Local Fields.

1. Introduction.

1.1. Valuations.

Definition: Let k be a field. A real-valued function $|b|$ for $b \in k$ is a valuation if $\exists C \in \mathbb{R}$ such that: (i) $|b| \geq 0$, equality iff $b=0$.

(ii) $|bc| = |b|.|c|$ $\forall b,c \in k$.

(iii) $|b| \leq 1 \Rightarrow |1+b| \leq C$.

Examples: (i): The trivial valuation $|.|_0$ given by $|b|_0 = \begin{cases} 0 & \text{if } b=0 \\ 1 & \text{otherwise.} \end{cases}$

Lemma 1.1: If $|.|$ is a valuation on k and $\lambda > 0$ is real, then $|a|_1 = |a|^\lambda$ is a valuation.
Proof: Trivial. The corresponding constant is $C_1 = C^\lambda$. $|.|$ and $|.|_1$ are said to be equivalent.

Lemma 1.2: A valuation $|.|$ satisfies the triangle inequality iff can take constant $C=2$.
Proof: $(\Rightarrow)$. Suppose $|a| \leq 1$. Then $|1+a| \leq |1| + |a| \leq 2$.

$(\Leftarrow)$. Suppose $C=2$. Let $a_1, a_2 \in k$ such that $|a_1| \geq |a_2|$, $a_2 = aa_1$, $|a| \leq 1$.

Then $|a_1+a_2| = |a_1(1+a)| = |a_1|.|1+a| \leq 2|a_1| = 2.\max\{|a_1|, |a_2|\}$.

By induction, $|a_1 + \dots + a_{2^n}| \leq 2^n \max |a_j|$.

Take $a_1, \dots, a_N \in k$. Fix n by $2^{n-1} < N \leq 2^n$ and set $a_{N+1} = \dots = a_{2^n} = 0$.

Then, $|a_1 + \dots + a_N| \leq 2^n \max|a_j| \leq 2N.\max|a_j|$. (Note: $a_j = 1$ $\forall 1 \leq j \leq N \Rightarrow |N| \leq 2N$)

Now let $b,c \in k$, $n \in \mathbb{N}$. Then, $|b+c|^n = |(b+c)^n| = |\sum_{r=0}^{n} \binom{n}{r} b^r c^{n-r}|$

$\leq 2(n+1).\max_r |\binom{n}{r} b^r c^{n-r}| \leq 2(n+1).\max_r |\binom{n}{r}|.|b|^r.|c|^{n-r} \leq 4(n+1) \max_r \binom{n}{r}.|b|^r.|c|^{n-r}$

$\leq 4(n+1).\sum_r \binom{n}{r} |b|^r |c|^{n-r} = 4(n+1)(|b|+|c|)^n$

Take n-th root and let $n \to \infty$. Get $|b+c| \leq |b|+|c|$.

Definition: A valuation is non-archimedean if one can take $C=1$. ("non-arch.")

Lemma 1.3: The valuation $|.|$ is non-arch. iff it satisfies the ultrametric inequality: $|b+c| \leq \max\{|b|, |c|\}$.
Proof: $(\Rightarrow)$: Suppose $|b| \geq |c|$. Then $|b+c| = |b|.|1+\frac{c}{b}| \leq |b|$, as $|\frac{c}{b}| \leq 1$.

$(\Leftarrow)$: Suppose $|b| \leq 1$. Then $|1+b| \leq \max\{|1|, |b|\} = 1$.

Lemma 1.4: Suppose $|.|$ is non-arch. and $|c| < |b|$. Then $|b+c| = |b|$.
Proof: From Lemma 1.3 $(\Rightarrow)$, have $|b+c| \leq |b|$. Also, $b = (b+c) + (-c)$, so $|b| \leq \max\{|b+c|, |c|\}$.

Examples: (ii) Let $k = \mathbb{C}$. For $a = u+iv$ $(u,v \in \mathbb{R})$ the absolute value is $|a| = \sqrt{u^2+v^2}$. Then:

(a) $|a| \geq 0$, with $=$ iff $a=0$.

(b) $|ab| = |a|.|b|$.

(c) $|a+b| \leq |a|+|b|$. - triangle inequality.

(iii) Let $k = k_0(T)$, k_0 any field and T a transcendental over k_0. Consider first $k_0[T]$, the ring of polynomials. Choose some $c > 1$. If $f = f(T) = f_0 + f_1 T + \dots + f_n T^n$ $(f_n \neq 0)$ then set $|f| = c^n$, $|0| = 0$. Now, any element h of $k_0(T)$ is of the form $f(T)/g(T)$

with $f(T), g(T) \in k_0[T]$. Set $|h| = |f|/|g|$. Then, for $f, g \in k_0(T)$, have:

(a) $|f| \geq 0$, with $=$ iff $f = 0$.

(b) $|fg| = |f|.|g|$.

(c) $|f+g| \leq \max\{|f|, |g|\}$ - ultrametric inequality.

(iv) The p-adic valuation. Let p be a (positive) prime and let $\gamma \in (0,1)$. Any $0 \neq r \in \mathbb{Q}$ then can be written as $r = p^\rho u/v$, with $p \nmid uv$. Set $|r|_p = \gamma^\rho$, $|0|_p = 0$. The usual (a), (b) hold trivially.

(c) $|r+s|_p \leq \max\{|r|_p, |s|_p\}$. To check this, suppose $|r|_p \geq |s|_p > 0$. Then $r = \frac{p^\rho u}{v}$, $s = \frac{p^\sigma x}{y}$ with $\rho, \sigma, u, v, x, y \in \mathbb{Z}$, and $p \nmid uvxy$, and $\sigma = \rho + \tau$ some $\tau \geq 0$.

Now, $r+s = p^\rho U/V$, where $V = vy$, $U = uy + p^\tau vx$. Clearly $p \nmid V$. But it is possible that $p \nmid U$, say $U = p^\lambda W$, $\lambda \geq 0$, $p \nmid W$. Then $|r+s|_p = \gamma^{\rho+\lambda} \leq \gamma^\rho = \max\{|r|_p, |s|_p\}$

If we take $\gamma = p^{-1}$, we have the p-adic valuation on $\mathbb{Q}$

Application: The Bernoulli numbers B_k are defined by $\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k x^k}{k!}$; $B_k = 0$, k odd.

For k even, $B_k + \sum_{\substack{q \text{ prime} \\ (q-1)|k}} q^{-1} \in \mathbb{Z}$.

Proof: Let $S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$. On comparing coefficients in $1 + e^x + \cdots + e^{(n-1)x} = \frac{e^{nx} - 1}{x} \cdot \frac{x}{e^x - 1}$, we obtain $S_k(n) = \sum_{r=0}^{k} \binom{k}{r} \cdot \frac{B_r}{k+1-r} \cdot n^{k+1-r}$.

This gives that $B_k = \lim_{n \to 0} n^{-1} S_k(n)$ - nonsense in the usual sense!

Instead, choose prime p, and work with $|\cdot|_p$. For example, n can run through $p, p^2, p^3, \cdots$

So compare $p^{-m-1} S_k(p^{m+1})$ and $p^{-m} S_k(p^m)$.

Now, every integer $0 \leq j < p^{m+1}$ is uniquely of form $j = up^m + v$ $(0 \leq u < p,\ 0 \leq v < p^m)$.

Hence $S_k(p^{m+1}) = \sum_j j^k = \sum_u \sum_v (up^m + v)^k \equiv p \sum_v v^k + kp^m \sum_u u \cdot \sum_v v^{k-1} \pmod{p^{2m}}$.

Now, $\sum_v v^k = S_k(p^m)$ and $2\sum u = p(p-1) \equiv 0 \pmod p$. Hence $S_k(p^{m+1}) \equiv p S_k(p^m) \pmod{p^{m+1}}$

Dividing by p^{m+1}, we can write $|p^{-m-1} S_k(p^{m+1}) - p^{-m} S_k(p^m)|_p \leq 1$.

By the ultrametric inequality, we thus have $|p^{-l} S_k(p^l) - p^{-m} S_k(p^m)|_p \leq 1$ $\forall\, l, m \in \mathbb{N}$.

Put $m = 1$ and let $l \to \infty$ so that $|p^l|_p \to 0$. Then $|B_k - p^{-1} S_k(p)|_p \leq 1$

Now, $S_k(p) = \sum_0^{p-1} j^k \equiv \begin{cases} -1 & \text{if } (p-1)|k, \\ 0 & \text{otherwise} \end{cases}$ hence $\begin{cases} |B_k + p^{-1}|_p \leq 1 & \text{if } (p-1)|k \\ |B_k|_p \leq 1 & \text{otherwise.} \end{cases}$

Let $W_k = B_k + \sum_{\substack{q \text{ prime} \\ (q-1)|k}} q^{-1}$. If p is prime, have $W_k = \begin{cases} (B_k + p^{-1}) + \sum_{q \neq p} q^{-1} & \text{if } p \in \{q\} \\ B_k + \sum_q q^{-1} & \text{if not.} \end{cases}$

Both cases imply $|W_k|_p \leq 1$ $\forall$ primes p, by the ultrametric inequality. But this means that W_k has no primes in its denominator, so $W_k \in \mathbb{Z}$.

Lemma 1.5: Let $|\cdot|$ be a valuation on field k. Then $|\cdot|$ is non-arch iff $|e| \leq 1$ $\forall\, e$ in the ring generated by 1 in k.

Proof: ($\Rightarrow$) Clear.

($\Leftarrow$) By lemmas 1.1, 1.2, may suppose that $|\cdot|$ satisfies the triangle inequality. Then, for $b, c \in k$ and $n \in \mathbb{N}$, we have $|b+c|^n = |\sum \binom{n}{r} b^r c^{n-r}| \leq \sum |\binom{n}{r}| . |b|^r . |c|^{n-r} \leq \sum |b|^r . |c|^{n-r}$ $\leq (n+1) . \{\max(|b|, |c|)\}^n$. Take nth root and let $n \to \infty$. $\hookrightarrow \in \langle 1 \rangle$, so $|\cdot| \leq 1$

Corollary: (i) $k \subset K$ be fields, $|\cdot|$ a valuation on K. Then $|\cdot|$ is non-arch on K iff $|\cdot|$ is non-arch on restriction to k

(ii) Let k have prime characteristic. Then every valuation on k is non-arch.

Theorem 2.1: Every non-trivial valuation on $\mathbb{Q}$ is equivalent to either a p-adic valuation or to the ordinary absolute value.

Proof: As before, we may suppose $|\ |$ satisfies the triangle inequality.
Let $a>1$, $c>0$ be integers. Can write c in "base a": $c = c_m a^m + \dots + c_0$, where $m = m(c,a)$, $c_i \in \{0,1,\dots,a-1\}$, $c_m \neq 0$. Note $m \le \log c / \log a$.
By the triangle inequality, $|c| \le |c_m a^m| + \dots + |c_0| \le (m+1) \cdot \max\{|c_i|\} \cdot \max\{|a^i|\}$
$\le (m+1) \cdot M \cdot \max\{|a|^m, 1\}$, where $M = \max\{|1|, |2|, \dots, |a-1|\}$, independent of c.
Now let $b>1$ be an integer, and set $c = b^n$, some $n \in \mathbb{N}$. By the above, have
$|b|^n \le \{n \log b/\log a + 1\} \cdot M \cdot \max\{|a|^{n \log b/\log a}, 1\}$.
Take nth root and let $n \to \infty$, and get: $|b| \le \max\{|a|^{\log b/\log a}, 1\}$. $-(*)$.
Two cases:
(i) $\exists\, b \in \mathbb{N}$ with $|b|>1$. Then by $(*)$ we have $|a|>1$ $\forall\, a>1$. On interchanging a,b in $(*)$, we get $|b|^{1/\log b} = |a|^{1/\log a}$. This is true for all pairs a,b, so $|b| = b^\lambda$ $\forall\, b \in \mathbb{N}$, some λ.
It follows then that $|x| = |x|_\infty^\lambda$ $\forall\, x \in \mathbb{Q}$, with $|\ |_\infty$ the ordinary absolute value.
(ii) $|b| \le 1$ $\forall\, b>1$. Then $|\ |$ is non-arch., by lemma 1.5. Now, if $|b|=1$ $\forall\, b>1$, then $|\ |$ is trivial. Else $\exists\, b>1$ with $|b|<1$. Choose minimal such b. If $b = cd$ with $c,d>1$, then $1 > |b| = |c|.|d|$, then either $|c|$ or $|d| < 1$ - # minimality of b. So $b = p$, prime.
Let $c \in \mathbb{Z}$, $p \nmid c$. Then $c = up + v$, $0<v<p$. Now, $|v|=1$ by minimality of b, but $|up| = |u|.|p| < 1$
Hence $|c| = 1$, by lemma 1.4. From all this, it follows that $|\ |$ is equivalent to the p-adic valuation.

1.3. Independence of Valuations.

Lemma 3.1: Let $|\ |_1, |\ |_2$ be two valuations of k. Suppose $|\ |_1$ is non-trivial and $|a|_1 < 1 \Rightarrow |a|_2 < 1$. Then $|\ |_1, |\ |_2$ are equivalent.

Proof: Replacing a by a^{-1} see that $|a|_1 > 1 \Rightarrow |a|_2 > 1$. Now, suppose, if possible, that $\exists\, b \in k$ with $|b|_1 = 1$, $|b|_2 \neq 1$, say $|b|_2 > 1$. Pick $c \in k \setminus \{0\}$ with $|c|_1 < 1$. Then $|cb^n|_1 = |c|_1 |b|_1^n < 1$ $\forall\, n \geq 0$, but $|cb^n|_2 = |c|_2 |b|_2^n > 1$ for large enough n, contradicting hypothesis. Similarly if $|b|_2 < 1$.
So $|a|_1 \lesseqgtr 1$ iff $|a|_2 \lesseqgtr 1$. Now, let $b, c \in k \setminus \{0\}$, and apply this to $a = b^m c^n$, $m,n \in \mathbb{Z}$.
Take logs: $m \log |b|_1 + n \log |c|_1 \gtreqless 0$ iff $m \log |b|_2 + n \log |c|_2 \gtreqless 0$. $(*)$
Assume that $|c|_1 \neq 1$, say $|c|_1 > 1$. So $|c|_2 > 1$. So $\log |c|_2 > 0$.
$(*)$ becomes: $m \log |b|_1 \gtreqless -n \log |c|_1$ iff $m \log |b|_2 \gtreqless -n \log |c|_2$
So, $\dfrac{m \log |b|_1}{n \log |c|_2} \gtreqless -\lambda$, i.e. $m \log |b|_1 \gtreqless -\lambda n \log |c|_2$ iff $m \log |b|_2 \gtreqless -n \log |c|_2$, $\lambda = \dfrac{\log |c|_1}{\log |c|_2}$.
So, $<$ so that we have $=$, get $|b|_1 = |b|_2^\lambda$ all $b \in k$, as required.

Observe that a valuation $|\ |$ on k induces a topology, a basis for the open sets being $U(b,\delta) = \{c : |c-b| < \delta\}$. Equivalent valuations obviously induce the same topology.
If $|\ |$ satisfies the triangle inequality, the topology is that induced by the metric $d(b,c) = |b-c|$.
Clearly, we get the discrete topology iff $|\ |$ is the trivial valuation.

Lemma 3.2: Let $|\ |_1, |\ |_2$ induce the same topology on k. Then they are equivalent.

Proof: We may suppose $|\ |_1, |\ |_2$ are non-trivial. Then $|b|_1 < 1 \iff |b^n|_1 \to 0$ as $n \to \infty \iff b^n$ tends to 0 wrt the topology $\iff |b^n|_2 \to 0$ as $n \to \infty \iff |b|_2 < 1$. Then use lemma 3.1.

Lemma 3.3: Let $|\,|_1, \dots, |\,|_J$ be non-trivial valuations on k, with no two equivalent. Then $\exists\, a \in k$ with $|a|_1 > 1$ and $|a|_j < 1$ $(1 < j \le J)$.

Proof: Use induction on J.

$J=2$: Since $|\,|_1$ is not trivial and $|\,|_1, |\,|_2$ are not equivalent, by lemma 3.1 $\exists\, b \in k$ with $|b|_1 < 1$, $|b|_2 \geq 1$. Similarly, $\exists\, c \in k$ with $|c|_2 < 1$, $|c|_1 \geq 1$. Take $a = cb^{-1}$.

$J > 2$: By induction, $\exists\, b \in k$ with $|b|_1 > 1$, $|b|_j < 1$ $(2 \le j \le J-1)$.
As in case $J=2$, $\exists\, c \in k$ with $|c|_1 > 1$, $|c|_J < 1$. Three cases.

(i) $|b|_J < 1$: take $a = b$.

(ii) $|b|_J = 1$: $a = b^n c$ will do for large enough n.

(iii) $|b|_J > 1$: take $a = \frac{b^n}{1+b^n} c$. Since $\frac{b^n}{1+b^n} = \frac{1}{1+b^{-n}} \to \begin{cases} 1 & \text{for } |\,|_1, |\,|_J \\ 0 & \text{otherwise.} \end{cases}$ So a will do.

Theorem 3.1: Let $|\,|_j$ $(1 \le j \le J)$ be pairwise inequivalent non-trivial valuations. Choose $b_1, \dots, b_J \in k$ arbitrarily and let real $\varepsilon > 0$. Then $\exists\, a \in k$ such that $|a - b_j|_j < \varepsilon$ $\forall j$.

Proof: By lemma 3.3, $\exists\, c_j \in k$ such that $|c_j|_j > 1$, $|c_j|_i < 1$ $(i \neq j)$.
Then consider $\sum_j \frac{c_j^n}{1+c_j^n} b_j$ as $n \to \infty$.

