{O}$. Then $U' \cap K = U$ is the group of units of $\mathfrak{o}$. Hence we have a canonical injection

$$K^*/U \to L^*/U'$$

which is immediately verified to be order-preserving. Identifying K^*/U in L^*/U' we have obtained an extension of our valuation of K to a valuation of L.

Of course, when we deal with absolute values, we require that the value group be a subgroup of the multiplicative reals. Thus we must still prove something about the nature of the value group L^*/U', whenever L is algebraic over K.

Proposition 4.2. *Let L be a finite extension of K, of degree n. Let w be a valuation of L with value group Γ'. Let Γ be the value group of K. Then $(\Gamma' : \Gamma) \leqq n$.*

Proof. Let $y_1, \ldots, y_r$ be elements of L whose values represent distinct cosets of Γ in Γ'. We shall prove that the y_j are linearly independent over K. In a relation $a_1 y_1 + \cdots + a_r y_r = 0$ with $a_j \in K$, $a_j \neq 0$ two terms must have the same value, say $|a_i y_i| = |a_j y_j|$ with $i \neq j$, and hence

$$|y_i| = |a_i^{-1} a_j| |y_j|.$$

This contradicts the assumption that the values of y_i, y_j $(i \neq j)$ represent distinct cosets of Γ in Γ', and proves our proposition.

Corollary 4.3. *There exists an integer $e \geqq 1$ such that the map $\gamma \mapsto \gamma^e$ induces an injective homomorphism of Γ' into Γ.*

Proof. Take e to be the index $(\Gamma' : \Gamma)$.

Corollary 4.4. *If K is a field with a valuation v whose value group is an ordered subgroup of the ordered group of positive real numbers, and if L is an algebraic extension of K, then there exists an extension of v to L whose value group is also an ordered subgroup of the positive reals.*

Proof. We know that we can extend v to a valuation w of L with some value group Γ', and the value group Γ of v can be identified with a subgroup of $\mathbf{R}^+$. By Corollary 4.3, every element of Γ' has finite period modulo Γ. Since every element of $\mathbf{R}^+$ has a unique e-th root for every integer $e \geqq 1$, we can find in an obvious way an order-preserving embedding of Γ' into $\mathbf{R}^+$ which induces the identity on Γ. In this way we get our extension of v to an absolute value on L.

Corollary 4.5. *If L is finite over K, and if Γ is infinite cyclic, then Γ' is also infinite cyclic.*

Proof. Use Corollary 4.3 and the fact that a subgroup of a cyclic group is cyclic.

We shall now strengthen our preceding proposition to a slightly stronger one. We call $(\Gamma' : \Gamma)$ the **ramification index**.

Proposition 4.6. *Let L be a finite extension of degree n of a field K, and let $\mathfrak{O}$ be a valuation ring of L. Let $\mathfrak{M}$ be its maximal ideal, let $\mathfrak{o} = \mathfrak{O} \cap K$, and let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$, i.e. $\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o}$. Then the residue class degree $[\mathfrak{O}/\mathfrak{M} : \mathfrak{o}/\mathfrak{m}]$ is finite. If we denote it by f, and if e is the ramification index, then $ef \leqq n$.*

Proof. Let $y_1, \ldots, y_e$ be representatives in L^* of distinct cosets of Γ'/Γ and let $z_1, \ldots, z_s$ be elements of $\mathfrak{O}$ whose residue classes mod $\mathfrak{M}$ are linearly independent over $\mathfrak{o}/\mathfrak{m}$. Consider a relation

$$\sum_{i,j} a_{ij} z_j y_i = 0$$

with $a_{ij} \in K$, not all $a_{ij} = 0$. In an inner sum

$$\sum_{j=1}^{s} a_{ij} z_j,$$

divide by the coefficient a_{iv} having the biggest valuation. We obtain a linear combination of $z_1, \ldots, z_s$ with coefficients in $\mathfrak{o}$, and at least one coefficient equal to a unit. Since $z_1, \ldots, z_s$ are linearly independent mod $\mathfrak{M}$ over $\mathfrak{o}/\mathfrak{m}$, it follows that our linear combination is a unit. Hence

$$\left| \sum_{j=1}^{s} a_{ij} z_j \right| = |a_{iv}|$$

for some index v. In the sum

$$\sum_{i=1}^{e}\left(\sum_{j=1}^{s} a_{ij}z_j\right)y_i = 0$$

viewed as a sum on i, at least two terms have the same value. This contradicts the independence of $|y_1|, \ldots, |y_e| \bmod \Gamma$ just as in the proof of Proposition 4.2.

Remark. Our proof also shows that the elements $\{z_j y_i\}$ are linearly independent over K. This will be used again later.

If w is an extension of a valuation v, then the ramification index will be denoted by $e(w|v)$ and the residue class degree will be denoted by $f(w|v)$.

Proposition 4.7. *Let K be a field with a valuation v, and let $K \subset E \subset L$ be finite extensions of K. Let w be an extension of v to E and let u be an extension of w to L. Then*

$$e(u|w)e(w|v) = e(u|v),$$
$$f(u|w)f(w|v) = f(u|v).$$

Proof. Obvious.

We can express the above proposition by saying that the ramification index and the residue class degree are multiplicative in towers.

We conclude this section by relating valuation rings in a finite extension with the integral closure.

Proposition 4.8. *Let $\mathfrak{o}$ be a valuation ring in a field K. Let L be a finite extension of K. Let $\mathfrak{O}$ be a valuation ring of L lying above $\mathfrak{o}$, and $\mathfrak{M}$ its maximal ideal. Let B be the integral closure of $\mathfrak{o}$ in L, and let $\mathfrak{P} = \mathfrak{M} \cap B$. Then $\mathfrak{O}$ is equal to the local ring $B_{\mathfrak{P}}$.*

Proof. It is clear that $B_{\mathfrak{P}}$ is contained in $\mathfrak{O}$. Conversely, let x be an element of $\mathfrak{O}$. Then x satisfies an equation with coefficients in K, not all 0, say

$$a_n x^n + \cdots + a_0 = 0, \qquad a_i \in K.$$

Suppose that a_s is the coefficient having the biggest value among the a_i for the valuation associated with the valuation ring $\mathfrak{o}$, and that it is the coefficient farthest to the left having this value. Let $b_i = a_i/a_s$. Then all $b_i \in \mathfrak{o}$ and

$$b_n, \ldots, b_{s+1} \in \mathfrak{M}.$$

Divide the equation by x^s. We get

$$(b_n x^{n-s} + \cdots + b_{s+1}x + 1) + \frac{1}{x}\left(b_{s-1} + \cdots + b_0 \frac{1}{x^{s-1}}\right) = 0.$$

Let y and z be the two quantities in parentheses in the preceding equation, so that we can write

$$-y = z/x \quad \text{and} \quad -xy = z.$$

To prove our proposition it will suffice to show that y and z lie in B and that y is not in $\mathfrak{P}$.

We use Proposition 3.5 of Chapter VII. If a valuation ring of L above contains x, then it contains y because y is a polynomial in x with coefficients in

Hence such a valuation ring also contains $z = -xy$. If on the other hand the valuation ring of L above contains $1/x$, then it contains z because z is a polynomial in $1/x$ with coefficients in . Hence this valuation ring also contains y. From this we conclude by Chapter VII, Proposition 3.5, that y, z lie in B.

Furthermore, since $x \in \mathfrak{O}$, and $b_n, \ldots, b_{s+1}$ are in $\mathfrak{M}$ by construction, it follows that y cannot be in $\mathfrak{M}$, and hence cannot be in $\mathfrak{P}$. This concludes the proof.

Corollary 4.9. *Let the notation be as in the proposition. Then there is only a finite number of valuation rings of L lying above* $\mathfrak{P}$.

Proof. This comes from the fact that there is only a finite number of maximal ideals $\mathfrak{P}$ of B lying above the maximal ideal of $\mathfrak{o}$ (Corollary of Proposition 2.1, Chapter VII).

Corollary 4.10. *Let the notation be as in the proposition. Assume in addition that L is Galois over K. If* $\mathfrak{O}$ *and* $\mathfrak{O}'$ *are two valuation rings of L lying above* $\mathfrak{o}$, *with maximal ideals* $\mathfrak{M}$, $\mathfrak{M}'$ *respectively, then there exists an automorphism* σ *of L over K such that* $\sigma\mathfrak{O} = \mathfrak{O}'$ *and* $\sigma\mathfrak{M} = \mathfrak{M}'$.

Proof. Let $\mathfrak{P} = \mathfrak{O} \cap B$ and $\mathfrak{P}' = \mathfrak{O}' \cap B$. By Proposition 2.1 of Chapter VII, we know that there exists an automorphism σ of L over K such that $\sigma\mathfrak{P} = \mathfrak{P}'$. From this our assertion is obvious.

Example. Let k be a field, and let K be a finitely generated extension of transcendence degree 1. If t is a transcendence base of K over k, then K is finite algebraic over $k(t)$. Let $\mathfrak{O}$ be a valuation ring of K containing k, and assume that $\mathfrak{O}$ is $\neq K$. Let $\mathfrak{o} = \mathfrak{O} \cap k(t)$. Then $\mathfrak{o}$ is obviously a valuation ring of $k(t)$ (the

condition about inverses is *a fortiori* satisfied), and the corresponding valuation of $k(t)$ cannot be trivial. Either t or $t^{-1} \in \mathfrak{o}$. Say $t \in \mathfrak{o}$. Then $\mathfrak{o} \cap k[t]$ cannot be the zero ideal, otherwise the canonical homomorphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ of $\mathfrak{o}$ modulo its maximal ideal would induce an isomorphism on $k[t]$ and hence an isomorphism on $k(t)$, contrary to hypothesis. Hence $\mathfrak{m} \cap k[t]$ is a prime ideal $\mathfrak{p}$, generated by an irreducible polynomial $p(t)$. The local ring $k[t]_{\mathfrak{p}}$ is obviously a valuation ring, which must be $\mathfrak{o}$ because every element of $k(t)$ has an expression of type $p^r u$ where u is a unit in $k[t]_{\mathfrak{p}}$. Thus we have determined all valuation rings of $k(t)$ containing k, and we see that the value group is cyclic. Such valuations will be called discrete and are studied in greater detail below. In view of Corollary 4.5, it follows that the valuation ring $\mathfrak{O}$ of K is also discrete.

The residue class field $\mathfrak{o}/\mathfrak{m}$ is equal to $k[t]/\mathfrak{p}$ and is therefore a finite extension of k. By Proposition 4.6, it follows that $\mathfrak{O}/\mathfrak{M}$ is finite over k (if $\mathfrak{M}$ denotes the maximal ideal of $\mathfrak{O}$).

Finally, we observe that there is only a finite number of valuation rings $\mathfrak{O}$ of K containing k such that t lies in the maximal ideal of $\mathfrak{O}$. Indeed, such a valuation ring must lie above $k[t]_{\mathfrak{p}}$ where $\mathfrak{p} = (t)$ is the prime ideal generated by t, and we can apply Corollary 4.9.

§5. COMPLETIONS AND VALUATIONS

Throughout this section, we deal with a non-archimedean absolute value v on a field K. This absolute value is then a valuation, whose value group Γ_K is a subgroup of the positive reals. We let $\mathfrak{o}$ be its valuation ring, $\mathfrak{m}$ the maximal ideal.

Let us denote by $\hat{K}$ the completion of K at v, and let $\hat{\mathfrak{o}}$ (resp. $\hat{\mathfrak{m}}$) be the closure of $\mathfrak{o}$ (resp. $\mathfrak{m}$) in $\hat{K}$. By continuity, every element of $\hat{\mathfrak{o}}$ has value $\leqq 1$, and every element of $\hat{K}$ which is not in $\hat{\mathfrak{o}}$ has value > 1. If $x \in \hat{K}$ then there exists an element $y \in K$ such that $|x - y|$ is very small, and hence $|x| = |y|$ for such an element y (by the non-archimedean property). Hence $\hat{\mathfrak{o}}$ is a valuation ring in $\hat{K}$, and $\hat{\mathfrak{m}}$ is its maximal ideal. Furthermore,

$$\hat{\mathfrak{o}} \cap K = \mathfrak{o} \quad \text{and} \quad \hat{\mathfrak{m}} \cap K = \mathfrak{m},$$

and we have an isomorphism

$$\mathfrak{o}/\mathfrak{m} \xrightarrow{\sim} \hat{\mathfrak{o}}/\hat{\mathfrak{m}}.$$

Thus the residue class field $\mathfrak{o}/\mathfrak{m}$ does not change under completion.