1.4. Completeness.

Let k be a field with valuation $|\,|$. We say that a sequence $\{a_n\} = \{a_1, a_2, \dots\}$ tends to b as a limit (wrt $|\,|$) if for every $\varepsilon > 0$ $\exists\, n_0(\varepsilon)$ such that $|a_n - b| < \varepsilon$ $\forall\, n > n_0$.
A limit of a sequence, if it exists, is clearly unique.
Say $\{a_n\}$ is fundamental if for every $\varepsilon > 0$ $\exists$ an $n_1(\varepsilon)$ such that $|a_m - a_n| < \varepsilon$ $\forall\, m, n > n_1$.

Definition: The field k is complete wrt $|\cdot|$ if every fundamental sequence has a limit.

Let k have valuation $|\,|$, let $k \subset K$. Say $\|\,\|$ on K extends $|\,|$ if it takes the same values on k.

Definition: k with $|\,|$. We say field K together with valuation $\|\,\|$ extending $|\,|$ is a completion of k if
(i) K is complete
(ii) K is the closure of k wrt (the topology induced by) $\|\,\|$.

Theorem 4.1: Let k be a field with valuation $|\,|$. A completion exists and any two completions are canonically isomorphic.

Proof: By taking an equivalent valuation, we may suppose that $|\,|$ satisfies the triangle inequality, giving k a metric space structure. Let K be the completion of k wrt the metric. Let D be the metric of K, and set $\|\alpha\| = D(\alpha, 0)$ for $\alpha \in K$. We show that K can be given a field structure and that $\|\,\|$ is a valuation on it.
Let $\alpha, \beta \in K$, so they are limits of sequences $\{a_n\}, \{b_n\}$ in k. Then $a_n + b_n$ is a fundamental sequence, so has limit γ (say) $\in K$. Similarly, $a_n b_n$ has limit $\delta \in K$.
Define $\gamma = \alpha + \beta$, $\delta = \alpha\beta$. (Ring axioms are satisfied).

Now let $\alpha \in K, \alpha \neq 0$. Then $\|\alpha\| \neq 0$. Let $\{a_n\}$ be a sequence in k with limit α. Then $|a_n| \to \|\alpha\|$, since distance on a metric space is a continuous function wrt the induced topology. Hence $a_n = 0$ for only finitely many n; so suppose $a_n \neq 0 \ \forall n$. Set $b_n = a_n^{-1}$.

Then, $|b_m - b_n| = \dfrac{|a_m - a_n|}{|a_m||a_n|} \to 0$ (as $m, n \to \infty$), since $|a_m - a_n| \to 0$ and $|a_m|, |a_n| \to \|\alpha\| \neq 0$. Hence by completeness $\{b_n\}$ has a limit, which we define to be α^{-1}. It is now easy to check that K satisfies the field axioms.

By continuity, $\| \ \|$ on K satisfies the valuation axioms, since $| \ |$ does in k.

It remains to show uniqueness: Let L be any field complete wrt valuation $||| \ |||$ for which there is an embedding $\psi : k \hookrightarrow L$, respecting $| \ |, ||| \ |||$. Then ψ extends uniquely to an embedding of K in L since $\{\psi(a_n)\}$ is a fundamental sequence precisely when $\{a_n\}$ is one. Clearly $\psi(K)$ is the closure $\overline{\psi(k)}$ of $\psi(k)$ in L. If we now suppose that L is a completion of k, then $L = \overline{\psi(k)}$, so we have established an isomorphism between K and L.

Corollary: Let L be a complete valued field and let ψ be an embedding of the valued field k in L. Then the closure $\overline{\psi(k)}$ is a completion of k.

Theorem 4.2: Let k be a field and $| \ |_j$ $(1 \leq j \leq J)$ be non-trivial pairwise inequivalent valuations on k. Let k_j be the respective completions and let $\Delta : k \hookrightarrow \prod_j k_j$ be the diagonal map. Then $\Delta(k)$ is everywhere dense. (ie, $\overline{\Delta(k)} = \prod_j k_j$).

Proof: Wlog, $| \ |_j$ satisfy the triangle inequality. Let $\alpha_j \in k_j$ $(1 \leq j \leq J)$. Then, by the definition of completion, $\exists \ a_j \in k$ so that $|a_j - \alpha_j|_j < \varepsilon$, for given $\varepsilon > 0$.

By Theorem 3.1, $\exists \ b \in k$ such that $|b - a_j|_j < \varepsilon$ $(1 \leq j \leq J)$. Hence $|b - \alpha_j|_j < 2\varepsilon$ $(1 \leq j \leq J)$

1.5 Formal Series.

Let $\gamma \in (0,1)$, k a field. Define valuation $| \ |$ on $k(T)$ as follows. For $h(T) \in k(T)$, write $h(T) = T^p . f(T)/g(T)$ where $T \nmid f, g$ and $p \in \mathbb{Z}$ and $f(0), g(0) \neq 0$. Define $|h| = \gamma^p$.

Let $N \in \mathbb{Z}$, let $\{f_n\}$ be some sequence in k, $(n \geq N)$. Then, $f^{(m)} = \sum_{n=N}^{m} f_n T^n$ is a fundamental sequence of elements of $k(T)$, since $|f^{(M)} - f^{(m)}| \leq \gamma^{m+1}$ $(M > m)$.

We denote the limit in the completion $k((T))$ of $k(T)$ by $f = f(T) = \sum_N^\infty f_n T^n =: \sum_{n \gg -\infty} f_n T^n$, - $(*)$ where the notation here means $f_n = 0 \quad \forall n < N$, some N, when we are not actually concerned with the value of N.

Such elements form a commutative ring with a 1. We will now show that any element of type $(*)$ (not 0) has an inverse, of same type.

Note that $f(T) = T^p . b . (1 + \sum_{n \geq 1} g_n T^n)$, some $0 \neq b \in k$, $g_n \in k$. Let $h(T) = 1 + \sum_{m \geq 1} (-\sum_{n \geq 1} g_n T^n)^m$ $=: 1 + \sum_{n \geq 1} h_n T^n$. Then $(1 + \sum_{n \geq 1} g_n T^n)(1 + \sum_{n \geq 1} h_n T^n) = 1$. We have proved:

Lemma 5.1: The completion $k((T))$ of $k(T)$ is just the set of expressions $(*)$, together with 0.

We denote by $k[[T]]$ the set of $f(T)$ of $k((T))$ for which $|f(T)| \leq 1$. Clearly, $f(T) \in k[[T]]$ iff it can be written $f(T) = \sum_{n \geq 0} f_n T^n$.

$k[[T]]$ is a ring, the ring of formal power series.

Now let $k = \mathbb{Q}$

Definition: $f(T) = \sum_{n\geq 0} f_n T^n \in \mathbb{Q}[[T]]$ is said to satisfy Eisenstein's condition if $\exists\, u, v \in \mathbb{Z}$, $u, v \neq 0$ such that $uv^n f_n \in \mathbb{Z}$ $\forall n$.

Theorem 5.1 (Eisenstein): Let $f = f(T) \in \mathbb{Q}[[T]]$ and suppose that there are $g_j = g_j(T) \in \mathbb{Q}[T]$ (not all zero) such that $\sum_{0\leq j\leq J} g_j f^j = 0$. Then f satisfies Eisenstein's condition.

Proof: For indeterminates, X, Y, write $H(X) = \sum_j g_j(T) X^j \in \mathbb{Q}[T, X]$, and
$H(X+Y) = H(X) + H_1(X)Y + \dots + H_J(X)Y^J$, where $H_j \in \mathbb{Q}[T, X]$.
By hypothesis, $H(f) = 0$. Wlog, $H_1(f) \neq 0$. Define m by $|H_1(f)| = \gamma^m$
Put $f(T) = u(T) + T^{m+1}v(T)$, where $u(T) = f_0 + \dots + f_{m+1}T^{m+1} \in \mathbb{Q}[T]$,
$v(T) = 0 + f_{m+2}T + f_{m+3}T^2 + \dots \in \mathbb{Q}[[T]]$.
It clearly suffices to show $v(T)$ satisfies Eisenstein's condition.
We have $H(f) = 0 = H(u + T^{m+1}v) = H(u) + T^{m+1}H_1(u)v + \sum_{j\geq 2} T^{(m+1)j} H_j(u) v^j$,
where $H, H_1, H_j \in \mathbb{Q}[T]$.
Here, all summands except possibly the first are divisible by T^{2m+1}, and so $H(u)$ is divisible by T^{2m+1} (in $\mathbb{Q}[T]$). On dividing by T^{2m+1}, we obtain
$(*)$: $0 = h + h_1 v + \dots + h_J v^J$, with $h, h_1, \dots, h_J \in \mathbb{Q}[T]$, and $h_j(0) = 0$ $(j > 1)$, but $h_1(0) \neq 0$.
Multiplying throughout by an integer, we may assume $h, h_1, \dots, h_J \in \mathbb{Z}[[T]]$
Let $b = h_1(0)$. We have constructed $v = v(T) = \sum v_n T^n$ so that it has constant term 0. We shall show $b^n v_n \in \mathbb{Z}$.
On equating coefficients in $(*)$ we get that bv_n is a sum of terms of the form $e\prod_{m<n} v_m^{\mu(m)}$ with $e \in \mathbb{Z}$ and $\sum m\mu(m) < n$. $b^n v_n \in \mathbb{Z}$ follows by induction.

3. Archimedean Valuations.

3.1. Introduction.

A valuation is said to be Archimedean if it is not non-archimedean.
We will prove the following:

Theorem (Ostrowski): Let k be a field complete w.r.t an arch. valuation $|\cdot|$. Then $k \cong \mathbb{R}$ or $\mathbb{C}$ and $|\,|$ is equivalent to the ordinary absolute value.

This will be proved later. Note the following: char $k = 0$ (by cor. (ii) to Lemma 1.5, §1). So $k \supseteq \mathbb{Q}$. So the valuation induced by $|\,|$ on $\mathbb{Q}$ must be arch. (cor. (ii) of same), so is equivalent to $|\,|_\infty$. Since k is complete it therefore contains the completion $\mathbb{R}$ of $\mathbb{Q}$ wrt $|\,|_\infty$. (§2, Thm 4.1, Cor.)

Suppose first that k contains i with $i^2 = -1$. Then $k \supset \mathbb{C}$. We have then to show that the valuation on $\mathbb{C}$ induced by $|\,|$ is $|\,|_\infty$.
If k does not contain a solution of $i^2 = -1$, then we adjoin one, and show that the valuation $|\,|$ on k can be extended to $k(i)$.

3.2. Some Lemmas.

Lemma 2.1: Any archimedean valuation $|\ |$ on $\mathbb{C}$ is equivalent to the absolute value $|\ |_\infty$.

Proof: Wlog $|\ |$ satisfies the triangle inequality. By remark above, the valuations induced by $|\ |$ and $|\ |_\infty$ on $\mathbb{R}$ are equivalent, say $|a| = |a|_\infty^\lambda$ $\forall a \in \mathbb{R}$, some $0 < \lambda < \infty$.
Let $\alpha = a + ib$, $a, b \in \mathbb{R}$. Then $|a|_\infty, |b|_\infty \leq |\alpha|_\infty$, so $|\alpha| \leq |a| + |ib| = |a| + |b| \leq 2|\alpha|_\infty^\lambda$.
if $|\ |$ and $|\ |_\infty$ were inequivalent, this would contradict Thm 3.1, Ch. 2.

Lemma 2.2: Let k be complete wrt valuation $|\cdot|$. Suppose T^2+1 is irreducible in $k[T]$. Then there is $\Delta > 0$ such that $|a^2+b^2| \geq \Delta . \max\{|a|^2, |b|^2\}$, $\forall a, b \in k$.

Proof: We may suppose $|\cdot|$ satisfies the triangle inequality, and show that $\Delta = \frac{|4|}{1+|4|}$ will do.
By homogeneity, we have to show that if there is a $c_1 \in k$ with $|c_1^2+1| = \delta_1 < \Delta$, $-(*)$
then T^2+1 is reducible. We shall construct a $c^* \in k$ with $c^{*2}+1 = 0$ by successive approximation.
By $(*)$ and the triangle inequality, we have $|c_1^2| \geq 1 - \delta_1$. Put $c_2 = c_1 + h_1$, some $h_1 \in k$.
Then $c_2^2 + 1 = c_1^2 + 1 + 2h_1c_1 + h_1^2$. Choose $h_1 = -(c_1^2+1)/2c_1$ to eliminate linear terms.
Then, δ_2 (say) $= |c_2^2+1| = |h_1|^2 = |c_1^2+1|^2/|4|.|c_1|^2 \leq \theta\delta_1$, where we can take $\theta = \frac{\delta_1}{|4|(1-\delta_1)} < 1$.
On repeating the process, we obtain a sequence of elements $c_n \in k$ such that
δ_n (say) $= |c_n^2+1| \leq \theta\delta_{n-1} \leq \theta^{n-1}\delta_1$. Further, $|c_{n+1} - c_n|^2 = |c_n^2+1|^2/|4|.|c_n|^2 = \delta_{n+1} \leq \theta^n\delta_1$.
This implies that $\{c_n\}$ is a fundamental sequence, so $c_n \to c^* \in k$, by completeness.
Now, $|c^{*2}+1| = \lim_n |c_n^2+1| = 0$. So $c^{*2}+1 = 0$, as required.

Lemma 2.3: Let k be complete wrt valuation $|\ |$. Suppose T^2+1 is irreducible in $k[T]$. Then $\exists$ an extension of $|\ |$ to $k(i)$, where $i^2 = -1$.

Proof: Wlog, $|\ |$ satisfies the triangle inequality. Set $\|a+ib\| = |a^2+b^2|^{1/2}$. It is easy to check that this coincides with $|\ |$ on k, and that parts (i), (ii) of the definition of a valuation are satisfied. It remains to verify (iii).
Suppose that $\|a+ib\| \leq 1$. Then $|a|, |b| \leq \Delta^{-1/2}$, by lemma 2.2.
Hence, $\|1+(a+ib)\|^2 = |(1+a)^2+b^2| \leq 1 + |2|.|a| + |a|^2 + |b|^2 \leq 1 + |2|.|\Delta|^{-1/2} + 2|\Delta|^{-1}. = C^2$, say,
which is what was required.

3.3. Completion of Proof.

Lemma 3.1: Let k be complete wrt the archimedean valuation $|\ |$ and suppose $\exists\ i \in k$ with $i^2 = -1$. Then $k = \mathbb{C}$, and $|\ |$ is equivalent to $|\ |_\infty$.

Proof: Wlog, $|\ |$ satisfies the triangle inequality. We know $k \supset \mathbb{R}$, and so $k \supset \mathbb{R}(i) = \mathbb{C}$.
By lemma 2.1, the valuation induced by $|\ |$ on $\mathbb{C}$ is equivalent to $|\ |_\infty$.
Suppose that $k \neq \mathbb{C}$; let $\alpha \in k \setminus \mathbb{C}$. Then $|\alpha - a|$ is a continuous function of $a \in \mathbb{C}$, so attains its lower bound, say at $b \in \mathbb{C}$. Put $\beta = \alpha - b$. Then $|\beta| > 0$ since $\beta \neq 0$, and
$0 < |\beta| = \inf_{a \in \mathbb{C}} |\beta - a|$. Now let $c \in \mathbb{C}$, $0 < |c| < |\beta|$, and $n \in \mathbb{N}$.
Then, $\frac{\beta^n - c^n}{\beta - c} = \prod_{\substack{\varepsilon^n=1 \\ \varepsilon \neq 1}} (\beta - \varepsilon c)$, and $|\beta - \varepsilon c| \geq |\beta|$, hence $\frac{|\beta - c|}{|\beta|} \leq \frac{|\beta^n - c^n|}{|\beta|^n} = |1 - (c/\beta)^n|$

$\leq 1 + |c/\beta|^n \to 1$ as $n \to \infty$

Thus $|\beta - c| \le |\beta|$, so $|\beta - c| = |\beta|$. In particular, we may take $\beta - c$ instead of β and repeat the process. Hence $|\beta - mc| = |\beta|$ $\forall\, m \in \mathbb{N}$.
But then, $|m|.|c| \le |\beta| + |\beta - mc| \le 2|\beta|$ is bounded, # to $|\,|$ being archimedean.
(cf. Ch.2, Lemma 1.4).

4. Non-archimedean valuations.

4.1 Definitions and Basics.

Let $|\,|$ be a non-arch valuation the field k. The set $\mathfrak{o} = \{a : |a| \le 1\}$ is clearly a ring, called the ring of (valuation) integers. The set $\mathfrak{p} = \{a : |a| < 1\}$ is a maximal ideal of $\mathfrak{o}$. The quotient ring $\mathfrak{o}/\mathfrak{p}$ is thus a field - the residue class field.
If $|a| = 1$ we say that a is a (valuation) unit.

Let $\bar{k}$ be the completion of k wrt $|\,|$, and let $\bar{\mathfrak{o}}, \bar{\mathfrak{p}}$ be the corresponding ring of integers and maximal ideal. Clearly $\mathfrak{o} = \bar{\mathfrak{o}} \cap k$, $\mathfrak{p} = \bar{\mathfrak{p}} \cap k$.

Lemma 1.1: The natural map $\mathfrak{o}/\mathfrak{p} \to \bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ induced by the inclusion of $\mathfrak{o}$ into $\bar{\mathfrak{o}}$, is an isomorphism.
Proof: We need only show it is an epimorphism. If $\alpha \in \bar{\mathfrak{o}}$, then by the definition of $\bar{k}$, $\exists\, a \in k$ such that $|\alpha - a| < 1$. Then $a \in \mathfrak{o}$ and $\alpha - a \in \bar{\mathfrak{p}}$.