Let E be an extension of K, and let $\mathfrak{o}_E$ be a valuation ring of E lying above $\mathfrak{o}$. Let $\mathfrak{m}_E$ be its maximal ideal. We assume that the valuation corresponding to $\mathfrak{o}_E$ is in fact an absolute value, so that we can form the completion E. We then have

a commutative diagram:

$$\begin{array}{ccc} \mathfrak{o}_E/\mathfrak{m}_E & \xrightarrow{\approx} & \hat{\mathfrak{o}}_E/\hat{\mathfrak{m}}_E \\ \uparrow & & \uparrow \\ \mathfrak{o}/\mathfrak{m} & \xrightarrow{\approx} & \hat{\mathfrak{o}}/\hat{\mathfrak{m}} \end{array}$$

the vertical arrows being injections, and the horizontal ones being isomorphisms. Thus the residue class field extension of our valuation can be studied over the completions E of K.

We have a similar remark for the ramification index. Let $\Gamma_v(K)$ and $\Gamma_v(\hat{K})$ denote the value groups of our valuation on K and $\hat{K}$ respectively (i.e. the image of the map $x \mapsto |x|$ for $x \in K^*$ and $x \in \hat{K}^*$ respectively). We saw above that $\Gamma_v(K) = \Gamma_v(\hat{K})$; in other words, the value group is the same under completion, because of the non-archimedean property. (This is of course false in the archimedean case.) If E is again an extension of K and w is an absolute value of E extending v, then we have a commutative diagram

$$\begin{array}{ccc} \Gamma_w(E) & \xrightarrow{=} & \Gamma_w(\hat{E}) \\ \uparrow & & \uparrow \\ \Gamma_v(K) & \xrightarrow{=} & \Gamma_v(\hat{K}) \end{array}$$

from which we see that the ramification index $(\Gamma_w(E) : \Gamma_v(K))$ also does not change under completion.

§6. DISCRETE VALUATIONS

A valuation is called **discrete** if its value group is cyclic. In that case, the valuation is an absolute value (if we consider the value group as a subgroup of the positive reals). The p-adic valuation on the rational numbers is discrete for each prime number p. By Corollary 4.5, an extension of a discrete valuation to a finite extension field is also discrete. Aside from the absolute values obtained by embedding a field into the reals or complex numbers, discrete valuations are the most important ones in practice. We shall make some remarks concerning them.

Let v be a discrete valuation on a field K, and let $\mathfrak{o}$ be its valuation ring. Let $\mathfrak{m}$ be the maximal ideal. There exists an element π of $\mathfrak{m}$ which is such that its value $|\pi|$ generates the value group. (The other generator of the value group is $|\pi^{-1}|$.) Such an element π is called a **local parameter** for v (or for $\mathfrak{m}$). Every

element x of K can be written in the form

$$x = u\pi^r$$

with some unit u of $\mathfrak{o}$, and some integer r. Indeed, we have $|x| = |\pi|^r = |\pi^r|$ for some $r \in \mathbf{Z}$, whence x/π^r is a unit in $\mathfrak{o}$. We call r the **order** of x at v. It is obviously independent of the choice of parameter selected. We also say that x has a **zero of order** r. (If r is negative, we say that x has a **pole** of order $-r$.)

In particular, we see that $\mathfrak{m}$ is a principal ideal, generated by π. As an exercise, we leave it to the reader to verify that every ideal of $\mathfrak{o}$ is principal, and is a power of $\mathfrak{m}$. Furthermore, we observe that $\mathfrak{o}$ is a factorial ring with exactly one prime element (up to units), namely π.

If $x, y \in K$, we shall write $x \sim y$ if $|x| = |y|$. Let π_i $(i = 1, 2, \ldots)$ be a sequence of elements of $\mathfrak{o}$ such that $\pi_i \sim \pi^i$. Let R be a set of representatives of $\mathfrak{o}/\mathfrak{m}$ in $\mathfrak{o}$. This means that the canonical map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ induces a bijection of R onto $\mathfrak{o}/\mathfrak{m}$.

Assume that K is complete under our valuation. Then every element x of $\mathfrak{o}$ can be written as a convergent series

$$x = a_0 + a_1\pi_1 + a_2\pi_2 + \cdots$$

with $a_i \in R$, and the a_i are uniquely determined by x.

This is easily proved by a recursive argument. Suppose we have written

$$x \equiv a_0 + \cdots + a_n\pi_n \pmod{\mathfrak{m}^{n+1}}$$

then $x - (a_0 + \cdots + a_n\pi_n) = \pi_{n+1}y$ for some $y \in \mathfrak{o}$. By hypothesis, we can write $y = a_{n+1} + \pi z$ with some $a_{n+1} \in R$. From this we get

$$x \equiv a_0 + \cdots + a_{n+1}\pi_{n+1} \pmod{\mathfrak{m}^{n+2}},$$

and it is clear that the n-th term in our series tends to 0. Therefore our series converges (by the non-archimedean behavior!). The fact that R contains precisely one representative of each residue class mod $\mathfrak{m}$ implies that the a_i are uniquely determined.

Examples. Consider first the case of the rational numbers with the p-adic valuation v_p. The completion is denoted by $\mathbf{Q}_p$. It is the field of ***p*-adic numbers**. The closure of $\mathbf{Z}$ in $\mathbf{Q}_p$ is the ring of ***p*-adic integers** $\mathbf{Z}_p$. We note that the prime number p is a prime element in both $\mathbf{Z}$ and its closure $\mathbf{Z}_p$. We can select our set of representatives R to be the set of integers $(0, 1, \ldots, p-1)$. Thus every p-adic integer can be written uniquely as a convergent sum $\sum a_i p^i$ where a_i is an integer, $0 \leqq a_i \leqq p - 1$. This sum is called its p-adic expansion. Such sums are added and multiplied in the ordinary manner for convergent series.

For instance, we have the usual formalism of geometric series, and if we take $p = 3$, then

$$-1 = \frac{2}{1-3} = 2(1 + 3 + 3^2 + \cdots).$$

We note that the representatives $(0, 1, \ldots, p-1)$ are by no means the only ones which can be used. In fact, it can be shown that $\mathbf{Z}_p$ contains the $(p-1)$-th roots of unity, and it is often more convenient to select these roots of unity as representatives for the non-zero elements of the residue class field.