The set $\{|a| : a \in k^*\}$ is a subgroup of $\mathbb{R}^+$, called the valuation group.
We say that the valuation is discrete if the valuation group is discrete in the real topology, ie if $\exists\, \delta > 0$ such that $1 - \delta < |a| < 1 + \delta \Rightarrow |a| = 1$.

Lemma 1.2: The valuation is discrete iff $\mathfrak{p}$ is principal.
Proof: ($\Leftarrow$) Suppose $\mathfrak{p} = (\pi)$. Then $|a| < 1 \Rightarrow a \in \mathfrak{p} \Rightarrow a = \pi b$ $(b \in \mathfrak{o}) \Rightarrow |a| \le |\pi|$.
Similarly, $|a| > 1 \Rightarrow |a| \ge |\pi|^{-1}$.
($\Rightarrow$) Suppose $|\,|$ is discrete. Then the set $\{|a| : |a| < 1\}$ attains its upper bound, say at $a = \pi$.
Then $|a| < 1 \Rightarrow a = \pi b$, $|b| \le 1$, ie. $b \in \mathfrak{o}$.

If $\mathfrak{p} = (\pi)$, we say that π is a prime element for the valuation.
If $|\,|$ is discrete and $b \in k^*$ then $\exists\, n \in \mathbb{Z}$ such that $|b| = |\pi|^n$. n is the order of b, $n = \operatorname{ord} b$, independent of choice of π.
The axioms of a non-arch. valuation are equivalent to:

$$\operatorname{ord}(b+c) \ge \min\{\operatorname{ord} b, \operatorname{ord} c\}$$
$$\operatorname{ord}(bc) = \operatorname{ord} b + \operatorname{ord} c.$$

We set $\operatorname{ord} 0 = +\infty$.

We shall say that the infinite sum $\sum_0^\infty a_n$, $a_n \in k$, converges to the sum s if $s = \lim_{N \to \infty} S_N$, where $S_N = \sum_0^N a_n$
Clearly, the non-arch. property is inherited by infinite sums: $\left|\sum_0^\infty a_n\right| \le \max_n |a_n|$

Lemma 1.3: Suppose k is complete. Then Σa_n converges iff $a_n \to 0$.

Proof: ($\Rightarrow$) Suppose Σa_n converges. Then $\lim a_N = \lim (S_N - S_{N-1}) = \lim S_N - \lim S_{N-1} = s - s = 0$.

($\Leftarrow$) Suppose $a_n \to 0$, $M > N$. Then $|S_M - S_N| = |a_{N+1} + \dots + a_M| \leq \max_{N < n \leq M} |a_n| < \varepsilon \quad (N \geq N_0(\varepsilon))$.

Hence $\{S_N\}$ is a fundamental sequence, so converges by completeness.

Lemma 1.4: Suppose k is complete wrt the discrete valuation $|\,|$ and let π be a prime element. Let $\mathcal{A} \subset \mathfrak{o}$ be a set of representatives of $\mathfrak{o}/\mathfrak{p}$. Then every $a \in \mathfrak{o}$ is uniquely of the form $a = \sum_0^\infty a_n \pi^n$ ($a_n \in \mathcal{A}$).

Conversely, any such sum always converges to give an $a \in \mathfrak{o}$.

Proof: Converse is trivial by lemma 1.3, as $|a_n \pi^n| \leq |\pi|^n$, so $a \in \mathfrak{o}$.

Now let $a \in \mathfrak{o}$. $\exists$ precisely one $a_0 \in \mathcal{A}$ with $|a - a_0| < 1$, and then $a = a_0 + \pi b_1$, some $b_1 \in \mathfrak{o}$. $\exists$ precisely one $a_1 \in \mathcal{A}$ with $|b_1 - a_1| < 1$, and then $b_1 = a_1 + \pi b_2$, and so on. We get, for every N, $a = a_0 + \dots + a_N \pi^N + b_{N+1}\pi^{N+1}$, with $a_n \in \mathcal{A}$ and $b_{N+1} \in \mathfrak{o}$.

But $b_{N+1}\pi^{N+1} \to 0$, so done.

In the case $k = \mathbb{Q}_p$, the ring of integers is denoted $\mathbb{Z}_p$, the ring of p-adic integers. We can take $\pi = p$ and $\mathcal{A} = \{0, 1, \dots, p-1\}$.

Corollary: Suppose also $0 \in \mathcal{A}$, the every $a \in k^*$ is uniquely of the form $a = \sum_N^\infty a_n \pi^n$ ($a_n \in \mathcal{A}$, $a_N \neq 0$) for some $N \in \mathbb{Z}$.

Proof: For $\pi^{-N} a \in \mathfrak{o}$, some N.

Lemma 1.5: Suppose k is complete wrt a discrete valuation $|\,|$, and that the residue class $\mathfrak{o}/\mathfrak{p}$ is finite. Then $\mathfrak{o}$ is compact.

Proof: Since $|\,|$ makes $\mathfrak{o}$ a metric space, compactness $\equiv$ sequential compactness. So we have to show that every sequence $\{a^{(j)}\}$ of elements of $\mathfrak{o}$ has a convergent subsequence. Use the "diagonal process" on the representation $a^{(j)} = \sum_0^\infty a_{j_n} \pi^n$ ($a_{j_n} \in \mathcal{A}$), as in lemma 1.4.

$\mathcal{A}$ finite $\Rightarrow$ $\exists$ some a_0^* which occurs as a_{j_0} for infinitely many j. For the $a^{(j)}$ with $a_{j_0} = a_0^*$, $\exists$ some a_1^* which occurs as a_{j_1} for infinitely many j. For the $a^{(j)}$ with $a_{j_0} = a_0^*$, $a_{j_1} = a_1^*$, $\exists$ some a_2^* occurring as a_{j_2} for infinitely many j. And so on.

There is then a subsequence tending to $a^* = \Sigma a_n^* \pi^n$.

4.2 An Application to Finite Groups of Rational Matrices.

Lemma 2.1: Let $p \neq 2$ and $A \in GL_n(\mathbb{Z}_p)$. If $(*)$: $A \equiv I \pmod p$, $A \not\equiv I$, then A is of infinite order.

Proof: It is enough to show $A^q \neq I$ $\forall$ primes q and every A satisfying $(*)$. Write $A = I + B$, where B has elements $b_{ij} \in \mathbb{Z}_p$, ($1 \leq i, j \leq n$). Then $\exists$ u, v with $0 < \delta = |b_{uv}| = \max_{i,j} |b_{ij}| \leq p^{-1}$, by $(*)$, where $|\,| = |\,|_p$. We know: $A^q = (I+B)^q = I + \binom{q}{1}B + \binom{q}{2}B^2 + \dots + \binom{q}{q}B^q$.

(i) $q \neq p$. All elements of the matrices $\binom{q}{j}B^j$ ($j \geq 2$) have value at most δ^2. Also, $\binom{q}{1}B$ contains the element $q b_{uv}$, with value δ. Hence, $A^q - I \neq 0$

(ii) $q = p$: The binomial coefficients $\binom{p}{j}$ ($2 \leq j \leq p-1$) are all divisible by p, so the elements of $\binom{p}{j}B^j$ ($2 \leq j \leq p-1$) all have value $\leq p^{-1}\delta^2$. Elements of $\binom{p}{p}B^p$ have value $\leq \delta^p \leq \delta^3$ ($p \neq 2$). Also, $\binom{p}{1}B$ contains the element $p b_{uv}$, with value $p^{-1}\delta$. But $\delta \leq p^{-1}$, so $p^{-1}\delta > \max(p^{-1}\delta^2, \delta^3)$

Hence $A^q - I \neq 0$, as before.

Lemma 2.2: Let $p \neq 2$ and let G be a finite subgroup of $GL_n(\mathbb{Z}_p)$. Then $|G|$ divides

$$(p^n - p^{n-1})(p^n - p^{n-2})\dots(p^n-1) \quad -(*)$$

Proof: The residue class map $\mathbb{Z}_p \to \mathbb{F}_p$ induces a group homomorphism $\tau: GL_n(\mathbb{Z}_p) \to GL_n(\mathbb{F}_p)$. Let $A \in G$ be in $\ker \tau$. Then $A \equiv I \pmod p$, but A is of finite order, so $A = I$ by lemma 2.1. So τ gives an isomorphism from G to a subgroup of $GL_n(\mathbb{F}_p)$, and $(*)$ is the order of $GL_n(\mathbb{F}_p)$.

Theorem 2.1: Let $G < GL_n(\mathbb{Q})$ have finite order g. Then g divides $g^*(n) = \prod_{q \text{ prime}} q^{\beta(q)}$, where $\beta(2) = n + 2\lfloor n/2 \rfloor + \lfloor n/2^2 \rfloor + \lfloor n/2^3 \rfloor + \cdots$

$$\beta(q) = \lfloor n/(q-1) \rfloor + \lfloor n/q(q-1) \rfloor + \lfloor n/q^2(q-1) \rfloor + \cdots \quad (q \neq 2).$$

Proof: Since G is finite, there is only a finite set S of primes which occur in the denominators of elements of the matrices of G. For $p \notin S$, we have $G < GL_n(\mathbb{Z}_p)$

By Lemma 2.2, if $p \neq 2$, $p \notin S$, then g divides $(*)$ in 2.2.

We use Dirichlet's Theorem on primes in arithmetic progression, ie, if $(a,b)=1$ then $a+bm$ is prime for infinitely many $m \in \mathbb{Z}$.

Let $q \neq 2$ be prime. By Dirichlet, $\exists$ infinitely many primes p which are primitive roots modulo q^2. So $\exists$ $p \notin S$. We know that p is a primitive root modulo q^j $\forall j > 0$. It is then easy to see that $q^{\beta(q)}$ is the exact power of q dividing $(*)$.

For $q = 2$, take $p \notin S$, $p \equiv 3 \pmod 8$, and again $2^{\beta(2)}$ is the precise power of 2 dividing $(*)$.

This completes the proof.

4.3. Hensel's Lemma.

Lemma 3.1 ("Hensel's Lemma"): Let k be complete wrt $|\,|$, and let $f(X) \in \mathfrak{o}[X]$.

Let $a_0 \in \mathfrak{o}$ satisfy $|f(a_0)| < |f'(a_0)|^2$, where $f'(x)$ is the (formal) derivative. $-(1)$

Then $\exists$ $a \in \mathfrak{o}$ such that $f(a) = 0$.

Proof: Let $f_j(X)$ $(j = 1, 2, \dots)$ be defined by: $f(X+Y) = f(X) + f_1(X)Y + f_2(X)Y^2 + \cdots$, $-(2)$ for independent indeterminates X, Y. Then, $f_1(X) = f'(X)$.

By (1), $\exists$ $b_0 \in \mathfrak{o}$ such that $f(a_0) + b_0 f_1(a_0) = 0$. $-(3)$

Then, by (2), we have: $|f(a_0+b_0)| \leq \max_{j \geq 2} |f_j(a_0) b_0^j|$. Here, $|f_j(a_0)| \leq 1$ since $f_j(X) \in \mathfrak{o}[X]$ and $a_0 \in \mathfrak{o}$. Hence $|f(a_0+b_0)| \leq |b_0^2| = |f(a_0)|^2/|f'(a_0)|^2 < |f(a_0)|$, by (1).

Similarly, $|f_1(a_0+b_0) - f_1(a_0)| \leq |b_0| < |f_1(a_0)|$, and so $|f_1(a_0+b_0)| = |f_1(a_0)|$.

Now put $a_1 = a_0 + b_0$ and repeat.

Get a sequence of $a_n = a_{n-1} + b_{n-1}$ such that $|f_1(a_n)| = |f_1(a_0)|$ (all n), and $|f(a_{n+1})| \leq |f(a_n)|^2/|f_1(a_n)|^2 = |f(a_n)|^2/|f_1(a_0)|^2$, so $f(a_n) \to 0$.

Further, $|a_{n+1} - a_n| = |b_n| = |f(a_n)|/|f_1(a_n)| = |f(a_n)|/|f_1(a_0)| \to 0$, so $\{a_n\}$ is a fundamental sequence. By completeness, it has a limit a, and $f(a) = 0$.

Corollary 1: We have: $|a - a_0| \leq \dfrac{|f(a_0)|}{|f'(a_0)|}$ $-(*)$. Also, $\exists$ only one solution of $f(a)=0$ satisfying $(*)$.

Proof: We have $a - a_0 = \sum b_n$, so $(*)$ follows from (3) above.

Suppose $\exists$ $a^* \neq a$ with $f(a^*) = 0$, $|a^* - a_0| \leq |f(a_0)|/|f'(a_0)|$. Put $a^* = a + b^*$.

Then $0 = f(a+b^*) - f(a) = b^* f_1(a) + b^{*2} f_2(a) + \cdots$. Here $|b^*| \leq \dfrac{|f(a_0)|}{|f_1(a_0)|} < |f_1(a_0)| = |f_1(a)|$, by lemma 3.1. Since $|f_j(a)| \leq 1$ for $j \geq 2$, $|b^* f_1(a)| >$ value of the other terms. $-\#$ to non-arch.

Corollary 2: Let $f(X) \in \mathfrak{o}[X]$ have discriminant D and let $a_0 \in \mathfrak{o}$ satisfy $|f(a_0)| < |D|^2$.
Then $f(X)$ has a root in $\mathfrak{o}$.

Proof: Recall that D is a polynomial in the coefficients of f with coefficients in $\mathbb{Z}$, so $D \in \mathfrak{o}$.
Further, $\exists\ u(X), v(X) \in \mathfrak{o}[X]$ such that $u(X)f(X) + v(X)f'(X) = D$. – (i)
Now, $|u(a_0)| \le 1$, $|v(a_0)| \le 1$, and $|f(a_0)| < |D|^2 \le |D|$, by hypothesis. Hence (i) with $X \mapsto a_0$ implies $|f'(a_0)| \ge |D|$. Hence the conditions of the lemma are satisfied.

Example: $f(X) = f_0 + f_1 X + f_2 X^2$. $D = f_1^2 - 4f_0 f_2 = -4f_2 f(X) + (f_1 + 2f_2 X)f'(X)$.

Lemma 3.2: $p \ne 2$. Let $b \in \mathbb{Z}_p$, $|b| = 1$, and suppose there is an $a_0 \in \mathbb{Z}_p$ such that $|a_0^2 - b| < 1$.
Then $b = a^2$ for some $a \in \mathbb{Z}_p$.

Proof: Follows from lemma 3.1 with $f(x) = X^2 - b$, since $|f'(a_0)| = |2a_0| = 1$.
(or use corollary 2, as $|D| = |-4b| = 1$).

Corollary: The group $\mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$ has order 4 and exponent 2. Cosets representatives are $1, p, c, pc$, with c any quadratic non-residue.

Lemma 3.3: $(p = 2)$ If $b \in \mathbb{Z}_2$, $b \equiv 1 \pmod 8$, then $b = a^2$ for some $a \in \mathbb{Z}_2$.

Proof: In lemma 3.1, take $f(X) = X^2 - b$, so $|f(1)| \le 2^{-3}$, $|f'(1)| = 2^{-1}$.

Corollary: $\mathbb{Q}_2^* / \mathbb{Q}_2^{*2}$ has order 8 and exponent 2. Representatives of a set of generators are $-1, 5, 2$.

Lemma 3.4: $p \ne 3$, $b \in \mathbb{Z}_p$, $|b| = 1$. Suppose $b \equiv c^3 \pmod p$, some $c \in \mathbb{Z}_p$. Then $b = a^3$ for some a in $\mathbb{Z}_p$.

Proof: Apply lemma 3.1 to $X^3 - b$.

Lemma 3.5: $(p = 3)$. 3-adic unit b is a cube iff $b \equiv \pm 1 \pmod 9$

Proof: $\exists\ e \in \{0, \pm 1\}$ with $b \equiv \pm(1 + 3e)^3 \pmod{27}$. Now apply lemma 3.1 to $X^3 - b$ with $a_0 = \pm(1 + 3e)$

4.3*: Application to Diophantine Equations.

A diophantine equation is one in which the unknowns are required to lie in some specified field or ring.

We will consider the quadratic form: $F(\underset{\sim}{X}, \underset{\sim}{Y}) = F(X_1, .., X_n, Y_1, .., Y_m) = \sum_{j=1}^{n} a_j X_j^2 + \sum_{i=1}^{m} p b_i Y_i^2$, $(*1)$.
where the a_j and b_i are p-adic units.

Lemma 3*.1: Let $p \ne 2$ and F as in $(*1)$, where $|a_j| = |b_i| = 1\ \forall j, i$. Then,
$\exists\ x_1, .., x_n, y_1, .., y_m \in \mathbb{Q}_p$ (not all zero) such that $F(\underset{\sim}{x}, \underset{\sim}{y}) = 0$, iff either of
(i) $\exists\ c_1, .., c_n \in \mathbb{Z}$ (not all divisible by p) such that $\sum a_j c_j^2 \equiv 0 \pmod p$, or
(ii) $\exists\ d_1, .., d_m \in \mathbb{Z}$ (not all divisible by p) such that $\sum b_i d_i^2 \equiv 0 \pmod p$ - holds.

Proof: ($\Rightarrow$) Suppose $\exists$ such x_j, y_i. By multiplying throughout by a suitable power of p, we may assume that $\max\{|x_j|, |y_i|\} = 1$. Either $\max|x_j| = 1$, in which case we choose any $c_j \equiv x_j \pmod p$ and get (i). Or $\max|x_j| \le p^{-1}$, $\max|y_i| = 1$, and get (ii) with any $d_i \equiv y_i \pmod p$
($\Leftarrow$) Suppose (i) holds. Wlog $c_1 \not\equiv 0 \pmod p$. Hensel on $G(X) = a_1 X^2 + \sum_{j \ne 1} a_j c_j^2 \Rightarrow \exists\ x_1$ with $\sum a_j x_j^2 = 0$ and $x_j = c_j$ $(j \ne 1)$. Similarly for (ii)

Corollary: For $p=2$, the lemma continues to be true, provided that (i), (ii) are replaced by
(i) $\exists\, c_1,\dots,c_n \in \mathbb{Z}$ (not all even) and $d_1,\dots,d_m \in \mathbb{Z}$ such that $\sum a_j c_j^2 + 2\sum b_i d_i^2 \equiv 0 \pmod 8$
(ii) $\exists\, d_1,\dots,d_m \in \mathbb{Z}$ (not all even) and $c_1,\dots,c_n \in \mathbb{Z}$ such that $\sum b_i d_i^2 + 2\sum a_j c_j^2 \equiv 0 \pmod 8$

Definitions: $\mathbb{Q}$ is an example of a global field. The $\mathbb{Q}_p$ (including $\mathbb{Q}_\infty = \mathbb{R}$) are the corresponding local fields. We shall say that a diophantine equation has a solution globally if it has a solution in $\mathbb{Q}$, and that it has a solution everywhere locally if it has a solution in all localisations $\mathbb{Q}_p$.

Clearly: $\exists$ global solution $\Rightarrow$ $\exists$ solution everywhere locally. Is the converse true?

Example 3*.2: The equation $(X^2-2)(X^2-17)(X^2-34)=0$ has a solution everywhere locally but not globally.

Proof: No global solution – clear. There are obviously solutions in $\mathbb{Q}_\infty$. Further, $2 \in (\mathbb{Q}_{17}^*)^2$ and $17 \in (\mathbb{Q}_2^*)^2$. If $p \neq 2, 17, \infty$, then $2, 17, 34$ are p-adic units, and at least one of them is a quadratic residue mod p. This gives a root in $\mathbb{Q}_p$ by lemma 3.2.

Example 3*.3: There are rational solutions of $X^4 - 17 = 2Y^2$ everywhere locally but not globally.

Proof: There are clearly real solutions. For $\mathbb{Q}_2$, there is a solution with $Y=0$, and for $\mathbb{Q}_{17}$ there is one with $X=1$. For $p \neq 2, 17, \infty$, the theory of equations over finite fields shows that there are $a, b \in \mathbb{Z}$ such that $a^4 - 17 \equiv b^2 \pmod p$, and this gives a solution in $\mathbb{Q}_p$ by Hensel's Lemma.
Exercise: Show $\nexists$ global solutions.

4.4. Elementary Analysis.

Let k be a field complete wrt a non-arch. valuation $|\ |$.

Lemma 4.1: Let $b_{ij} \in k$ $(i,j = 0,1,2,\dots)$. Suppose that for every $\varepsilon > 0$, $\exists\, J(\varepsilon)$ such that $|b_{ij}| < \varepsilon$ whenever $\max(i,j) \geq J(\varepsilon)$. Then the series: $\sum_i(\sum_j b_{ij})$, $\sum_j(\sum_i b_{ij})$ both converge, and their sums are equal.

Proof: Clearly $\sum_j b_{ij}$ converges for every i, and $|\sum_j b_{ij}| < \varepsilon$, $(i \geq J(\varepsilon))$, by non-arch. Hence the first double sum converges. It is easily seen that $\left|\sum_{i=0}^{J}(\sum_{j=0}^{J} b_{ij}) - \sum_{i=0}^{\infty}(\sum_{j=0}^{\infty} b_{ij})\right| < \varepsilon$. Similarly, we get this with i, j interchanged. Hence the two infinite double sums differ by at most ε in value. As ε is arbitrary, they must be equal.

The notion of radius of convergence of a power series $f(X) = f_0 + f_1 X + f_2 X^2 + \dots$ applies in this context, and is simpler than for $\mathbb{R}$ or $\mathbb{C}$.
Put $R = \dfrac{1}{\limsup_n |f_n|^{1/n}}$.

So $0 \leq R \leq +\infty$, with the obvious conventions.

Lemma 4.2: Let $\mathcal{D}$ be the set of $a \in k$ for which the series $f(X) = f_0 + f_1 X + f_2 X^2 + \cdots$ converges.
Then: (i) if $R = 0$, then $\mathcal{D}$ consists of 0 alone
(ii) if $R = \infty$, then $\mathcal{D}$ consists of all of k.
(iii) if $0 < R < \infty$ and $|f_n| R^n \to 0$, then $\mathcal{D} = \{a \in k : |a| \le R\}$
(iv) otherwise $\mathcal{D} = \{a \in k : |a| < R\}$.

Proof: By lemma 1.3, $\mathcal{D}$ is precisely the set of $a \in k$ for which $f_n a^n \to 0$. Proof is now immediate.

Note: If R is not in the value group of k, options (iii) and (iv) coincide. It is useful, however, to maintain the distinction, say, when considering fields K containing k.

Lemma 4.3: Let $f(X)$, $\mathcal{D}$ be as in lemma 4.2 and let $c \in \mathcal{D}$. For $0 \le m < \infty$, put $g_m = \sum_{n \ge m} \binom{n}{m} f_n c^{n-m}$.
Then the series $g(X) = \sum_m g_m X^m$ has domain of convergence $\mathcal{D}$, and $f(b+c) = g(b)$ $\forall b \in \mathcal{D}$.

Proof: Note first that the series for g_m clearly converges. Let $b \in \mathcal{D}$.
Then $f(b+c) = \sum_n f_n (b+c)^n = \sum_n \sum_{m \le n} \binom{n}{m} f_n c^{n-m} b^m$.
It is to easy that Lemma 4.1 applies, and we obtain $\cdots = g(b)$ on interchanging the order of summation. Hence the domain of convergence of $g(X)$ contains that of $f(X)$.
That it cannot be larger follows on reversing the rôles of f and g.

Corollary: A function $f(X)$ defined by a power series is continuous within its domain of convergence.

Proof: For $g(b)$ above is certainly continuous at $b = 0$.

Theorem 4.1 (Strassman): Let k be complete wrt the non-arch. valuation $|\ |$, and let $f(X) = \sum_0^\infty f_n X^n$. Suppose that $f_n \to 0$ (so $f(X)$ converges in $\mathfrak{o}$), but that not all f_n are 0. Then there is at most a finite number of $b \in \mathfrak{o}$ such that $f(b) = 0$.
More precisely, there are at most N such b, where N is defined by $|f_N| = \max_n |f_n|$ and $|f_n| < |f_N|$, $\forall n > N$. $(*)$.

Proof: Use induction on N. Suppose first that $N = 0$ but $f(b) = 0$ for some $b \in \mathfrak{o}$.
Then $f_0 = -\sum_{n \ge 1} f_n b^n$. ✗ - since $|\sum_{n \ge 1} f_n b^n| \le \max_{n \ge 1} |f_n b^n| \le \max_{n \ge 1} |f_n| < |f_0|$.
Now suppose that $N > 0$ and $f(b) = 0$ ($b \in \mathfrak{o}$). Let $c \in \mathfrak{o}$.
Then, $f(c) = f(c) - f(b) = \sum_{n \ge 1} f_n (c^n - b^n) = (c-b) . \sum_{n \ge 1} \sum_{j < n} f_n c^j b^{n-1-j}$
By lemma 4.1, we may rearrange in powers of c, so $f(c) = (c-b) g(c)$, where $g(X) = \sum g_j X^j$, and $g_j = \sum_{r \ge 0} f_{j+1+r} b^r$.
It is easy to see that conditions $(*)$ imply that: $|g_j| \le |f_N|$ (all j), $|g_{N-1}| = |f_N|$, $|g_j| < |f_N|$ ($j > N-1$).
Hence $g(X)$ satisfies the hypotheses of the Theorem, but with $N-1$ instead of N. By the induction hypothesis, $g(X)$ has at most $N-1$ zeroes $c \in \mathfrak{o}$. But $f(c) = 0$ implies either $c = b$ or $g(c) = 0$. Hence $f(X)$ has at most N zeroes, as required.

Corollary 1: Suppose that both $f(X)$, $g(X)$ converge in $\mathfrak{o}$ and that $f(b) = g(b)$ for infinitely many $b \in \mathfrak{o}$. Then $f(X)$, $g(X)$ have the same coefficients.

Proof: For $f(X) - g(X)$ has infinitely many zeroes $b \in \mathfrak{o}$.

Corollary 2: Suppose char $k = 0$. Let $f(x)$ be a power series converging in $\mathfrak{o}$. Suppose $f(x+d) = f(x)$ for some $d \in \mathfrak{o}$. Then $f(x)$ is constant.

Proof: $f(x) - f(0)$ has infinitely many zeroes md $(m \in \mathbb{Z})$ in $\mathfrak{o}$.

4.5. A Useful Expansion

There are analogues in non-arch. valued fields of most of the standard functions of analysis. They share many properties with their analogues in $\mathbb{R}$ or $\mathbb{C}$, but there are also differences (cf. cor. 2 above). Here we shall prove the existence of a useful expansion.

Lemma 5.1: $|m!|_p = p^{-M}$, where $M = \lfloor m/p \rfloor + \lfloor m/p^2 \rfloor + \lfloor m/p^3 \rfloor + \cdots$

Proof: For $j \geq 1$, let $s(j)$ of the integers $1, \ldots, m$ be divisible by p^j but not by p^{j+1}.

Then $M = \sum_j j s(j) = \sum_i t(i)$, where $t(i) = s(i) + s(i+1) + s(i+2) + \cdots$

Here, $t(i)$ is the number of the integers $1, \ldots, m$ which are divisible by p^i.

Hence $t(i) = \lfloor m/p^i \rfloor$.

Corollary: $|m!| > p^{-m/(p-1)}$

Proof: $M < m/p + m/p^2 + \cdots = m/(p-1)$.

Lemma 5.2: Let $b \in \mathbb{Q}_p$ and suppose that $(*)\begin{cases} |b| \leq 2^{-2} & (p=2) \\ |b| \leq p^{-1} & (\text{otherwise}) \end{cases}$, $|\ |$ the p-adic valuation

Then there is a power series $\Phi_b(x) = \sum_0^\infty \gamma_n x^n$, where $\gamma_n \in \mathbb{Q}_p$, $\gamma_n \to 0$, such that $(1+b)^r = \Phi_b(r)$ $\forall r \in \mathbb{Z}$.

Proof: Suppose first that $r \geq 0$. Then $(1+b)^r = \sum_{s=0}^\infty \binom{r}{s} b^s$. Here $\binom{r}{s} = 0$ for $s > r$, but we ignore this, and rewrite as: $(1+b)^r = \sum_{s=0}^\infty r(r-1)\ldots(r-s+1)\,(b^s/s!)$. $\quad -(1)$.

Now $|b^s/s!| \to 0$, by $(*)$ and the above corollary. By Lemma 4.1, we may therefore rearrange (1) in powers of r to obtain: $(1+b)^r = \sum_{n=0}^\infty \gamma_n r^n$ $-(2)$,

where $\gamma_n \in \mathbb{Q}_p$ independent of r, and $\gamma_n \to 0$. So done for $r \geq 0$.

Note now that on putting $r = p^m$ $(m = 1, 2, \ldots)$ in (2) that $\lim_m (1+b)^{p^m} = 1$ $\quad -(3)$

Let $r < 0$, so $p^m + r > 0$ for large enough m, so (2) $\Rightarrow (1+b)^{p^m+r} = \sum_n \gamma_n (p^m+r)^n$. $-(4)$

Now let $m \to \infty$, so $p^m \to 0$. LHS $\to (1+b)^r$ by (3). RHS $\to \sum_n \gamma_n r^n$, as a power series in its domain of convergence (by Lemma 4.3, Cor.). So (2) holds also for $r < 0$.

Note: The lemma extends to any complete field $k \supset \mathbb{Q}_p$ with valuation extending the p-adic valuation. It is then appropriate to replace $(*)$ by $|b| < p^{-1/(p-1)}$ (all p).

4.6. An Application to Recurrent Sequences.

Lemma 6.1 (Nagell): Define u_n by $u_0 = 0, u_1 = 1$, and $u_n = u_{n-1} - 2u_{n-2}$ $(n \geq 2)$. Then $u_n = \pm 1$ only for $n = 1, 2, 3, 5$ and 13.

Proof: The first few values are:

n	0	1	2	3	4	5	6	7	8	9
u_n	0	1	1	-1	3	-1	5	7	-3	-17

We get $u_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$,

where α, β are the roots of $F(X) = X^2 - X + 2$.

[This has roots $\alpha = \frac{1}{2}(1+\sqrt{-7})$, $\beta = \frac{1}{2}(1-\sqrt{-7})$] We can work in any p-adic field $\mathbb{Q}_p$ in which $F(x)$ splits. This is the case for $\mathbb{Q}_{11}$, by Hensel (3.1) Cor. 2, as $D = -7$ and $F(5) = 22 \equiv 0 \pmod{11}$. Working through Hensel, we get root $\alpha \in \mathbb{Z}_{11}$: $\alpha \equiv 16 \pmod{11^2}$, $\beta = 1-\alpha \equiv 106 \pmod{11^2}$.

We would like to expand u_n as a power series in n and apply Strassman's Theorem. This does not work directly because α, β do not satisfy lemma 5.2.

But by Fermat's Little Theorem: $\left.\begin{array}{l} A = \alpha^{10} \equiv 1 \pmod{11} \\ B = \beta^{10} \equiv 1 \pmod{11} \end{array}\right\}$ so lemma 5.2 applies to A, B.

Write $n = r + 10s$, $0 \le r \le 9$, so $u_{r+10s} = \dfrac{\alpha^r A^s - \beta^r B^s}{\alpha - \beta}$. Note that $u_{r+10s} \equiv u_r \pmod{11}$, so we need only consider $r = 1, 2, 3, 5$.

r	$\alpha^r \bmod 11^2$	$\beta^r \bmod 11^2$
1	16	106
2	14	104
3	103	13
5	111	21
10	100	78

We now write $\alpha^{10} = A = 1 + a$, $\beta^{10} = B = 1 + b$. So $a \equiv 99 \pmod{11^2}$, $b \equiv 77 \pmod{11^2}$.

We develop $(\alpha-\beta)(u_{r+10s} \mp 1) = \alpha^r (1+a)^s - \beta^r (1+b)^s \mp (\alpha - \beta)$ as a power series $c_0 + c_1 s + c_2 s^2 + \ldots$ using Lemma 5.2.

Here, the upper sign is correct for $r = 1, 2$ and the lower for $r = 3, 5$.

In each case, $c_0 = 0$. Easy that $c_j \equiv 0 \pmod{11^2}$. $(\forall j \ge 2)$

For $r = 1, 2, 5$, the table shows that $c_1 \equiv \alpha^r a - \beta^r b \not\equiv 0 \pmod{11^2}$. Hence the powes series has at most one zero $s \in \mathbb{Z}$. Since in each case, $s = 0$ is a solution, there are no others.

For $r = 3$ however, we have $c_1 \equiv 0 \pmod{11^2}$, so we must estimate the c_j more precisely. We have: $2.11^{-2} c_2 \equiv \alpha^3 (a/_{11})^2 - \beta^3 (b/_{11})^2 \equiv 6 \pmod{11}$, so $c_2 \not\equiv 0 \pmod{11^3}$. Since $c_j \equiv 0 \pmod{11^3}$ $(j \ge 3)$, Strassman $\Rightarrow$ the series can vanish for at most two values of s. Since $u_3 = u_{13} = -1$, there can be no others.

<u>Corollary</u>: The only solutions of $x^2 + 7 = 2^m$ $(x, m \in \mathbb{Z})$, have $m = 3, 4, 5, 7, 15$.

<u>Proof</u>: Clearly x is odd, say $x = 2y - 1$ $(y \in \mathbb{Z})$. Then: $y^2 - y + 2 = 2^{m-2}$. The ring $\mathbb{Z}[\alpha]$, where $\alpha^2 - \alpha + 2 = 0$, has a Euclidean algorithm and so is a UFD. On considering factorisation of both sides, we get $y \pm \alpha = \pm \alpha^{m-2}$ (some choice of signs). Then $y \pm \beta = \pm \beta^{m-2}$, for the conjugate root β. Hence $(\alpha - \beta) = \pm(\alpha^{m-2} - \beta^{m-2})$, which is Lemma 6.1 with $n = m-2$.

<u>Lemma 6.2 (Mignotte)</u>: Define u_n by $u_0 = u_1 = 0$, $u_2 = 1$ and $u_{n+3} = 2u_{n+2} - 4u_{n+1} + 4u_n$ $(n \ge 0)$. Then $u_n = 0$ precisely for $n = 0, 1, 4, 6, 13, 52$.

<u>Proof (sketch)</u>: The auxiliary polynomial is: $F(X) = X^3 - 2X^2 + 4X - 4$. The smallest prime for which it splits completely is 47, so we work in $\mathbb{Q}_{47}$. Roots of $F(x)$ are: $\alpha \equiv 1398$, $\beta \equiv 550$, $\gamma \equiv 263 \pmod{47^2}$

We have $u_n = A\alpha^n + B\beta^n + C\gamma^n$ (all n), where $A \equiv 319$, $B \equiv 578$, $C \equiv 1312 \pmod{47^2}$.

Also, $\alpha^{46} = 1 + a$, $\beta^{46} = 1 + b$, $\gamma^{46} = 1 + c$, where $a \equiv 1457 = 31.47$, $b \equiv 1316 = 28.47$, $c \equiv 1363 = 29.47 \pmod{47^2}$

Put $n = r + 46s$. One checks that $u_n \equiv 0 \pmod{47}$ precisely when $r \equiv 0, 1, 4, 6$, or $13 \pmod{46}$.

Then similar to Lemma 6.1: For $r = 0, 1, 4, 13$, the Strassman bound is 1, and there is a solution with $s = 0$. For $r = 6$, the Strassman bound is 2, and there are solutions with $s = 0, 1$.