Next consider the case of a rational field $k(t)$, where k is any field and t is transcendental over k. We have a valuation determined by the prime element t in the ring $k[t]$. This valuation is discrete, and the completion of $k[t]$ under this valuation is the power series ring $k[[t]]$. In that case, we can take the elements of k itself as repersentatives of the residue class field, which is canonically isomorphic to k. The maximal ideal of $k[[t]]$ is the ideal generated by t.

This situation amounts to an algebraization of the usual situation arising in the theory of complex variables. For instance, let z_0 be a point in the complex plane. Let $\mathfrak{o}$ be the ring of functions which are holomorphic in some disc around z_0. Then $\mathfrak{o}$ is a discrete valuation ring, whose maximal ideal consists of those functions having a zero at z_0. Every element of $\mathfrak{o}$ has a power series expansion

$$f(z) = \sum_{\nu=m}^{\infty} a_\nu (z - z_0)^\nu.$$

The representatives of the residue class field can be taken to be complex numbers, a_ν. If $a_m \neq 0$, then we say that $f(z)$ has a zero of order m. The order is the same, whether viewed as order with respect to the discrete valuation in the algebraic sense, or the order in the sense of the theory of complex variables. We can select a canonical uniformizing parameter namely $z - z_0$, and

$$f(z) = (z - z_0)^m g(z)$$

where $g(z)$ is a power series beginning with a non-zero constant. Thus $g(z)$ is invertible.

Let K be again complete under a discrete valuation, and let E be a finite extension of K. Let $\mathfrak{o}_E$, $\mathfrak{m}_E$ be the valuation ring and maximal ideal in E lying above $\mathfrak{o}$, $\mathfrak{m}$ in K. Let π be a prime element in E. If Γ_E and Γ_K are the value groups of the valuations in E and K respectively, and

$$e = (\Gamma_E : \Gamma_K)$$

is the ramification index, then

$$|\Pi^e| = |\pi|,$$

and the elements

$$\Pi^i \pi^j, \qquad 0 \leqq i \leqq e-1, j = 0, 1, 2, \ldots$$

have order $je + i$ in E.

Let $\omega_1, \ldots, \omega_f$ be elements of E such that their residue classes mod $\mathfrak{m}_E$ from a basis of $\mathfrak{o}_E/\mathfrak{m}_E$. If R is as before a set of representatives of $\mathfrak{o}/\mathfrak{m}$ in $\mathfrak{o}$, then the set consisting of all elements

$$a_1\omega_1 + \cdots + a_f\omega_f$$

with $a_j \in R$ is a set of representatives of $\mathfrak{o}_E/\mathfrak{m}_E$ in $\mathfrak{o}_E$. From this we see that every element of $\mathfrak{o}_E$ admits a convergent expansion

$$\sum_{i=0}^{e-1} \sum_{v=1}^{f} \sum_{j=0}^{\infty} a_{v,i,j} \pi^j \omega_v \Pi^i.$$

Thus the elements $\{\omega_v \Pi^i\}$ form a set of generators of $\mathfrak{o}_E$ as a module over $\mathfrak{o}$. On the other hand, we have seen in the proof of Proposition 4.6 that these elements are linearly independent over K. Hence we obtain:

Proposition 6.1. *Let K be complete under a discrete valuation. Let E be a finite extension of K, and let e, f be the ramification index and residue class degree respectively. Then*

$$ef = [E : K].$$

Corollary 6.2. *Let $\alpha \in E$, $\alpha \neq 0$. Let v be the valuation on K and w its extension to E. Then*

$$\operatorname{ord}_v N_K^E(\alpha) = f(w|v) \operatorname{ord}_w \alpha.$$

Proof. This is immediate from the formula

$$|N_K^E(\alpha)| = |\alpha|^{ef}$$

and the definitions.

Corollary 6.3. *Let K be any field and v a discrete valuation on K. Let E be a finite extension of K. If v is well behaved in E (for instance if E is separable over K), then*

$$\sum_{w|v} e(w|v) f(w|v) = [E : K].$$

If E is Galois over K, then all e_w are equal to the same number e, all f_w are

equal to the same number f, and so

$$efr = [E : K],$$

where r is the number of extensions of v to E.

Proof. Our first assertion comes from our assumption, and Proposition 3.3. If E is Galois over K, we know from Corollary 4.10 that any two valuations of E lying above v are conjugate. Hence all ramification indices are equal, and similarly for the residue class degrees. Our relation $efr = [E : K]$ is then obvious.

§7. ZEROS OF POLYNOMIALS IN COMPLETE FIELDS

Let K be complete under a non-trivial absolute value.

Let

$$f(X) = \prod (X - \alpha_i)^{r_i}$$

be a polynomial in $K[X]$ having leading coefficient 1, and assume the roots α_i are distinct, with multiplicities r_i. Let d be the degree of f. Let g be another polynomial with coefficients in K^a, and assume that the degree of g is also d, and that g has leading coefficient 1. We let $|g|$ be the maximum of the absolute values of the coefficients of g. One sees easily that if $|g|$ is bounded, then the absolute values of the roots of g are also bounded.

Suppose that g comes close to f, in the sense that $|f - g|$ is small. If β is any root of g, then

$$|f(\beta) - g(\beta)| = |f(\beta)| = \prod |\alpha_i - \beta|^{r_i}$$

is small, and hence β must come close to some root of f. As β comes close to say $\alpha = \alpha_1$, its distance from the other roots of f approaches the distance of α_1 from the other roots, and is therefore bounded from below. In that case, we say that β **belongs to** α.

Proposition 7.1. *If g is sufficiently close to f, and $\beta_1, \ldots, \beta_s$ are the roots of g belonging to α (counting multiplicities), then $s = r_1$ is the multiplicity of α in f.*

Proof. Assume the contrary. Then we can find a sequence g_v of polynomials approaching f with precisely s roots $\beta_1^{(v)}, \ldots, \beta_s^{(v)}$ belonging to α, but with $s \neq r$. (We can take the same multiplicity s since there is only a finite number of choices for such multiplicities.) Furthermore, the other roots of g also

belong to roots of f, and we may suppose that these roots are bunched together, according to which root of f they belong to. Since $\lim g_v = f$, we conclude that α must have multiplicity s in f, contradiction.