6. Transcendental Extensions and Factorisation.

6.1. Introduction.

Let $|\ |$ be a non-arch. valuation on a field k. We introduce a family of extensions $\|\ \|$ of $|\ |$ to $k(X)$, where X is a transcendental over k. k will be complete. We show that the set of values $|f_j|$ of the coefficients of $f(X) = f_0 + \dots + f_n X^n \in k[X]$ give a great deal of information about the factorisation of $f(X)$ in $k[X]$.

Lemma 1.1: Let $|\ |$ be a non-arch. valuation on the field k and let $c>0$. For $f(X) \in k[X]$, put $\|f\| = \|f\|_c = \max_j c^j |f_j|$. For $h(X) = \frac{f(X)}{g(X)} \in k(X)$, put $\|h\| = \|f\|/\|g\|$.

Then $\|\ \|$ is a valuation on $k(X)$ which coincides with $|\ |$ on k.

Proof: Let $f(X), g(X) \in k[X]$. Clearly, $\|f+g\| \le \max\{\|f\|, \|g\|\}$ -(1) and $\|fg\| \le \|f\|.\|g\|$. -(2)

We must show equality in (2). $\exists\, I \in \mathbb{Z}$ with $\|f_I X^I\| = \|f\|$, $\|f_i x^i\| < \|f\|$ $(i < I)$.

If $g(X) = g_0 + \dots + g_m X^m$, we define J by $\|g_J X^J\| = \|g\|$, $\|g_j X^j\| < \|g\|$ $(j < J)$

The coefficient of X^{I+J} in fg is: $\sum_{i+j=I+J} f_i g_j$. Three cases:

(i) $i < I$. Then $\|f_i X^i\| < \|f\|$, ie $|f_i| < c^{-i}\|f\|$. Further, $\|g_j X^j\| \le \|g\|$, ie $|g_j| \le c^{-j}\|g\|$.

Hence $|f_i g_j| < c^{-I-J}\|f\|.\|g\|$.

(ii) $j < J$ - get same result.

(iii) $i = I$, $j = J$. Here, $|f_I| = c^{-I}\|f\|$, $|g_J| = c^{-J}\|g\|$, and $|f_I g_J| = c^{-I-J}\|f\|.\|g\|$.

Hence, $|\sum_{i+j=I+J} f_i g_j| = c^{-I-J}\|f\|.\|g\|$.

So, by the definition of $\|\ \|$, have $\|fg\| \ge \|f\|.\|g\|$. So, by (2), $\|fg\| = \|f\|.\|g\|$, -(2') as required.

Now let $h(X) \in k(X)$, say $h(X) = \frac{f(X)}{g(X)} = \frac{F(X)}{G(X)}$, $f, g, F, G \in k[X]$. Then $f(X)G(X) = F(X)g(X)$, so $\|f\|.\|G\| = \|F\|.\|g\|$. Hence $\|h\|$ is independent of choice of f, g.

So, by (1) and (2'), $\|\ \|$ is a (non-arch.) valuation on $k(X)$.

Corollary: Let $X_1, \dots, X_n$ be independent transcendentals over k and let $c_1, \dots, c_n > 0$.

For $f(X_1, \dots, X_n) = \sum f(i_1, \dots, i_n) X_1^{i_1} \dots X_n^{i_n}$ $(f(i_1, \dots, i_n) \in k)$, put $\|f\| = \|f\|_{c_1, \dots, c_n} = \max c_1^{i_1} \dots c_n^{i_n} |f(i_1, \dots, i_n)|$

Then $\|\ \|$ extends uniquely to $k(X_1, \dots, X_n)$ and is a valuation.

Proof: Since $k(X_1, \dots, X_n) = k(X_1, \dots, X_{n-1})(X_n)$, this follows by induction.

6.2: Gauss' Lemma and Eisenstein Irreducibility.

Lemma 2.1 ("Gauss"): Suppose $f(X_1, \dots, X_n) \in \mathfrak{o}[X_1, \dots, X_n]$ is the product of two non-constant elements of $k[X_1, \dots, X_n]$. Then it is the product of two non-constant elements of $\mathfrak{o}[X_1, \dots, X_n]$.

Proof: Use the valuation $\|\ \|$ on $k[X_1, \dots, X_n]$ from the above corollary, with $c_1 = \dots = c_n = 1$.

Then $\mathfrak{o}[X_1, \dots, X_n]$ is just the set of elements of $k[X_1, \dots, X_n]$ which are valuation integers.

Further, $|\ |$ and $\|\ \|$ have the same value group.

Suppose that $f = gh$, $g, h \in k[X_1, \dots, X_n]$. $\exists\, b \in k$ with $|b| = \|g\|$. Replace g by $b^{-1}g$ and h by bh, so that $\|g\| = 1$. Then $1 \ge \|f\| = \|g\|.\|h\| = \|h\|$

Hence $g, h \in \mathfrak{o}[X_1, \dots, X_n]$, as required.

Corollary: If f is irreducible is $\mathfrak{o}[X_1,\dots,X_n]$, then it is so in $k[X_1,\dots,X_n]$.

Lemma 2.2 (Gauss): Suppose that $f(X_1,\dots,X_n)\in\mathbb{Z}[X_1,\dots,X_n]$ is the product of two non-constant elements of $\mathbb{Q}[X_1,\dots X_n]$. Then it is the product of two non-constant elements of $\mathbb{Z}[X_1,\dots,X_n]$.

Proof: Suppose that $f=gh$, $g,h\in\mathbb{Q}[X_1,\dots,X_n]$. Then $g,h\in\mathbb{Z}_p[X_1,\dots,X_n]$, except for the primes p in a finite set S. If $S=\emptyset$, we are done. Otherwise, for each $p\in S$ there is, by the proof of the preceding lemma, a power $p^{m(p)}$ such that $p^{m(p)}g,\ p^{-m(p)}h\in\mathbb{Z}_p[X_1,\dots,X_n]$.
Put $r=\prod_{p\in S}p^{m(p)}$. Then $rg,\ r^{-1}h\in\mathbb{Z}_p[X_1,\dots,X_n]$ $\forall$ primes p. Hence $rg,\ r^{-1}h\in\mathbb{Z}[X_1,\dots,X_n]$.

Theorem 2.1 ("Eisenstein"): Let the valuation $|\ |$ on k be discrete with prime element π. Suppose that $f(X)=f_0+\dots+f_nX^n$ has $|f_n|=1$, $|f_j|<1$ $(j<n)$, $|f_0|=|\pi|$. Then $f(X)$ is irreducible in $k[X]$.

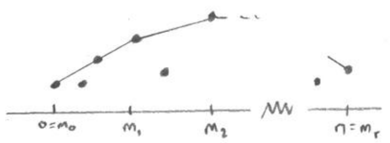
Proof: By Lemma 2.1, if $f(X)$ is reducible in $k[X]$ then it is reducible in $\mathfrak{o}[X]$, say $f(X)=g(X)h(X)$ where $g(X)=g_0+\dots+g_rX^r$, $h(X)=h_0+\dots+h_sX^s$, and $r+s=n$.
Denote by a bar $\bar{\ }$ the map from $\mathfrak{o}$ onto the residue class field, $\mathfrak{o}/\mathfrak{p}$, and also the induced map from $\mathfrak{o}[X]$ to $\mathfrak{o}/\mathfrak{p}[X]$. Then, $\bar f(X)=\bar f_nX^n$, and so $\bar g(X)=\bar g_rX^r$, $\bar h(X)=\bar h_sX^s$.
In particular, $|g_0|<1$, $|h_0|<1$, so $|g_0|\le|\pi|$, $|h_0|\le|\pi|$. Thus, $|f_0|=|g_0h_0|\le|\pi|^2$ – #.

Corollary 1: The polynomial $\phi(X)=X^{p-1}+X^{p-2}+\dots+1=\dfrac{X^p-1}{X-1}$ is irreducible in $\mathbb{Q}_p[X]$.
Proof: $\phi(Y+1)=Y^{p-1}+\binom{p}{1}Y^{p+2}+\dots+\binom{p}{2}Y+\binom{p}{1}$ is an Eisenstein polynomial.

Corollary 2: For any $n\geq1$, the polynomial $\psi(X)=(X^{p^n}-1)/(X^{p^{n-1}}-1)=\phi(X^{p^{n-1}})$ –(*) is irreducible in $\mathbb{Q}_p[X]$.
Proof: Again we put $X=Y+1$, say $\psi(Y+1)=\theta(Y)$. By (*) we have $\theta(0)=\psi(1)=p$.
Further, $\{(Y+1)^{p^{n-1}}-1\}\theta(Y)=\{(Y+1)^{p^n}-1\}$. On mapping the coefficients into the residue class field, as in the proof of the theorem, the two terms in $\{\}$ map to $Y^{p^{n-1}}$ and Y^{p^n}.
Hence $\bar\theta(Y)=Y^{p^n-p^{n-1}}$, so θ is an Eisenstein polynomial.

6.3. Newton Polygon.

k is complete w.r.t $|\ |$.
Let $f(X)=f_0+\dots+f_nX^n\in k[X]$, $f_0\neq0$, $f_n\neq0$. (So $X\nmid f$, $\deg f=n$). To obtain the "Newton Polygon" $\Pi(f)$ of f, we plot in $\mathbb{R}^2$ the pairs $P(j)=(j,\log|f_j|)$ $(f_j\neq0)$.
Then Π is most simply described as the upper boundary of the convex cover of the $P(j)$.
It thus consists of a set of line segments σ_s for $1\le s\le r$ (say), where σ_s joins $P(m_{s-1})$, $P(m_s)$, and $0=m_0<m_1<\dots<m_r=n$. The slope of σ_s is $\gamma_s=\dfrac{\log|f_{m_s}|-\log|f_{m_{s-1}}|}{m_s-m_{s-1}}$, and $\gamma_1>\dots>\gamma_r$.
Every $P(j)$ lies either on or below Π.
Example:



We shall say that f is of type $(l_1,\gamma_1;\dots;l_r,\gamma_r)$, where $l_1=m_1$, $l_s=m_s-m_{s-1}$ $(s>1)$. –(*).
If $r=1$, we say that f is pure. (Not standard terminology)

Theorem 3.1 ("Newton"): Suppose that k is complete and that $f(X) \in k[X]$ is of type (*). Then $f(X) = g_1(X) \cdots g_r(X)$, where $g_s(X)$ is pure of type (l_s, γ_s) $(1 \le s \le r)$.

Note: The Newton polygon is closely related to the norms $\| \ \|_c$ from §6.1
If $\log c = -\gamma_s$, then $\|f_j X^j\|_c = \|f\|$ $(j = m_{s-1}, m_s)$, and $\|f(X) - \sum_{m_{s-1} \le j \le m_s} f_j X^j\| < \|f\|$.
If $\log c$ is distinct from the γ_s, then $\|f_j X^j\| = \|f\|$ for precisely one value of j.

Lemma 3.1: Suppose that $f(X), g(X) \in k[X]$ are pure with the same slope γ. Then $f(X)g(X)$ is also pure of slope γ.

Proof: Let $\log c = -\gamma$. Then $\|f\| = \|f_0\| = \|f_n X^n\|$, and $\|g\| = \|g_0\| = \|g_N X^N\|$ $(N = \deg g)$.
Hence $\|fg\| = \|f_0 g_0\| = \|f_n g_N X^{n+N}\|$, so fg is pure of slope γ.

Lemma 3.2: Suppose f is of type (*) and that g is pure of type (N, γ), where $\gamma < \gamma_r$. Then fg is of type $(l_1, \gamma_1; \cdots; l_r, \gamma_r; N, \gamma)$.

Proof: Let $\log c = -\gamma_s$. Then $\|g(X) - g_0\|_c < \|g\|_c$, since $\gamma < \gamma_s$. Hence, and by above note, $\|f(X)g(X) - g_0 \cdot \sum_{m_{s-1} \le j \le m_s} f_j X^j\|_c < \|fg\|_c$.

Similarly, if we put $\log c = -\gamma$, we have $\|f(X)g(X) - f_n X^n g(X)\|_c < \|fg\|_c$
These inequalities, together with note and purity of g fully determine the Newton polygon of fg, and confirm it is of the stated type.

Lemma 3.3: Let $\| \ \| = \| \ \|_c$ for some c. Let $R(X) \in k[X]$ and suppose that $G(X) = G_0 + \cdots + G_N X^N \in k[X]$ has $\|G_N X^N\| = \|G\|$. Define L, M by: $R(X) = L(X)G(X) + M(X)$, $\deg M(X) < N$. Then $\|L\| \cdot \|G\| \le \|R\|$, $\|M\| \le \|R\|$.

Proof: Let $\deg R = n$, so $\deg L = n - N$. The coefficients of L, ie, $L_{n-N}, L_{n-N-1}, \ldots, L_0$ are determined in order by the equations: $G_N L_{n-N-j} + G_{N-1} L_{n-N-j+1} + \cdots + G_{N-j} L_{n-N} = R_{n-j}$, where R_{n-j} is the coefficient of X^{n-j} in $R(X)$. Using $\|G_N X^N\| = \|G\|$, it follows by induction on j that $\|L_{n-N-j} X^{n-N-j}\| \cdot \|G\| \le \|R\|$. This gives the first part, and the second follows at once.

Lemma 3.4: Let $\| \ \| = \| \ \|_c$ for some c and $f(X) = f_0 + \cdots + f_n X^n \in k[X]$. Suppose there is some $0 < N < n$ such that $\|f_N X^N\| = \|f\|$, $\|f_j X^j\| < \|f\|$ $(j > N)$. Then $f = gh$, where $g, h \in k[X]$ have degrees $N, n-N$ respectively.

Proof: $\exists \Delta < 1$ such that $\|f(X) - \sum^N f_j X^j\| = \Delta \|f\|$. We consider $G, H \in k[X]$ such that $\deg G = N$, $\deg H \le n - N$, and $\|f - G\| \le \Delta \|f\|$, $\|H - 1\| \le \Delta$. — (*)
Define δ by $\|f - GH\| = \delta \|f\|$, so $\delta \le \Delta$.
One such choice is $G^{(0)} = \sum^N f_j X^j$, $H^{(0)} = 1$, $\delta = \Delta$. We shall show in the spirit of Hensel's Lemma that if G, H are given and $\delta > 0$, then we can find G^*, H^* satisfying (*) and for which $\delta^* \le \Delta \delta$.
We have that G satisfies the condition in lemma 3.3. We apply it with $R = f - GH$ and obtain $L, M \in k[X]$ such that $f - GH = LG + M$, $\deg L \le n - N$, $\deg M < N$, $\|L\| \le \delta$, $\|M\| \le \delta \|f\|$
Put $G^* = G + M$, $H^* = H + L$. Then, $\delta^* \|f\| = \|f - G^* H^*\| = \|(H-1)M + ML\| \le \max\{\|H-1\| \cdot \|M\|, \|M\| \cdot \|L\|\} \le \Delta \delta \|f\|$.
Clearly G^*, H^* satisfy (*). If $\delta^* > 0$ we can repeat. Clearly the sequence G, H of polynomials tend to polynomials g, h such that $f = gh$.

Corollary 1: If $f(x) \in k[x]$ is irreducible, then it is pure.

Proof: If f is not pure, we can find c, N satisfying the conditions of the lemma. For example, one can take $-\log c$ to be the slope of the line segment joining P_0 and P_n.

Corollary 2: We can suppose wlog that $h(0) = 1$, $\|h-1\| < 1$.

Proof: For we can replace $h(x)$ by $\{h(0)\}^{-1} h(x)$.

Proof of Theorem 3.1: Let $f(x) = \prod_\lambda h_\lambda(x)$ be an expression of $f(x)$ in irreducibles. By Corollary 1, the $h_\lambda(x)$ are pure. If more than one of the $h_\lambda(x)$ have the same slope δ, then their product is also pure of slope δ. In this way we get an expression of $f(x)$ as the product of polynomials, $g_\mu(x)$ $(1 \le \mu \le M)$, where g_μ is pure of type (q_μ, δ_μ), say, and $\delta_1 > \dots > \delta_M$. By lemma 3.2 and induction, the type of $\prod g_\mu(x)$ is $(q_1, \delta_1; \dots; q_M, \delta_M)$. This must be the type of $f(x)$, so $M = r$ and $q_s = l_s$, $\delta_s = \gamma_s$ $(1 \le s \le r)$. So we are done.

7. Algebraic Extensions, Complete Fields.

7.1 Introduction.

Let $k \subset K$ be fields. Say K is a finite algebraic extension if the relative degree $[K:k]$ is finite. We shall show that if k is complete wrt valuation $|\,|$, there is precisely one extension of $|\,|$ to K. (If $|\,|$ is arch., we saw in Chapter 3 that the only case with $K \ne k$ is $k = \mathbb{R}$, $K = \mathbb{C}$.) We therefore suppose $|\,|$ is non-arch.

If $[K:k] < \infty$ and $A \in K$, we denote by $N_{K/k}(A)$ the relative norm of A, ie, the determinant of the map : $B \to AB$ $(B \in K)$, of $K \to K$, where K is viewed as a k-vector space. Then $N_{K/k}$ gives a homomorphism $K^* \to k^*$. Further $N_{K/k}(a) = a^n$ $(a \in k)$, where $n = [K:k]$.

Theorem 1.1: Let k be complete wrt $|\,|$, and let K be an extension with $[K:k] = n$. Then $\exists$ precisely one extension $\|\,\|$ of $|\,|$ to K. It is given by: $\|A\| = |N_{K/k}(A)|^{1/n}$ $(A \in K)$. Further, K is complete wrt $\|\,\|$.

7.2. Uniqueness.

For this section, we allow $|\,|$ to be archimedean, if it feels like it.

Definition 2.1: Let V be a vector space over the field k, and $|\,|$ a valuation on k satisfying the triangle inequality. A real-valued function $\|\,\|$ on V is called a norm if:

(i) $\|\underline{a}\| > 0$ $\forall\, \underline{a} \in V$, with equality iff $\underline{a} = 0$.

(ii) $\|\underline{a} + \underline{b}\| \le \|\underline{a}\| + \|\underline{b}\|$ $\forall\, \underline{a}, \underline{b} \in V$.

(iii) $\|c\,\underline{a}\| = |c| . \|\underline{a}\|$ for $c \in k$, $\underline{a} \in V$.

Definition 2.2: Two norms $\|\,\|_1, \|\,\|_2$ are said to be equivalent if there are $C_1, C_2 \in \mathbb{R}$ such that $\|\underline{a}\|_1 \le C_2 \|\underline{a}\|_2$, $\|\underline{a}\|_2 \le C_1 \|\underline{a}\|_1$, $\forall\, \underline{a} \in V$.

Note: In an obvious way, a norm induces a metric and hence a topology on V. Equivalent norms induce the same topology.

Lemma 2.1: Suppose k is complete wrt $| \, |$. Then any two norms on the same finite-dimensional k-vector space V are equivalent. Further, V is complete under the induced metrics.

Proof: Let $\underline{e}_1, \dots, \underline{e}_n$ be any k-basis for V. Put $\underline{a} = a_1\underline{e}_1 + \dots + a_n\underline{e}_n$ $(a_j \in k)$, and $\|\underline{a}\|_0 = \max |a_j|$ - (*).
Clearly $\| \, \|_0$ is a norm and V is complete wrt it.
It is enough to show that any norm $\| \, \|$ on V is equivalent to $\| \, \|_0$.
One way is easy: $\|\underline{a}\| = \|\Sigma a_j e_j\| \le \Sigma |a_j| . \|e_j\| \le C_0 \|\underline{a}\|_0$, where $C_0 = \Sigma \|e_j\|$.
It remains to show that $\exists$ C such that $\|\underline{a}\|_0 \le C\|\underline{a}\| \ \forall \ \underline{a} \in V$. - (1)
If not, then for every $\varepsilon > 0$, $\exists$ $\underline{b} = \underline{b}(\varepsilon) \in V$ with $\|\underline{b}\| < \varepsilon \|\underline{b}\|_0$. - (2)
On recalling (*) and permuting the e_j if necessary, we may suppose wlog that $\exists \ \underline{b} = \underline{b}(\varepsilon)$ satisfying (2) and $\|\underline{b}\|_0 = |b_n|$. On replacing $\underline{b}$ by $b_n^{-1}\underline{b}$ we have $\underline{b} = \underline{c} + \underline{e}_n$, where $\underline{c} \in W = \langle e_1, \dots, e_{n-1} \rangle$. So, if (1) is false, we can find a sequence $\underline{c}^{(m)}$ $(m = 1, 2, \dots)$ of elements of W such that $\|\underline{c}^{(m)} + \underline{e}_n\| \to 0$ $(m \to \infty)$.
By (ii) of the definition of a norm, we have $\|\underline{c}^{(l)} - \underline{c}^{(m)}\| \to 0$ $(l, m \to \infty)$.
We use induction on $\dim V = n$. Since W has dimension $n-1$, it is complete under $\| \, \|$.
So $\exists$ $\underline{c}^* \in W$ such that $\|\underline{c}^{(m)} - \underline{c}^*\| \to 0$ $(m \to \infty)$.
Now, $\|\underline{c}^* + \underline{e}_n\| = \lim_{m\to\infty} \|\underline{c}^{(m)} + \underline{e}_n\| = 0$ - # to (i) of definition 2.1.
So (1) holds, and $\| \, \|$ and $\| \, \|_0$ are equivalent.

Corollary 1 (Uniqueness in Theorem 1.1): Let k be complete wrt $| \, |$, and let K be a finite algebraic extension of k. There $\exists$ at most one extension $\| \, \|$ of $| \, |$ to K.

Proof: The function $\| \, \|$ on K, regarded as a finite-dimensional k-vector space, satisfies Definition 2.1, and so is a norm. By the lemma, any two valuations $\| \, \|_1$, $\| \, \|_2$ extending $| \, |$ are equivalent as norms, and so induce the same topology on K. By Lemma 3.2 of chapter 2, they are thus equivalent as valuations, and since they coincide on k, they must be identical.

Corollary 2: Let k be complete wrt $| \, |$ and suppose that $\| \, \|$ is an extension to the finite algebraic extension K of k. Then K is complete wrt $\| \, \|$.

Proof: The last sentence of the statement of the lemma.

7.3 Existence.

To complete the proof of Theorem 1.1, we must show that $\| \, \|$ as defined is a valuation on K extending $| \, |$.
Let $a \in k$. Then $N_{K/k}(a) = a^n$. Hence $\|a\| = |a|$.
Let $A, B \in K$. Then $N_{K/k}(AB) = N_{K/k}(A) N_{K/k}(B)$, so $\|AB\| = \|A\| . \|B\|$. In particular, if $A \neq 0$ we have $\|A\| . \|A^{-1}\| = \|1\| = 1$, so $\|A\| > 0$.
It remains to show that $\|A\| \le 1$ implies $\|1 + A\| \le C$, some C.
Let $F_A(T) = F(T) = T^n + F_{n-1}T^{n-1} + \dots + F_0 \in k[T]$ be the characteristic polynomial of A.
Then $|F_0| = |\pm N_{K/k}(A)| \le 1$. - (*)

Now, $F(T) = \{f(T)\}^r$, some $r>0$, where $f(T)$ is the minimal polynomial for A over k. Since $f(x)$ is irreducible, it is pure (Ch.4, Thm.3.1, Cor 1) and so F is pure (Ch.4. Lemma 3.1). In particular, $F(T) \in \mathfrak{o}[T]$ by $(*)$.
Now, $N_{K/k}(1+A) = (-1)^n F(-1)$, so $\|1+A\| = |F(-1)|^{1/n} \leq 1$, as required.

This concludes Theorem 1.1. Since $\| \ \|$ is unique, we will usually just write $| \ |$.

Corollary 1 (to Theorem 1.1): $\exists$ a unique extension of $| \ |$ to the algebraic closure $\bar{k}$ of k.
Proof: Use Zorn's Lemma.

Corollary 2: Let $A, A' \in K$ be conjugate over k. Then $\|A\| = \|A'\|$.
Proof: They have the same minimal polynomial, so the same norm.
Alternatively, we can suppose that K is normal over k. Then $A' = \sigma A$, some $\sigma \in Gal(K/k)$.
Define $\| \ \|_\sigma$ on K by $\|B\|_\sigma = \|\sigma B\|$. Then $\| \ \|_\sigma$ is an extension of $| \ |$, so $\| \ \|_\sigma = \| \ \|$.

Corollary 3: Let A and $A' \neq A$ be conjugate over k and let $a \in k$. Then $\|a - A\| \geq \|A - A'\|$.
Proof: For otherwise, $\|a - A'\| = \|A - A'\| > \|a - A\|$, contrary to Corollary 2 (with $a - A$ for A).

7.4 Residue Class Fields.

In this section, $k \subset K$ are fields, $[K:k] = n$, and $| \ |$ is a valuation on K wrt which k (and so K) is complete. The ring of integers and maximal ideal for k are $\mathfrak{o}, \mathfrak{p}$, and for K are $\mathcal{O}, \mathcal{P}$. We denote the residue class fields by: $\rho = \mathfrak{o}/\mathfrak{p}$, $P = \mathcal{O}/\mathcal{P}$.

Lemma 4.1: There is a natural injection $\rho \hookrightarrow P$. Further, $f := [P:\rho] \leq n = [K:k]$.
Proof: Any element $b \in \mathfrak{o}$ is in $\mathcal{P}$ iff it is in $\mathfrak{p}$. Hence the inclusion $\mathfrak{o} \hookrightarrow \mathcal{O}$ induces $\rho \hookrightarrow P$.
Let $A_1, \dots, A_{n+1} \in \mathcal{O}$. We shall show that the residue classes $\bar{A}_1, \dots, \bar{A}_{n+1} \in P$ are linearly dependent over ρ. Since $[K:k] = n$, $\exists\ a_1, \dots, a_{n+1}$ (not all zero), such that $\sum a_j A_j = 0$.
We may suppose, wlog, that $\max |a_j| = 1$. Then $a_j \in \mathfrak{o}$ $(1 \leq j \leq n+1)$, and not every residue class $\bar{a}_j \in \rho$ is 0. So $\sum \bar{a}_j \bar{A}_j = 0$, and we have shown $f \leq n$.

Definition 4.1: if $f = n$, we say that the extension K/k is unramified.

Definition 4.2: If $f = 1$, we say that K/k is completely ramified.

Lemma 4.2: L a field, $k \subset L \subset K$. Then $f(K/k) = f(K/L) f(L/k)$.
Proof: Clear.

Let ρ be a field, $\varphi(T) \in \rho[T]$ a polynomial in the indeterminate T. We say that $\varphi(T)$ is inseparable if $\varphi'(T) = 0$ (eg, $\varphi(T) = T^p - b$, where $b \in \rho$ and $p = \mathrm{char}\,\rho$). If φ is not inseparable then it is separable. An element α of some field algebraic over ρ is separable by definition if its minimal polynomial is separable. Clearly then $\varphi'(\alpha) \neq 0$. A finite algebraic extension P/ρ is separable by definition if every $\alpha \in P$ is separable. It can then be shown that

$P = \rho(\beta)$ for some β. Finally, the field ρ is perfect if every finite algebraic extension of ρ is separable.

ρ is perfect iff either (i) char $\rho = 0$, or (ii) char $\rho = p$ and every element is a p-th power. Indeed, if $\varphi(T) = \sum_j a_j T^{pj}$ is inseparable and $a_j = b_j^p$, then $\varphi(T) = (\sum_j b_j T^j)^p$ is reducible. In particular, any finite field is perfect.

Theorem 4.1: K, k, P, ρ as before (at start). Let $\alpha \in P$ be separable over ρ. Then $\exists$ $A \in \alpha$ such that $[k(A) : k] = [\rho(\alpha) : \rho]$. this says that $k(A)/k$ is unramified. Further, $k(A)$ depends only on α.

Proof: Let $\varphi(T) \in \rho[T]$ be the minimum polynomial for α over ρ, so $\varphi'(\alpha) \neq 0$ by hypothesis. Let $\Phi(T) \in \mathfrak{o}[T]$ be any lift of $\varphi(T)$: ie, (i) φ and Φ have the same degree, and (ii) the coefficients of φ are residue classes of those of Φ. Let $A_0 \in \mathcal{O}$ be any element of the residue class α. Then, $|\Phi(A_0)| < 1$, $|\Phi'(A_0)| = 1$.
By Hensel's Lemma, with $k(A_0)$ as groundfield, $\exists$ some $A \in k(A_0) \subset K$ such that $\Phi(A) = 0$, $|A - A_0| < 1$. Then $A \in \alpha$ and $[k(A) : k] = [\rho(\alpha) : \rho]$.
Further, if we suppose that $[k(A_0) : k] = [\rho(\alpha) : \rho]$, then $A \in k(A_0) \subset K$ implies $k(A) = k(A_0)$.

Corollary 1: Suppose that P/ρ is separable. Then $\exists$ a bijection between the fields $M \subset K$ which are unramified over k, and the fields μ with $\rho \subset \mu \subset P$. The field $\mu = \mu(M)$ corresponding to M is $(M \cap \mathcal{O}) \bmod \mathfrak{P}$.

Proof: By the earlier facts about separability, every μ is of the form $\mu = \rho(\alpha)$, some $\alpha \in P$.

Corollary 2: Suppose that P/ρ is separable. $\exists$ a field $k \subset L \subset K$ such that L/k is unramified and such that every $M \subset K$ which is unramified over k is contained in L. Further, K/L is completely ramified.

Proof: L corresponds to P in corollary 1.

Corollary 3: Suppose that ρ is perfect. Then the residue class field of the algebraic closure $\bar{k}$ of k is the algebraic closure of ρ. There is a subfield k_u of $\bar{k}$ such that a finite algebraic extension K/k is unramified precisely when $K \subset k_u$.

Proof: Let $\varphi(T) \in \rho[T]$ be irreducible and $\Phi(T)$ any lift to $k[T]$. Then $\bar{k}$ contains all the roots of $\Phi(T)$, so its residue class field contains all the roots of $\varphi(T)$. Hence the residue class field of $\bar{k}$ is the algebraic closure of ρ. The rest follows from Corollary 2 and Zorn's Lemma.

7.5. Ramification.

We now consider the relation between the value groups G_k and G_K for a finite algebraic extension K/k, when G_k is discrete.

Lemma 5.1: Suppose that $|\,|$ is discrete on k. Then it is discrete on K.

Proof: Follows from definition of $\|\,\|$ in Theorem 1.1.

Definition 5.1: The index $e = [G_K : G_k]$ is called the ramification index.

Lemma 5.2: Let L be a field, $k \subset L \subset K$. Then $e(K/k) = e(K/L)\,e(L/k)$

Proof: Clear.

Recall: An abelian group $\mathfrak{M}$ is an $\mathfrak{o}$-module if for every $a \in \mathfrak{o}$, $A \in \mathfrak{M}$ there is given an element $aA \in \mathfrak{M}$ satisfying the axioms: $1A = A$

$$a(A+B) = aA + aB$$
$$(a+b)A = aA + bA$$
$$(ab)A = a(bA).$$

It is torsion-free if $aA = 0$ implies that either $a = 0$ or $A = 0$. The module $\mathfrak{M}$ is finitely generated if $\exists\, E_1, \dots, E_n \in \mathfrak{M}$ such that every $A \in \mathfrak{M}$ can be written as $a_1E_1 + \dots + a_nE_n$ $(a_j \in \mathfrak{o})$. The set $\{E_1, \dots, E_n\}$ of generators is called a basis if $a_1E_1 + \dots + a_nE_n = 0$ implies $a_1 = \dots = a_n = 0$. (Here, $\mathfrak{o}$ is any ring with a 1).

Lemma 5.3: Let $\mathfrak{o}$ be the ring of integers of a (not necessarily complete) field, k, wrt a valuation $|\,|$. Then every torsion-free finitely-generated $\mathfrak{o}$-module $\mathfrak{M}$ has a basis.

Proof: Let $\{E_1, \dots, E_n\}$ be a set of generators. If they are not a basis, $\exists\, a_1, \dots, a_n \in \mathfrak{o}$, not all zero, such that $a_1E_1 + \dots + a_nE_n = 0$. Wlog, $|a_n| = \max|a_j|$, $a_j = a_n b_j$, $b_j \in \mathfrak{o}$.
Hence, $a_n(b_1E_1 + \dots + b_{n-1}E_{n-1} + E_n) = 0$. Since $\mathfrak{M}$ is torsion-free, $E_n = -b_1E_1 - \dots - b_{n-1}E_{n-1}$ and so $\{E_1, \dots, E_{n-1}\}$ is a set of generators. If it is not a basis, repeat the argument.

Lemma 5.4: Let $k \subset K$ be fields, $|\,|$ a valuation on K. Suppose that:

(i) k is complete wrt $|\,|$.

(ii) $|\,|$ is discrete on both k and K. Define $e = [G_K : G_k]$.

(iii) The residue class field extension P/p is of finite relative degree $[P:p] = f$.

Then the extension K/k is of finite relative degree $[K:k] = ef$.

Moreover: Let Π be a prime element of K and let $B_1, \dots, B_f$ be any lift to $\mathcal{O}$ of a basis of P/p. Then $\mathcal{B} = \{B_i\Pi^j : 1 \le i \le f,\ 0 \le j \le e-1\}$ is an $\mathfrak{o}$-basis of $\mathcal{O}$.

Proof: By the definition of e, we have $|\Pi|^e = |\pi|$, where π is a prime element of k.
We show first that $\mathcal{B}$ is linearly independent over k. If not, we have $\sum_{i,j} a_{ij}B_i\Pi^j = 0$, $-(*)$.
where $a_{ij} \in k$, not all zero. Wlog, $\max|a_{ij}| = 1$, and so $\exists\, I, J$ such that $|a_{IJ}| = 1$, $|a_{ij}| \le |\pi|$ $(1 \le i \le f,\ j < J)$. Then, $|\sum_i a_{iJ}B_i| = 1$, by the definition of the B_i.
Hence,

$$|\sum_i a_{ij}B_i\Pi^j| \begin{cases} \le |\pi| = |\Pi|^e & (j < J) \\ = |\Pi|^J & (j = J) \\ \le |\Pi|^{J+1} & (j > J) \end{cases} \qquad - \#\ \text{to } (*)$$

Hence $\mathcal{B}$ is linearly independent over k, and so over $\mathfrak{o}$.
We now show that $\mathcal{B}$ is a set of generators of $\mathcal{O}$. Let $A \in \mathcal{O}$. By the definition of the B_i, there are $a_{i0} \in \mathfrak{o}$ such that $A - \sum_i a_{i0}B_i = \Pi A_1 \in \Pi\mathcal{O}$, some $A_1 \in \mathcal{O}$.
We repeat the process with A_1, and so on, until we obtain $a_{ij} \in \mathfrak{o}$ such that $A - \sum_{j=0}^{e-1}\sum_i a_{ij}B_i\Pi^j = \Pi^eA_e \in \Pi^e\mathcal{O}$. Since $|\Pi|^e = |\pi|$, we have $\Pi^eA_e = \pi A^{(1)}$, some $A^{(1)} \in \mathcal{O}$.
We now start again, with $A^{(1)}$ instead of A. We get linear combinations C_r of $\mathcal{B}$ with coefficients in $\mathcal{O}$ such that $A - C_0 - \pi C_1 - \dots - \pi^sC_s \in \pi^{s+1}\mathcal{O}$, for every s. On letting $s \to \infty$ and using the completeness of k, we express A as a linear combination of $\mathcal{B}$ with coefficients in $\mathcal{O}$, as required. So $\mathcal{B}$ is an $\mathfrak{o}$-basis for $\mathcal{O}$, and a fortiori a k-basis for K. So done.