Next we investigate conditions under which a polynomial has a root in a complete field.

We assume that K is complete under a discrete valuation, with valuation ring $\mathfrak{o}$, *maximal ideal* $\mathfrak{p}$. We let π be a fixed prime element of $\mathfrak{p}$.

We shall deal with n-space over $\mathfrak{o}$. We denote a vector $(a_1, \ldots, a_n)$ with $a_i \in \mathfrak{o}$ by A. If $f(X_1, \ldots, X_n) \in \mathfrak{o}[X]$ is a polynomial in n variables, with integral coefficients, we shall say that A is a **zero** of f if $f(A) = 0$, and we say that A is a **zero** of f mod $\mathfrak{p}^m$ if $f(A) \equiv 0 \pmod{\mathfrak{p}^m}$.

Let $C = (c_0, \ldots, c_n)$ be in $\mathfrak{o}^{(n+1)}$. Let m be an integer $\geqq 1$. We consider the nature of the solutions of a congruence of type

$$(*) \qquad \pi^m(c_0 + c_1x_1 + \cdots + c_nx_n) \equiv 0 \pmod{\mathfrak{p}^{m+1}}.$$

This congruence is equivalent with the linear congruence

$$(**) \qquad c_0 + c_1x_1 + \cdots + c_nx_n \equiv 0 \pmod{\mathfrak{p}}.$$

If some coefficient c_i $(i = 1, \ldots, n)$ is not $\equiv 0 \pmod{\mathfrak{p}}$, then the set of solutions is not empty, and has the usual structure of a solution of one inhomogeneous linear equation over the field $\mathfrak{o}/\mathfrak{p}$. In particular, it has dimension $n - 1$. A congruence (*) or (**) with some $c_i \not\equiv 0 \pmod{\mathfrak{p}}$ will be called a **proper congruence**.

As a matter of notation, we write $D_i f$ for the formal partial derivative of f with respect to X_i. We write

$$\operatorname{grad} f(X) = (D_1 f(X), \ldots, D_n f(X)).$$

Proposition 7.2. *Let* $f(X) \in \mathfrak{o}[X]$. *Let* r *be an integer* $\geqq 1$ *and let* $A \in \mathfrak{o}^{(n)}$ *be such that*

$$f(A) \equiv 0 \pmod{\mathfrak{p}^{2r-1}},$$

$$D_i f(A) \equiv 0 \pmod{\mathfrak{p}^{r-1}}, \qquad \text{for all} \quad i = 1, \ldots, n,$$

$$D_i f(A) \not\equiv 0 \pmod{\mathfrak{p}^r}, \qquad \text{for some } i = 1, \ldots, n.$$

Let v *be an integer* $\geqq 0$ *and let* $B \in \mathfrak{o}^{(n)}$ *be such that*

$$B \equiv A \pmod{\mathfrak{p}^r} \quad \text{and} \quad f(B) \equiv 0 \pmod{\mathfrak{p}^{2r-1+v}}.$$

A vector $Y \in \mathfrak{o}^{(n)}$ *satisfies*

$$Y \equiv B \pmod{\mathfrak{p}^{r+v}} \quad \text{and} \quad f(Y) \equiv 0 \pmod{\mathfrak{p}^{2r+v}}$$

if and only if Y can be written in the form $Y = B + \pi^{r+v}C$, with some $C \in \mathfrak{o}^{(n)}$ satisfying the proper congruence

$$f(B) + \pi^{r+v} \operatorname{grad} f(B) \cdot C \equiv 0 \pmod{\mathfrak{p}^{2r+v}}.$$

Proof. The proof is shorter than the statement of the proposition. Write $Y = B + \pi^{r+v}C$. By Taylor's expansion,

$$f(B + \pi^{r+v}C) = f(B) + \pi^{r+v} \operatorname{grad} f(B) \cdot C \pmod{\mathfrak{p}^{2r+2v}}.$$

To solve this last congruence mod $\mathfrak{p}^{2r+v}$, we obtain a proper congruence by hypothesis, because $\operatorname{grad} f(B) \equiv \operatorname{grad} f(A) \equiv 0 \pmod{\mathfrak{p}^{r-1}}$.

Corollary 7.3. *Assumptions being as in Proposition 7.2, there exists a zero of f in $\mathfrak{o}^{(n)}$ which is congruent to A mod $\mathfrak{p}^r$.*

Proof. We can write this zero as a convergent sum

$$A + \pi^{r+1}C_1 + \pi^{r+2}C_2 + \cdots$$

solving for $C_1, C_2, \ldots$ inductively as in the proposition.

Corollary 7.4. *Let f be a polynomial in one variable in $\mathfrak{o}[X]$, and let $a \in \mathfrak{o}$ be such that $f(a) \equiv 0 \pmod{\mathfrak{p}}$ but $f'(a) \not\equiv 0 \pmod{\mathfrak{p}}$. Then there exists $b \in \mathfrak{o}$, $b \equiv a \pmod{\mathfrak{p}}$ such that $f(b) = 0$.*

Proof. Take $n = 1$ and $r = 1$ in the proposition, and apply Corollary 7.3.

Corollary 7.5. *Let m be a positive integer not divisible by the characteristic of K. There exists an integer r such that for any $a \in \mathfrak{o}$, $a \equiv 1 \pmod{\mathfrak{p}^r}$, the equation $X^m - a = 0$ has a root in K.*

Proof. Apply the proposition.

Example. In the 2-adic field $\mathbf{Q}_2$, there exists a square root of -7, i.e. $\sqrt{-7} \in \mathbf{Q}_2$, because $-7 = 1 - 8$.

When the absolute value is not discrete, it is still possible to formulate a criterion for a polynomial to have a zero by **Newton approximation**. (Cf. my paper, "On quasi-algebraic closure," *Annals of Math.* (1952) pp. 373–390.

Proposition 7.6. *Let K be a complete under a non-archimedean absolute value (nontrivial). Let $\mathfrak{o}$ be the valuation ring and let $f(X) \in \mathfrak{o}[X]$ be a polynomial in one variable. Let $\alpha_0 \in \mathfrak{o}$ be such that*

$$|f(\alpha_0)| < |f'(\alpha_0)^2|$$

(here f' denotes the formal derivative of f). Then the sequence

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

converges to a root α of f in $\mathfrak{o}$, and we have

$$|\alpha - \alpha_0| \leqq \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1.$$

Proof. Let $c = |f(\alpha_0)/f'(\alpha_0)^2| < 1$. We show inductively that:

1. $|\alpha_i| \leqq 1$,
2. $|\alpha_i - \alpha_0| \leqq c$,
3. $\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leqq c^{2^i}$.

These three conditions obviously imply our proposition. If $i = 0$, they are hypotheses. By induction, assume them for i. Then:

1. $|f(\alpha_i)/f'(\alpha_i)^2| \leqq c^{2^i}$ gives $|\alpha_{i+1} - \alpha_i| \leqq c^{2^i} < 1$, whence $|\alpha_{i+1}| \leqq 1$.
2. $|\alpha_{i+1} - \alpha_0| \leqq \max\{|\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0|\} = c$.
3. By Taylor's expansion, we have

$$f(\alpha_{i+1}) = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2$$

for some $\beta \in \mathfrak{o}$, and this is less than or equal to

$$\left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2$$

in absolute value.

Using Taylor's expansion on $f'(\alpha_{i+1})$ we conclude that

$$|f'(\alpha_{i+1})| = |f'(\alpha_i)|.$$

From this we get

$$\left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right| \leqq c^{2^{i+1}}$$

as desired.

The technique of the proposition is also useful when dealing with rings, say a local ring $\mathfrak{o}$ with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^r = 0$ for some integer $r > 0$. If one has a polynomial f in $\mathfrak{o}[X]$ and an approximate root α_0 such that

$$f'(\alpha_0) \not\equiv 0 \bmod \mathfrak{m},$$

then the Newton approximation sequence shows how to refine α_0 to a root of f.

Example in several variables. *Let K be complete under a non-archimedean absolute value. Let $f(X_1, \ldots, X_{n+1}) \in K[X]$ be a polynomial with coefficients in K. Let $(a_1, \ldots, a_n, b) \in K^{n+1}$. Assume that $f(a, b) = 0$. Let D_{n+1} be the*

partial derivative with respect to the $(n+1)$*-th variable, and assume that* $D_{n+1}f(a, b) \neq 0$. *Let* $(\bar{a}) \in K^n$ *be sufficiently close to* (a). *Then there exists an element* $\bar{b}$ *of* K *close to* b *such that* $f(\bar{a}, \bar{b}) = 0$.

This statement is an immediate corollary of Proposition 7.6. By multiplying all a_i, b by a suitable non-zero element of K one can change them to elements of $\mathfrak{o}$. Changing the variables accordingly, one may assume without loss of generality that a_i, $b \in \mathfrak{o}$, and the condition on the partial derivative not vanishing is preserved. Hence Proposition 7.6 may be applied. After perturbing (a) to $(\bar{a})$, the element b becomes an approximate solution of $f(\bar{a}, X)$. As $(\bar{a})$ approaches (a), $f(\bar{a}, b)$ approaches 0 and $D_{n+1}f(\bar{a}, b)$ approaches $D_{n+1}f(a, b) \neq 0$. Hence for $(\bar{a})$ sufficiently close to (a), the conditions of Proposition 7.6 are satisfied, and one may refine b to a root of $f(\bar{a}, X)$, thus proving the assertion.

The result was used in a key way in my paper "On Quasi Algebraic Closure". It is the analogue of Theorem 3.6 of Chapter XI, for real fields.

In the language of algebraic geometry (which we now assume), the result can be reformulated as follows. Let V be a variety defined over K. Let P be a simple point of V in K. Then there is a whole neighborhood of simple points of V in K. Especially, suppose that V is defined by a finite number of polynomial equations over a finitely generated field k over the prime field. After a suitable projection, one may assume that the variety is affine, and defined by one equation $f(X_1, \ldots, X_{n+1}) = 0$ as in the above statement, and that the point is $P = (a_1, \ldots, a_n, b)$ as above. One can then select $\bar{a}_i = x_i$ close to a_i but such that $(x_1, \ldots, x_n)$ are algebraically independent over k. Let y be the refinement of b such that $f(x, y) = 0$. Then (x, y) is a generic point of V over k, and the coordinates of (x, y) lie in K. In geometric terms, this means that the function field of the variety can be embedded in K over k, just as Theorem 3.6 of Chapter XI gave the similar result for an embedding in a real closed field, e.g. the real numbers.

EXERCISES

1. (a) Let K be a field with a valuation. If

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

is a polynomial in $K[X]$, define $|f|$ to be the max on the values $|a_i|(i = 0, \ldots, n)$. Show that this defines an extension of the valuation to $K[X]$, and also that the valuation can be extended to the rational field $K(X)$. How is Gauss' lemma a special case of the above statement? Generalize to polynomials in several variables.

(b) Let f be a polynomial with complex coefficients. Define $|f|$ to be the maximum of the absolute values of the coefficients. Let d be an integer $\geqq 1$. Show that

there exist constants C_1, C_2 (depending only on d) such that, if f, g are polynomials in $\mathbf{C}[X]$ of degrees $\leqq d$, then

$$C_1|f||g| \leqq |fg| \leqq C_2|f||g|.$$

[*Hint*: Induction on the number of factors of degree 1. Note that the right inequality is trivial.]

2. Let $M_{\mathbf{Q}}$ be the set of absolute values consisting of the ordinary absolute value and all p-adic absolute values v_p on the field of rational numbers $\mathbf{Q}$. Show that for any rational number $a \in \mathbf{Q}$, $a \neq 0$, we have

$$\prod_{v \in M_{\mathbf{Q}}} |a|_v = 1.$$

If K is a finite extension of $\mathbf{Q}$, and M_K denotes the set of absolute values on K extending those of $M_{\mathbf{Q}}$, and for each $w \in M_K$ we let N_w be the local degree $[K_w : \mathbf{Q}_v]$, show that for $\alpha \in K$, $\alpha \neq 0$, we have

$$\prod_{w \in M_K} |\alpha|_w^{N_w} = 1.$$

3. Show that the p-adic numbers $\mathbf{Q}_p$ have no automorphisms other than the identity. [*Hint*: Show that such automorphisms are continuous for the p-adic topology. Use Corollary 7.5 as an algebraic characterization of elements close to 1.]