Theorem 5.1: Let k be complete w.r.t the discrete valuation $|\ |$ and let K be an extension with finite relative degree $n = [K:k]$. Then $n = ef$.

Proof: Follows at once from Lemma 5.4 and Theorem 1.1.

Corollary: K/k is unramified precisely when $e=1$, and is completely ramified precisely when $e=n$.

7.6. Discriminants.

Let $K \supset k$ be fields with $[K:k] = n < \infty$. Recall that the trace $S_{K/k}(A)$ of an element $A \in K$ is defined to be the trace of the k-linear map $B \to AB$ $(B \in K)$ of K into itself. The trace is a k-linear map of K into k.

Let $A_1, .., A_n$ be any k-basis of K. Write $D(A_1,..,A_n) = \det(S(A_iA_j))_{i,j}$, where $S = S_{K/k}$.

Any other basis $B_1,..,B_n$ is of form $B_i = \sum t_{ij} A_j$, where $t_{ij} \in k$, $T := \det(t_{ij}) \neq 0$.

Clearly, $D(B_1,..,B_n) = T^2 D(A_1,..,A_n)$, by the k-linearity of the trace $\quad -(*)$

Now suppose K/k is separable and let N be a finite normal extension of k which contains K. Then there are n embeddings $\sigma_i : K \to N$ $(1 \le i \le n)$ of K into N which are the identity on k. If $K = k(C)$, these are given by $C \mapsto C^{(i)}$, where $C = C^{(1)}, C^{(2)},.., C^{(n)}$ are the conjugates of C over k. For any basis $A_1,..,A_n$ of K/k we put $\Delta(A_1,..,A_n) = \det(\sigma_i A_j)_{i,j}$, defined up to sign, since the ordering of the σ_i is arbitrary.

Now, $\{\Delta(A_1,..,A_n)\}^2 = \det(\sum_i \sigma_i A_i A_j)_{i,j} = \det(S(A_iA_j))_{i,j} = D(A_1,..,A_n)$.

In particular, we have $\Delta(1, C,.., C^{n-1}) = \prod_{i>j} (\sigma_i C - \sigma_j C) \neq 0$.

Hence, and by $(*)$ above, $D(A_1,..,A_n) \neq 0$ for all bases $A_1,..,A_n$ of K/k. By this and $(*)$:

Lemma 6.1: Let K/k be separable. Then the class of $k^*/(k^*)^2$ given by $D(A_1,..,A_n)$ is the same for all K/k-bases $A_1,..,A_n$.

Definition 6.1: The element of $k^*/(k^*)^2$ just defined is the field-discriminant.

Now suppose k is complete w.r.t a discrete valuation $|\ |$. Then we can consider $\mathfrak{o}$-bases $A_1,..,A_n$ of $\mathfrak{O}$. If $B_1,..,B_n$ is another such basis then we have $(t_{ij}) \in \mathfrak{o}$ and so $T \in \mathfrak{o}$. The inverse transformation to this has determinant T^{-1}, so $T^{-1} \in \mathfrak{o}$, so $|T| = 1$, or, in other words, $T \in \mathfrak{U}$, where $\mathfrak{U}$ is the group of units in k. Hence we have:

Lemma 6.2: Suppose that k is complete w.r.t the discrete valuation $|\ |$ and that K/k is separable. Then $D(A_1,..,A_n)$ for all $\mathfrak{o}$-bases $A_1,..,A_n$ of $\mathfrak{O}$ lies in the same non-zero class of $\mathfrak{o}$ modulo $\mathfrak{U}^2$.

Definition 6.2: This class of $\mathfrak{o}$ modulo $\mathfrak{U}^2$ just defined is the discriminant of K/k, and is denoted $D_{K/k}$.

In particular, $|D(A_1,..,A_n)|$ is the same for all $\mathfrak{o}$-bases $A_1,..,A_n$. We shall denote it by $|D_{K/k}|$.

Theorem 6.1: Suppose k is complete w.r.t the discrete valuation $|\,|$. Suppose that K/k is separable and that the corresponding residue class P/p is separable. Then $|D_{K/k}|=1$ iff K/k is unramified.

Proof: ($\Rightarrow$) Suppose that K/k is ramified, so we have a basis $\mathcal{B} = \{B_i \Pi^j : 1 \le i \le f,\ 0 \le j \le e-1\}$ of $\mathcal{O}$ with $e>1$. The valuation $|\,|$ extends to the normal extension N of k containing K and in our earlier notation, we have $|\sigma_i(B_i\Pi^j)| = |B_i\Pi^j| = |\Pi|^j$, by Thm 1, Cor. 2. Hence a whole column of the matrix defining $\Delta(\mathcal{B})$ has value <1. Thus $|\Delta(\mathcal{B})|<1$ and $|D_{K/k}| = |\Delta(\mathcal{B})|^2 < 1$.

($\Leftarrow$) Suppose that K/k is unramified. Denote the map from $\mathcal{O}$ to $P = \mathcal{O}/\mathfrak{p}$ by a bar $^-$. We shall show below (Lemma 6.3) that $\overline{S_{K/k}(A)} = S_{P/p}(\bar{A})$, for all $A \in \mathcal{O}$. Using a suffix K/k or P/p to denote the field extension under consideration, it follows from Definition 6.2 that $\overline{D_{K/k}(B_1,\dots,B_n)} = D_{P/p}(\bar{B}_1,\dots,\bar{B}_n)$. RHS $\neq 0$, by Lemma 6.1 applied to P/p. But then we get $|D_{K/k}(B_1,\dots,B_n)| = 1$, as required.

Corollary: $|D_{K/k}| \le |\pi|^{(e-1)f}$

Proof: Since $|\sigma_i(B_i\Pi^j)| = |B_i\Pi^j| = |\Pi|^j$, f of the columns defining $\Delta(\mathcal{B})$ are divisible by Π^j for $j=1,2,\dots,e-1$. Hence, $|D(\mathcal{B})| = |\Delta(\mathcal{B})|^2 \le |\Pi|^{2(1+2+\dots+(e-1))f} = |\Pi|^{e(e-1)f} = |\pi|^{(e-1)f}$.

Lemma 6.3: Suppose K/k is unramified and P/p is separable. For any $A \in \mathcal{O}$, the characteristic equation of $\bar{A} \in P$ is obtained from that of A by applying the map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p}$ to the coefficients.

Proof: Since $B_1,\dots,B_n$ is a basis for K/k, the characteristic equation of A is obtained by eliminating $B_1,\dots,B_n$ from the equations $AB_i = \sum_j a_{ij}B_j$ $(a_{ij} \in k)$. Since $B_1,\dots,B_n$ is an $\mathfrak{o}$-basis for $\mathcal{O}$, we have $a_{ij} \in \mathfrak{o}$, and can map into the residue class fields: $\bar{A}\bar{B}_i = \sum_j \bar{a}_{ij}\bar{B}_j$. But $\bar{B}_1,\dots,\bar{B}_n$ is a basis of P/p and the result follows.

Lemma 6.4: Let k be a finite extension of $\mathbb{Q}_2$. Then $D_{k/\mathbb{Q}_2} \equiv 1$ or $0 \pmod 4$.

Note: By definition, $D_{k/\mathbb{Q}_2}$ is an element of $\mathbb{Z}_2$ modulo U^2, where U is the group of 2-adic units. Since U^2 is precisely the set of $v \in \mathbb{Z}_2$ satisfying $v \equiv 1 \pmod 8$, this congruence makes sense.

Proof: Suppose first that $k/\mathbb{Q}_2$ is ramified. Then $D_{k/\mathbb{Q}_2} \equiv 0 \pmod 4$, by Corollary above, except possibly when $e=2, f=1$. Then k is a quadratic extension of $\mathbb{Q}_2$. Since it is ramified, it must be one of $\mathbb{Q}_2(\sqrt{\pm 2})$, $\mathbb{Q}_2(\sqrt{\pm 6})$, $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{-5})$, by Ch. 4, Lemma 3.3, Cor. It can be verified (see example 5) that these satisfy the congruence.
Suppose now that $k/\mathbb{Q}_2$ is unramified, and let $\mathcal{B}$ be a $\mathbb{Z}_2$-basis of the integers of k. Then $D(\mathcal{B}) = \Delta(\mathcal{B})^2 \equiv 1 \pmod 2$, where $\Delta(\mathcal{B}) \in k$. Hence either $\Delta(\mathcal{B}) \in \mathbb{Q}_2$ or $\mathbb{Q}_2(\Delta(\mathcal{B}))$ is an unramified quadratic extension. In the first case we have $D(\mathcal{B}) \equiv 1 \pmod 8$, and in the second we have $\mathbb{Q}_2(\Delta(\mathcal{B})) = \mathbb{Q}_2(\sqrt{5})$, and so $D(\mathcal{B}) \equiv 5 \pmod 8$.

7.7: Completely Ramified Extensions.

Recall that an Eisenstein polynomial is one satisfying the conditions of Theorem 2.1, Ch. 6.

Theorem 7.1: Let $| \; |$ be discrete on k. A finite algebraic extension K/k is completely ramified iff $K = k(B)$, where B is a root of an Eisenstein polynomial.

Proof: ($\Leftarrow$) Suppose that B is the root of an Eisenstein polynomial, say $f_0 + \dots + f_n B^n = 0$, where $|f_n| = 1$, $|f_j| < 1$ $(j < n)$, $|f_0| = \pi$. Then $|B|^n = |\pi|$. Hence $e(k(B)/k) \geq n$.

($\Rightarrow$) Suppose that K/k is completely ramified and $[K:k] = n$, and let Π be a prime element of K. Then $1, \Pi, \dots, \Pi^{n-1}$ are linearly independent over k, because their values are in distinct cosets of the value group G_K modulo G_k. There must be an equation $\Pi^n + f_{n-1}\Pi^{n-1} + \dots + f_0 = 0$ $(f_j \in k)$.

Here, $|f_j| < 1$ because two of the summands must have the same value, and $|f_0| = |\Pi|^n = |\pi|$

8. $\wp$-adic Fields.

8.1. Introduction

Definition 1.1: Let the field k be complete wrt the (non-arch.) valuation $| \; |$. We say that k is a $\wp$-adic field if

(i) k has characteristic 0.

(ii) $| \; |$ is discrete

(iii) the residue class field ρ is finite.

Lemma 1.1: The valued field k is a $\wp$-adic field iff it is a finite extension of $\mathbb{Q}_p$ for some p.

Proof: ($\Leftarrow$) Suppose that k is a finite extension of $\mathbb{Q}_p$. Then it is a $\wp$-adic field by Lemmas 4.1 and 5.1 of Chapter 7.

($\Rightarrow$) Let k be a $\wp$-adic field. Then $k \supset \mathbb{Q}$ by (i) of the definition. Since the residue class field ρ is finite (iii), it has characteristic p for some prime p. Hence the valuation on k induces a valuation equivalent to the p-adic valuation.
Hence $\mathbb{Q}_p \subset k$, since k is complete. We are now in the situation described by Lemma 5.4 of Chapter 7, and conclude that $[k:\mathbb{Q}_p] < \infty$.

Lemma 1.2: A field k of characteristic 0 complete wrt a non-arch. valuation is a $\wp$-adic field iff its ring $\mathfrak{o}$ of integers is compact.

Proof: Lemma 1.5 of Chapter 4.

Definition 1.1: Let q be the cardinality of the residue class field of the $\wp$-adic field k. The renormalised valuation $\| \; \|_k$ on k is determined by $\|\pi\|_k = q^{-1}$, where π is a prime element. (When $k = \mathbb{Q}_p$, this coincides with $| \; |_p$)

Lemma 1.3: Suppose that $[k:\mathbb{Q}_p]=n$. Then $\|a\|_k = |a|^n$, where $| \, |$ is the valuation which coincides with $| \, |_p$ on $\mathbb{Q}_p$.

Proof: It is enough to show this for one non-unit a, and we choose $a=p$. We have $\|p\|_k = \|\pi\|_k^e$, where e is the ramification of $k/\mathbb{Q}_p$. Further, $q=p^f$, where f is the degree of the residue class field extension. Hence, $\|p\|_k = q^{-e} = p^{-ef} = p^{-n}$.

Corollary 1: $\|a\|_k = |N_{k/\mathbb{Q}_p}(a)|_p$

Proof: Cf. Theorem 1.1 of Chapter 7.

Corollary 2: Let $a \in k \subset K$. Then $\|a\|_K = \|a\|_k^{[K:k]}$

Proof: Clear.

We will consider briefly the appropriate renormalization of the ordinary absolute value $| \, |_\infty$. The only complete fields to consider are $\mathbb{R}$ and $\mathbb{C}$.

Definition 1.2: $\|a\|_{\mathbb{R}} = |a|_\infty$, $\|a\|_{\mathbb{C}} = |a|_\infty^2$.

Lemma 1.4: (i) $\|A\|_{\mathbb{C}} = \|N_{\mathbb{C}/\mathbb{R}}(A)\|_{\mathbb{R}}$ for $A \in \mathbb{C}$

(ii) $\|a\|_{\mathbb{C}} = \|a\|_{\mathbb{R}}^2$ for $a \in \mathbb{R} \subset \mathbb{C}$.

Proof: Clear.

8.2 Unramified Extensions.

Lemma 2.1: For each $n=1,2,\dots$ there is precisely one unramified extension k of $\mathbb{Q}_p$ with $[k:\mathbb{Q}_p]=n$. It is the splitting field of $X^q - X$, $q=p^n$ over $\mathbb{Q}_p$.

Proof: The residue class field of $\mathbb{Q}_p$ is the finite field $\mathbb{F}_p$ of p elements. By the theory of finite fields, for every n there is precisely one extension ρ of $\mathbb{F}_p$ of degree n. It has q elements, and the multiplicative group ρ^* of non-zero elements is cyclic, so $\alpha^q = \alpha$ for all $\alpha \in \rho$, and ρ is the splitting field of $X^q - X$ over $\mathbb{F}_p$.
By Ch. 7, Thm 4.1, Cor. 3, there is precisely one unramified field extension k of $\mathbb{Q}_p$ whose residue class field is ρ. Put $f(X) = X^q - X$, so $f'(X) = qX^{q-1} - 1$ and $|f'(a)| = 1 \ \forall a \in \mathfrak{o}$.
Hence by Hensel's Lemma, for every $\alpha \in \rho = \mathfrak{o}/\mathfrak{p}$ there is some $\hat{\alpha} \in \alpha \subset \mathfrak{o}$ such that $f(\hat{\alpha}) = 0$.
Hence $X^q - X$ is split by k. The splitting field of $X^q - X$ over $\mathbb{Q}_p$ cannot be smaller than k because its residue class field must contain at least q elements. The concludes the proof.

Definition 2.1: The $\hat{\alpha} \in \alpha$ defined above is the Teichmüller representative of α.

Corollary 1: Let k be a $\mathfrak{p}$-adic field and let the cardinality of its residue class field be q. For every $n=1,2,\dots$ there is precisely one unramified extension K of k of relative degree n. It is the splitting field over k of $X^Q - X$, $Q=q^n$.
The extension K/k is normal with cyclic Galois group. There is a generator σ of this group which induces the automorphism $\beta \mapsto \beta^q$ of the residue class field P of K.

Definition 2.2: The σ just defined is the Frobenius automorphism of K/k.

Proof: The residue class field P must be the field of cardinality Q. Hence K must contain the field L given by Lemma 2.1 but with Q instead of q. Hence K is the composite of L and k. The field L is the splitting field of $X^Q - X$ over $\mathbb{Q}_p$, so K is the splitting field over k.

Every splitting field is normal. By the theory of finite fields, P/ρ is cyclic and a generating automorphism is $\beta \mapsto \beta^q$. Since K/k is unramified, its Galois group is that of P/ρ.

Corollary 2: The unramified closure k_u of the $\mathfrak{p}$-adic field k is obtained by adjoining the mth roots of unity for all m prime to the residue class field characteristic p.

Proof: By Corollary 1, k_u is obtained by adjoining the (q^n-1)th roots of unity for $n = 1, 2, \ldots$. For every m prime to p, there is an n such that $q^n - 1$ is divisible by m.

Lemma 2.2: Let k be a $\mathfrak{p}$-adic field, let q be the cardinality of ρ and let $b \in \mathfrak{o}$. Then $\hat{b} = \lim_{t\to\infty} b^{q^t}$ exists. Further $\hat{b}$ is the Teichmüller representative of (the residue class) of b.

Proof: If $|b| < 1$, then $\hat{b} = 0$, and we are done. Otherwise, $b^q = b + c$, where $|c| < 1$. Then, $b^{q^2} = (b+c)^q = b^q + cqb^{q-1} + \cdots + c^q$. Hence $|b^{q^2} - b^q| \leq \max\{|q|.|c|, |c|^2\} < |c|$. Continuing in this way, we that the limit exists. Clearly $\hat{b}^q = \hat{b}$, so $\hat{b}$ is the Teichmüller representative.

9. Algebraic Extensions (Incomplete Fields).

9.1. Introduction.

Let K/k be a finite algebraic extension and let $| \ |$ be a valuation on k. We do not suppose that k is complete, and ask what extensions there are of $| \ |$ to K. We will often consider arch. and non-arch. valuations together.