4. Let A be a principal entire ring, and let K be its quotient field. Let $\mathfrak{o}$ be a valuation ring of K containing A, and assume $\mathfrak{o} \neq K$. Show that $\mathfrak{o}$ is the local ring $A_{(p)}$ for some prime element p. [This applies both to the ring $\mathbf{Z}$ and to a polynomial ring $k[X]$ over a field k.]

5. Let A be the subring of polynomials $f(X) \in \mathbf{Q}[X]$ such that the constant coefficient of f is in $\mathbf{Z}$. Show that every finitely generated ideal in A is principal, but the ideal of polynomials in A with 0 constant coefficient is not principal. [Laura Wesson showed me the above, which gives a counterexample to the exercise stated in previous editions and printings, using the valuation ring $\mathfrak{o}$ on $\mathbf{Q}(X)$ containing $\mathbf{Q}$ and such that X has order 1. Then $\mathfrak{o} \neq A_{(p)}$ for any element p of A.]

6. Let $\mathbf{Q}_p$ be a p-adic field. Show that $\mathbf{Q}_p$ contains infinitely many quadratic fields of type $\mathbf{Q}(\sqrt{-m})$, where m is a positive integer.

7. Show that the ring of p-adic integers $\mathbf{Z}_p$ is compact. Show that the group of units in $\mathbf{Z}_p$ is compact.

8. If K is a field complete with respect to a discrete valuation, with finite residue class field, and if $\mathfrak{o}$ is the ring of elements of K whose orders are $\geqq 0$, show that $\mathfrak{o}$ is compact. Show that the group of units of $\mathfrak{o}$ is closed in $\mathfrak{o}$ and is compact.

9. Let K be a field complete with respect to a discrete valuation, let $\mathfrak{o}$ be the ring of integers of K, and assume that $\mathfrak{o}$ is compact. Let $f_1, f_2, \ldots$ be a sequence of polynomials in n variables, with coefficients in $\mathfrak{o}$. Assume that all these polynomials have degree $\leqq d$, and that they converge to a polynomial f (i.e. that $|f - f_i| \to 0$ as $i \to \infty$). If each f_i has a zero in $\mathfrak{o}$, show that f has a zero in $\mathfrak{o}$. If the polynomials f_i are homogeneous of degree d, and if each f_i has a non-trivial zero in $\mathfrak{o}$, show that f has a non-trivial zero in $\mathfrak{o}$. [*Hint*: Use the compactness of $\mathfrak{o}$ and of the units of $\mathfrak{o}$ for the homogeneous case.]

(For applications of this exercise, and also of Proposition 7.6, cf. my paper "On quasi-algebraic closure," *Annals of Math.*, **55** (1952), pp. 412–444.)

10. Show that if p, p' are two distinct prime numbers, then the fields $\mathbf{Q}_p$ and $\mathbf{Q}_{p'}$ are not isomorphic.
11. Prove that the field $\mathbf{Q}_p$ contains all $(p-1)$-th roots of unity. [*Hint*: Use Proposition 7.6, applied to the polynomial $X^{p-1}-1$ which splits into factors of degree 1 in the residue class field.] Show that two distinct $(p-1)$-th roots of unity cannot be congruent mod p.
12. (a) Let $f(X)$ be a polynomial of degree $\geqq 1$ in $\mathbf{Z}[X]$. Show that the values $f(a)$ for $a \in \mathbf{Z}$ are divisible by infinitely many primes.
    (b) Let F be a finite extension of $\mathbf{Q}$. Show that there are infinitely many primes p such that all conjugates of F (in an algebraic closure of $\mathbf{Q}_p$) actually are contained in $\mathbf{Q}_p$. [*Hint*: Use the irreducible polynomial of a generator for a Galois extension of $\mathbf{Q}$ containing F.]
13. Let K be a field of characteristic 0, complete with respect to a non-archimedean absolute value. Show that the series

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

converge in some neighborhood of 0. (The main problem arises when the characteristic of the residue class field is $p > 0$, so that p divides the denominators $n!$ and n. Get an expression which determines the power of p occurring in $n!$.) Prove that the exp and log give mappings inverse to each other, from a neighborhood of 0 to a neighborhood of 1.

14. Let K be as in the preceding exercise, of characteristic 0, complete with respect to a non-archimedean absolute value. For every integer $n > 0$, show that the usual binomial expansion for $(1+x)^{1/n}$ converges in some neighborhood of 0. Do this first assuming that the characteristic of the residue class field does not divide n, in which case the assertion is much simpler to prove.
15. Let F be a complete field with respect to a discrete valuation, let $\mathfrak{o}$ be the valuation ring, π a prime element, and assume that $\mathfrak{o}/(\pi) = k$. Prove that if $a, b \in \mathfrak{o}$ and $a \equiv b \pmod{\pi^r}$ with $r > 0$ then $a^{p^n} \equiv b^{p^n} \pmod{\pi^{r+n}}$ for all integers $n \geqq 0$.
16. Let F be as above. Show that there exists a system of representatives R for $\mathfrak{o}/(\pi)$ in $\mathfrak{o}$ such that $R^p = R$ and that this system is unique (Teichmüller). [*Hint*: Let α be a residue class in k. For each $v \geqq 0$ let a_v be a representative in $\mathfrak{o}$ of $a^{p^{-v}}$ and show that the sequence $a_v^{p^v}$ converges for $v \to \infty$, and in fact converges to a representative a of α, independent of the choices of a_v.] Show that the system of representatives R thus obtained is closed under multiplication, and that if F has characteristic p, then R is closed under addition, and is isomorphic to k.
17. (a) **(Witt vectors again).** Let k be a perfect field of characteristic p. We use the Witt vectors as described in the exercises of Chapter VI. One can define an absolute value on $W(k)$, namely $|x| = p^{-r}$ if x_r is the first non-zero component of x. Show that this is an absolute value, obviously discrete, defined on the ring, and which can be extended at once to the quotient field. Show that this quotient field is complete, and note that $W(k)$ is the valuation ring. The maximal ideal consists of those x such that $x_0 = 0$, i.e. is equal to $pW(k)$.

(b) Assume that F has characteristic 0. Map each vector $x \in W(k)$ on the element

$$\sum \xi_i^{p^{-i}} p^i$$

where ξ_i is a representative of x_i in the special system of Exercise 15. Show that this map is an embedding of $W(k)$ into $\mathfrak{o}$.

18. **(Local uniformization).** Let k be a field, K a finitely generated extension of transcendence degree 1, and $\mathfrak{o}$ a discrete valuation ring of K over k, with maximal ideal $\mathfrak{m}$. Assume that $\mathfrak{o}/\mathfrak{m} = k$. Let x be a generator of $\mathfrak{m}$, and assume that K is separable over $k(x)$. Show that there exists an element $y \in \mathfrak{o}$ such that $K = k(x, y)$, and also having the following property. Let φ be the place on K determined by $\mathfrak{o}$. Let $a = \varphi(x), b = \varphi(y)$ (of course $a = 0$). Let $f(X, Y)$ be the irreducible polynomial in $k[X, Y]$ such that $f(x, y) = 0$. Then $D_2 f(a, b) \neq 0$. [*Hint:* Write first $K = k(x, z)$ where z is integral over $k[x]$. Let $z = z_1, \ldots, z_n (n \geqq 2)$ be the conjugates of z over $k(x)$, and extend $\mathfrak{o}$ to a valuation ring $\mathfrak{O}$ of $k(x, z_1, \ldots, z_n)$. Let

$$z = a_0 + a_1 x + \cdots + a_r x^r + \cdots$$

be the power series expansion of z with $a_i \in k$, and let $P_r(x) = a_0 + \cdots + a_r x^r$. For $i = 1, \ldots, n$ let

$$y_i = \frac{z_i - P_r(x)}{x^r}.$$

Taking r large enough, show that y_1 has no pole at $\mathfrak{O}$ but $y_2, \ldots, y_n$ have poles at $\mathfrak{O}$. The elements $y_1, \ldots, y_n$ are conjugate over $k(x)$. Let $f(X, Y)$ be the irreducible polynomial of (x, y) over k. Then $f(x, Y) = \psi_n(x)Y^n + \cdots + \psi_0(x)$ with $\psi_i(x) k[x]$. We may also assume $\psi_i(0) \neq 0$ (since f is irreducible). Write $f(x, Y)$ in the form

$$f(x, Y) = \psi_n(x) y_2 \cdots y_n (Y - y_1)(y_2^{-1} Y - 1) \cdots (y_n^{-1} Y - 1).$$

Show that $\psi_n(x) y_2 \cdots y_n = u$ does not have a pole at $\mathfrak{O}$. If $w \in \mathfrak{O}$, let w denote its residue class modulo the maximal ideal of $\mathfrak{O}$. Then

$$0 \neq f(\bar{x}, Y) = (-1)^{n-1} \bar{u}(Y - \bar{y}_1).$$

Let $y = y_1, \bar{y} = b$. We find that $D_2 f(a, b) = (-1)^{n-1} \bar{u} \neq 0$.]

19. Prove the converse of Exercise 17, i.e. if $K = k(x, y)$, $f(X, Y)$ is the irreducible polynomial of (x, y) over k, and if $a, b \in k$ are such that $f(a, b) = 0$, but $D_2 f(a, b) \neq 0$, then there exists a unique valuation ring $\mathfrak{o}$ of K with maximal ideal $\mathfrak{m}$ such that $x \equiv a$ and $y \equiv b \pmod{\mathfrak{m}}$. Furthermore, $\mathfrak{o}/\mathfrak{m} = k$, and $x - a$ is a generator of $\mathfrak{m}$. [*Hint:* If $g(x, y) \in k[x, y]$ is such that $g(a, b) = 0$, show that $g(x, y) = (x - a)A(x, y)/B(x, y)$ where A, B are polynomials such that $B(a, b) \neq 0$. If $A(a, b) = 0$ repeat the process. Show that the process cannot be repeated indefinitely, and leads to a proof of the desired assertion.]

20. (**Iss'sa-Hironaka** *Ann. of Math* 83 (1966), pp. 34–46). This exercise requires a good working knowledge of complex variables. Let K be the field of meromorphic functions on the complex plane $\mathbf{C}$. Let $\mathfrak{O}$ be a discrete valuation ring of K (containing the

constants $\mathbf{C}$). Show that the function z is in $\mathfrak{O}$. [*Hint:* Let $a_1, a_2, \ldots$ be a discrete sequence of complex numbers tending to infinity, for instance the positive integers. Let $v_1, v_2, \ldots$, be a sequence of integers, $0 \leqq v_i \leqq p - 1$, for some prime number p, such that $\sum v_i p^i$ is not the p-adic expansion of a rational number. Let f be an entire function having a zero of order $v_i p^i$ at a_i for each i and no other zero. If z is not in $\mathfrak{o}$, consider the quotient

$$g(z) = \frac{f(z)}{\prod_{i=1}^{n} (z - a_i)^{v_i p^i}}.$$

From the Weierstrass factorization of an entire function, show that $g(z) = h(z)^{p^{n+1}}$ for some entire function $h(z)$. Now analyze the zero of g at the discrete valuation of $\mathfrak{o}$ in terms of that of f and $\prod (z - a_i)^{v_i p^i}$ to get a contradiction.]

If U is a non-compact Riemann surface, and L is the field of meromorphic functions on U, and if $\mathfrak{o}$ is a discrete valuation ring of L containing the constants, show that every holomorphic function φ on U lies in $\mathfrak{o}$. [*Hint*: Map $\varphi : U \to \mathbf{C}$, and get a discrete valuation of K by composing φ with meromorphic functions on $\mathbf{C}$. Apply the first part of the exercise.] Show that the valuation ring is the one associated with a complex number. [*Further hint*: If you don't know about Riemann surfaces, do it for the complex plane. For each $z \in U$, let f_z be a function holomorphic on U and having only a zero of order 1 at z. If for some z_0 the function f_{z_0} has order $\geqq 1$ at $\mathfrak{o}$, then show that $\mathfrak{o}$ is the valuation ring associated with z_0. Otherwise, every function f_z has order 0 at $\mathfrak{o}$. Conclude that the valuation of $\mathfrak{o}$ is trivial on any holomorphic function by a limit trick analogous to that of the first part of the exercise.]