Suppose that the valuation $| \ |_1$ on K extends $| \ |$ and let K_1 be the completion of K wrt it. Then K_1 contains the completion $\bar{k}$ of k wrt $| \ |$. A basis $\{B_i\}$ of K/k clearly generates K_1 as a $\bar{k}$-vector space. There is, however, no reason to expect that the B_i, considered as elements of K_1, will be linearly independent over $\bar{k}$, and we conclude only that $[K_1 : \bar{k}] \leq [K : k]$. Multiplication gives K_1 a natural structure as a K-module.

We shall also require the tensor product, $\bar{k} \otimes_k K$. This can be described as follows:
Let $B_1, \ldots, B_n$ be a basis for K/k. There are $c_{ijl} \in k$ such that $B_i B_j = \sum_l c_{ijl} B_l$. — (1)
Then $\bar{k} \otimes_k K$ is an n-dimensional $\bar{k}$-vector space, with a basis which we identify with the B_i: $\bar{k} \otimes_k K = \{a_1 B_1 + \cdots + a_n B_n : a_1, \ldots, a_n \in \bar{k}\}$.
It has a ring structure, multiplication being defined by (1), and by $\bar{k}$-linearity.
We identify K in $\bar{k} \otimes_k K$ with the linear combinations of the B_i with coefficients in k.

Theorem 1.1: Let K/k be a separable extension with $[K:k]=n<\infty$, and let $|\,|$ be any valuation on k. Then there are just finitely many extensions $|\,|_j$ $(1\le j\le J)$ of $|\,|$ to K.
Let $\bar{k}$ be the completion of k wrt $|\,|$, and K_j the completion of K wrt $|\,|_j$.
Then $\bar{k}\otimes_k K=\bigoplus_j K_j$. - (1)
In particular, $\sum_j [K_j:\bar{k}]=[K:k]$. - (2)

By (1) we mean that every $C\in\bar{k}\otimes_k K$ can be expressed uniquely as $C=\sum_j C_j$ $(C_j\in K_j)$.
if $D=\sum D_j$, then $C+D=\sum(C_j+D_j)$, $CD=\sum C_jD_j$, where $C_j+D_j,\ C_jD_j\in K_j$.
Further, $aC=\sum_j aC_j$, $BC=\sum_j BC_j$ for $a\in\bar{k}$, $B\in K$, where $aC_j, BC_j\in K_j$.

9.2. Proof of Theorem and Corollaries.

Lemma 2.1: Let $K=k(A)$ be a separable extension and let $F(X)\in k[X]$ be the minimum polynomial for A. Let $\bar{k}$ be the completion of k wrt any valuation $|\,|$. Let $F(X)=\varphi_1(X)\cdots\varphi_J(X)$ be the decomposition of $F(X)$ into irreducibles in $\bar{k}[X]$. Then the φ_j are distinct.
Let $K_j=\bar{k}(B_j)$, where B_j is a root of $\varphi_j(X)$. Then there is an injection $K=k(A)\hookrightarrow K_j=\bar{k}(B_j)$ extending $k\hookrightarrow\bar{k}$ under which $A\to B_j$. Denote by $|\,|_j$ the valuation on K induced by the injection and the unique valuation on K_j extending $|\,|$.
Then the $|\,|_j$ are precisely the extensions of $|\,|$ to K. Further, K_j is the completion of K wrt $|\,|_j$

Proof: Let $\|\,\|$ be any valuation of K extending $|\,|$ and let $\bar{K}$ be the completion wrt it.
Then $\bar{k}\subset\bar{K}$ and $A\in K\subset\bar{K}$. Further $\bar{k}(A)$ is complete, by Thm 1.1 of Ch. 7 if $|\,|$ is non-arch., and by Thm 1.1 of Ch. 3 if $|\,|$ is arch. Hence $\bar{K}=\bar{k}(A)$. Let $\varphi(X)\in\bar{k}[X]$ be the minimum polynomial for A over $\bar{k}$. Since $F(A)=0$ we have $\varphi(X)\mid F(X)$, and so φ is one of the φ_j, and we have the situation described in the lemma.
We now go in the opposite direction. Let B_j be as stated. Then $F(B_j)=0$, and so the extensions $k(A)=K$ and $k(B_j)\subset\bar{k}(B_j)=K_j$ are isomorphic. We can thus identify K with a subfield of K_j, and have the situation already discussed.
It remains to show the φ_j are distinct. If not, $F(X)$ and $F'(X)$ would have a common factor in $\bar{k}[X]$. Since it could be determined by the Euclidean algorithm, there would be a common factor in $k[X]$, and this is impossible since F is irreducible and separable, by hypothesis.

Proof of Theorem 1.1: In the above notation, we have the following obvious ring isomorphisms:
$\bar{k}[X]/F(X)\cong\bar{k}\otimes_k K$, $\bar{k}[X]/\varphi_j(X)\cong K_j$,
where in both cases $X\mapsto A$. After Lemma 2.1, we are done, following the following general result of commutative algebra:

Lemma 2.2: Let k be a field, $F(X)=\varphi_1(X)\cdots\varphi_J(X)$, with the $\varphi_j(X)\in k[X]$ coprime in pairs.
Then $k[X]/F(X)\cong\bigoplus_j k[X]/\varphi_j(X)$.

Proof: The two sides have the same dimension as k-vector spaces. Let θ be the map LHS $\to$ RHS induced by the identity map on $k[X]$ and let $f(X)$ mod $F(X)$ be in the kernel.
Then $f(X)\equiv 0 \bmod \varphi_j(X)$ $\forall j$. Hence $f(X)\equiv 0 \bmod F(X)$, ie θ is a monomorphism.
Because of the equality of dimensions, θ is an isomorphism, as required.

Corollary 1: Let $A \in K$. Then the trace and norm are given by: $S_{K/k}(A) = \sum_j S_{K_j/\bar{k}}(A)$ and $N_{K/k}(A) = \prod_j N_{K_j/\bar{k}}(A)$.

Proof: By definition, $S_{K/k}$ and $N_{K/k}$ are respectively the trace and the determinant of the k-linear map induced on K by multiplication with A. So done, as $\bar{k} \otimes_k K = \bigoplus_j K_j$.

Corollary 2: $\prod_j |A|_j^{n(j)} = |N_{K/k}(A)|$, where $n(j) = [K_j : \bar{k}]$.

Proof: Immediate from Cor. 1 and Ch. 7, Thm 1.1.

Corollary 3: Suppose that either $\bar{k}$ is $\mathfrak{p}$-adic or is $\mathbb{R}$ or $\mathbb{C}$. Let $\| \|$ be the renormalisation of $| |$ on k introduced in Ch. 8, §1, and let $\| \|_j$ be the renormalisation of $| |_j$ on K_j. Then $\prod_j \|A\|_j = \|N_{K/k}(A)\|$

Proof: Lemma 1.3 Cor 2, or Lemma 1.4, Ch. 8.

9.3 Integers and Discriminants.

Let $| |$ be non-arch., we shall call $A \in K$ a (semi-local) integer if $|A|_j \le 1 \ \forall j$. The ring of such A will be denoted by $\mathfrak{O}$. Clearly, $\mathfrak{O} = \bigcap_j \{K \cap \mathfrak{O}_j\}$, where $\mathfrak{O}_j$ is the ring of integers of the complete field K_j. Denote the ring of integers of $k, \bar{k}$ by $\mathfrak{o}, \bar{\mathfrak{o}}$.

Lemma 3.1: $\mathfrak{O} \otimes_{\mathfrak{o}} \bar{\mathfrak{o}} = \bigoplus_j \mathfrak{O}_j$.

Proof: We use the identification in Thm 1.1, in which we identify $A \in K$ with $1 \otimes A \in \bar{k} \otimes_k K$. In terms of these identifications, $\mathfrak{O} = K \cap \{\bigoplus_j \mathfrak{O}_j\}$.

Let B_{ij} $(1 \le i \le n_j)$ be an $\bar{\mathfrak{o}}$-basis of $\mathfrak{O}_j$ $(1 \le j \le J)$. By Thm 3.1, Ch. 2, we can choose $C_{ij} \in K$ such that $|C_{ij} - B_{ij}|_j < 1$, $|C_{ij}|_l < 1$ $(l \ne j,\ 1 \le l \le J)$

Then $C_{ij} \in \bigoplus_j \mathfrak{O}_j$. Indeed, the matrix $\mathfrak{M}$ representing the C_{ij} in terms of the B_{ij} is congruent to the identity modulo the maximal ideal $\bar{\mathfrak{p}}$ of $\bar{\mathfrak{o}}$.

It follows that the C_{ij} are an $\bar{\mathfrak{o}}$-basis of $\bigoplus_j \mathfrak{O}_j$. But $C_{ij} \in K$, so the C_{ij} are an $\mathfrak{o}$-basis of $\mathfrak{O}$. So we are done.

Definition 3.1: Let $A_1, \dots, A_n$ be an $\mathfrak{o}$-basis of $\mathfrak{O}$. Then the element of $\mathfrak{o}/\mathfrak{U}^2$ given by $\det(S_{K/k} A_i A_j)$ is the (semi-local) discriminant $D_{K/k}$.

Lemma 3.2: $D_{K/k} \mapsto \prod_j D_{K_j/\bar{k}}$ under the homomorphism $\mathfrak{o}/\mathfrak{U}^2 \to \bar{\mathfrak{o}}/\bar{\mathfrak{U}}^2$ induced by $k \hookrightarrow \bar{k}$. In particular, $|D_{K/k}| = \prod_j |D_{K_j/\bar{k}}|$.

Proof: We are interested only up to a factor in $\bar{\mathfrak{U}}^2$ and so may take for $A_1, \dots, A_n$ an $\bar{\mathfrak{o}}$-basis of $\bar{\mathfrak{o}} \otimes_{\mathfrak{o}} \mathfrak{O}$. As in the proof of lemma 3.1, we take for $\{A_1, \dots, A_n\}$ the union of $\bar{\mathfrak{o}}$-bases $\{B_{ij}\}$ $(1 \le i \le n_j)$ of $\mathfrak{O}_j$. Then $B_{ij} B_{uv} = 0$ for $j \ne v$ and by §2, Cor 1, the matrix $(S_{K/k} A_i A_j)$ becomes a chain of submatrices along the diagonal.

The determinant of the jth submatrix is: $\det(S_{K_j/\bar{k}} B_{uj} B_{vj})_{u,v}$, which maps into $D_{K_j/\bar{k}} \in \bar{\mathfrak{o}}/\bar{\mathfrak{U}}^2$.

Corollary: All the $| |_j$ are unramified iff $|D_{K/k}| = 1$

Proof: For $|D_{K_j/\bar{k}}| \le 1$, with equality only when $K_j/\bar{k}$ is unramified, by Thm 6.1, Ch. 7.

Lemma 3.3: Let $K = k(B)$ be an extension of degree n and suppose that B is a root of $F(x)$, where $F(x) \in \mathfrak{o}[X]$ has top coefficient 1. Suppose further that $|F'(B)|_j = 1$ for all extensions $|\,|_j$ of $|\,|$ to k. Then all the $|\,|_j$ are unramified and $1, B, .., B^{n-1}$ is an $\mathfrak{o}$-basis of $\mathfrak{O} = \bigcap_j \mathfrak{O}_j$.

Proof: It follows at once from $F(x) \in \mathfrak{o}[x]$ that $B \in \mathfrak{O}$. Let $G(x) \in k[x]$ be the minimum polynomial for B (with top coefficient 1), so $F(X) = G(X)H(X)$ for some $H(X) \in k[X]$. By "Gauss' Lemma" 2.1 (Ch 6), we have $G(X), H(X) \in \mathfrak{o}[X]$. Now, $F'(B) = G'(B)H(B)$, where $|H(B)|_j \le 1 \;\forall_j$ (as $B \in \mathfrak{O}$, $G, H \in \mathfrak{o}[X]$). Hence, $|G'(B)|_j = 1$ for all j. Thus the conditions of the theorem are satisfied with G instead of F. It is therefore enough to prove the lemma under the additional assumption that F is the minimum polynomial of B, which we now suppose.

Let $\mathcal{H}$ be the splitting field of F over k, let $B_1, .., B_n \in \mathcal{H}$ be the roots, and let $\|\,\|$ be any extension of $|\,|$ to $\mathcal{H}$.

The discriminant of the set $1, B, .., B^{n-1}$ of elements of $\mathfrak{O}$ is $D(1, B, .., B^{n-1}) = \prod_{i<j} (B_i - B_j)^2 = \pm \prod_j F'(B_j)$.

Now, $\|F'(B_j)\| = |F'(B)|_l$ for the valuation $|\,|_l$ with $l = l(j)$ induced by $\|\,\|$ on $k(B)$ by the injection $B \to B_j$. Hence, $|D(1, B, .., B^{n-1})| = \|D(1, B, .., B^{n-1})\| = 1$. $-(*)$

Now let $A_1, .., A_n$ be an $\mathfrak{o}$-basis of $\mathfrak{O}$, say $B^{j-1} = \sum_i t_{ji} A_i$ $(1 \le j \le n)$, with $t_{ji} \in \mathfrak{o}$.

Then, $|D(1, B, .., B^{n-1})| = |T|^2 . |D(A_1, .., A_n)| = |T|^2 . |D_{K/k}|$, where $T = \det(t_{ji})$.

By $(*)$, we have $|T| = 1$, $|D_{K/k}| = 1$. Hence $1, B, .., B^{n-1}$ is a basis, and the $|\,|_j$ are unramified by Lemma 3.2, Corollary.

9.4. Application to Cyclotomic Fields.

We denote by $\mathbb{Q}^{(m)}$ the splitting field of $X^m - 1$ over $\mathbb{Q}$. Since obviously $\mathbb{Q}^{(2m)} = \mathbb{Q}^{(m)}$ for m odd, we shall assume that either $2 \nmid m$ or $2^2 \mid m$. $-(*)$

The roots of unity of order precisely m are the roots of the polynomial

$$F_m(x) = \prod_{d \mid m} (X^d - 1)^{\mu(m/d)} \in \mathbb{Z}[X],$$

where μ is the Möbius function, and φ is Euler's totient function.

Hence there are $\varphi(m)$ roots of unity M of order precisely m, and clearly $\mathbb{Q}^{(m)} = \mathbb{Q}(M)$, for any one of them. The non-trivial fact which we shall require is that $F_m(x)$ is irreducible in $\mathbb{Q}^{(m)}[X]$, or, what is the same thing, that $\mathbb{Q}^{(m)}/\mathbb{Q}$ has degree $\varphi(m)$.

Lemma 4.1: (i) $\mathbb{Q}^{(m)}/\mathbb{Q}$ has degree $\varphi(m)$

(ii) A prime q is ramified in $\mathbb{Q}^{(m)}$ precisely when $q \nmid m$ (with convention $(*)$ for $q = 2$)

Proof: Suppose $q \nmid m$. Then the q-adic valuation is unramified in $\mathbb{Q}^{(m)}$ by lemma 3.3, with $F(x) = X^m - 1$ and $B = M$. Now suppose that $m = q^\alpha$ (with $\alpha \ge 2$ if $q = 2$). Then the degree of $\mathbb{Q}^{(m)}$ is $q^\alpha - q^{\alpha-1} = \varphi(q^\alpha)$ and q is completely ramified, by Cor's 1, 2 to Thm 2.1, Ch. 6, and Thm 7.1, Ch 7.

Finally, suppose that $m = q^\alpha l$, where $q \nmid l$. Clearly $\mathbb{Q}^{(m)}$ is the composite of the two fields $\mathbb{Q}^{(q^\alpha)}$ and $\mathbb{Q}^{(l)}$ (which gives (ii) for $q \mid m$)

Let $I = \mathbb{Q}^{(q^\alpha)} \cap \mathbb{Q}^{(l)}$. Then q is completely ramified in I (since $I \subset \mathbb{Q}^{(q^\alpha)}$), but is also unramified (since $I \subset \mathbb{Q}^{(l)}$). The only possibility is that $I = \mathbb{Q}$.

Since $\mathbb{Q}^{(m)}$ is a normal (Galois) extension of $\mathbb{Q}$ it follows that the degree of $\mathbb{Q}^{(m)}$ is the product of the degrees of $\mathbb{Q}^{(q^\alpha)}$ and $\mathbb{Q}^{(l)}$.

This proves (i) by induction on the number of primes dividing m.

We now consider the semi-local situation when $k = \mathbb{Q}$, $\mathrm{II} = \mathrm{II}_p$ and $K = \mathbb{Q}^{(m)}$ for some m and some prime p.

Lemma 4.2: Let $\mathfrak{O}$ be the set of elements of $\mathbb{Q}^{(m)}$ which are integral for all valuations extending the p-adic valuation. Then a $\mathbb{Z}_p$-basis of $\mathfrak{O}$ is given by $1, M, .., M^{\varphi-1}$, where M is any primitive mth root of unity and $\varphi = \varphi(m)$.

Proof: As we saw in the proof of lemma 4.1, this follows immediately from lemma 3.3 when $p \nmid m$. Now suppose that $m = p^{\alpha} l$, $p \nmid l$ and let $L = 1 - N$ for some primitive p^{α}-th root of unity N. Then any $A \in \mathbb{Q}^{(m)}$ is uniquely of the form $A = \sum_{j=0}^{\psi-1} L^j A_j$ – (*), where $\psi = \varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$; and $A_j \in \mathbb{Q}^{(l)}$. Further, $A \in \mathfrak{O}$ precisely when all the A_j are in $\mathfrak{O} \cap \mathbb{Q}^{(l)}$.
By the unramified case, a basis $\mathfrak{O} \cap \mathbb{Q}^{(l)}$ is given by the powers of a primitive l-th root of unity. The result now follows on putting $L = 1 - N$ in (*). (More precisely, this shows that $\mathfrak{O} \subset \mathbb{Z}_p[M]$, so $\mathfrak{O} = \mathbb{Z}_p[M]$ and this has basis $1, M, .., M^{\varphi-1}$, since M is integral).