## LECTURE NOTES ON VALUATION THEORY

PETE L. CLARK

## Contents

1. Absolute values and valuations ..... 1
1.1. Basic definitions ..... 1
1.2. Absolute values and the Artin constant ..... 2
1.3. Equivalence of absolute values ..... 4
1.4. Artin-Whaples Approximation Theorem ..... 5
1.5. Archimedean absolute values ..... 7
1.6. Non-archimedean norms and valuations ..... 9
1.7. $\quad R$-regular valuations; valuations on Dedekind domains ..... 11
1.8. Some Classification Theorems ..... 12
References ..... 16

## 1. Absolute values and valuations

### 1.1. Basic definitions.

All rings are commutative with unity unless explicit mention is made otherwise.
A norm, on a field $k$ is a map $|\mid: k \rightarrow \mathbb{R} \geq 0$ satisfying:
(V1) $|x|=0 \Longleftrightarrow x=0$.
(V2) $\forall x, y \in k,|x y|=|x||y|$.
(V3) $\forall x, y \in k,|x+y| \leq|x|+|y|$.
Example 1.1.0: On any field $k$, define $\left|\left.\right|_{0}: k \rightarrow \mathbb{R}^{\geq 0}\right.$ by $0 \mapsto 0, x \in k \backslash\{0\} \mapsto 1$. This is immediately seen to be an absolute value on $k$ (Exercise!), called the trivial norm. In many respects it functions as an exception in the general theory.

Example 1.1.1: The standard norm on the complex numbers: $|a+b i|=\sqrt{a^{2}+b^{2}}$. The restriction of this to $\mathbb{Q}$ or to $\mathbb{R}$ will also be called "standard".

Example 1.1.2: The $p$-adic norm on $\mathbb{Q}$ : write $\frac{a}{b}=p^{n} \frac{c}{d}$ with $\operatorname{gcd}(p, c d)=1$ and put $\left|\frac{a}{b}\right|_{p}=p^{-n}$.

We will see more examples later. In particular, to each prime ideal in a Dedekind

[^0]domain we may associate a norm. This remark serves to guarantee both the plenitude of examples of norms and their link to classical algebraic number theory.

Exercise 1.1: Let $\mid \|$ be a norm on the field $k$. Show that for all $a, b \in k$, $||a|-|b|| \leq|a-b|$.

Exercise 1.2: Let $R$ be a ring which is not the zero ring (i.e., $1 \neq 0$ in $R$ ). Let $\|: R \rightarrow \mathbb{R}^{\geq 0}$ be a map which satisfies (V1) and (V2) (with $k$ replaced by $R$ ) above. a) Show that $|1|=1$.
b) Show that $R$ is an integral domain, hence has a field of fractions $k$.
c) Show that there is a unique extension of $\|$ to $k$, the fraction field of $R$, satisfying (V1) and (V2).
d) Suppose that moreover $R$ satisfies (V3). Show that the extension of part b) to $k$ satisfies (V3) and hence defines a norm on $k$.
e) Conversely, show that every integral domain admits a mapping | | satisfying (V1), (V2), (V3).

Exercise 1.3:
a) Let || be a norm on $k$ and $x \in k$ a root of unity. ${ }^{1}$ Show $|x|=1$.
b) Show that for a field $k$, TFAE:
(i) Every nonzero element of $k$ is a root of unity.
(ii) The characteristic of $k$ is $p>0$, and $k / \mathbb{F}_{p}$ is algebraic.
c) If $k / \mathbb{F}_{p}$ is algebraic, show that the only norm on $k$ is $\left|\left.\right|_{0}\right.$.

Remark: In Chapter 2 we will see that the converse of Exercise 1.3c) is also true: any field which is not algebraic over a finite field admits at least one (and in fact infinitely many) nontrivial norm.

Exercise 1.4: Let $(k,| |$ be a normed field, and let $\sigma: k \rightarrow k$ be a field automorphism. Define $\sigma^{*}| |: k \rightarrow \mathbb{R}$ by $x \mapsto|\sigma(x)|$.
a) Show that $\sigma^{*}| |$ is a norm on $k$.
b) Show that this defines a left action of $\operatorname{Aut}(k)$ on the set of all norms on $k$ which preserves equivalence.
c) Let $d$ be a squarefree integer, not equal to 0 or 1 . Let $k=\mathbb{Q}(\sqrt{d})$ viewed as a subfield of $\mathbb{C}$ (for specificity, when $d<0$, we choose $\sqrt{d}$ to lie in the upper half plane, as usual), and let $|\mid$ be the restriction of the standard valuation on $\mathbb{C}$ to $k$. Let $\sigma: \sqrt{d} \mapsto-\sqrt{d}$ be the nontrivial automorphism of $k$. Is $\sigma^{*}| |=| |$ ? (Hint: the answer depends on $d$.)

### 1.2. Absolute values and the Artin constant.

For technical reasons soon to be seen, it is convenient to also entertain the following slightly version of (V3): for $C \in \mathbb{R}^{>0}$, let (V3C) be the statement
(V3C) $\forall x \in k,|x| \leq 1 \Longrightarrow|x+1| \leq C$.
A mapping $\left|\mid: k \rightarrow \mathbb{R}^{\geq 0}\right.$ satisfying (V1), (V2) and (V3C) for some $C$ will be

[^1]called an absolute value.
For an absolute value $\left|\mid\right.$ on a field $k$, we define the Artin constant $C_{k}$ to be the infimum of all $C \in \mathbb{R}^{>0}$ such that $|\mid$ satisfies (V3C).

Exercise 1.5: Let || be an absolute value on $k$.
a) Show that || satisfies (V3C) for some $C$, then $C \geq 1$.
b) Let $C_{k}$ be the Artin constant. Show that || satisfies $\left(\mathrm{V} 3 C_{k}\right)$.
c) Compute $C_{k}$ for the standard norm on $\mathbb{C}$ and the $p$-adic norms on $\mathbb{Q}$.

Lemma 1. Let $k$ be a field and $|\mid$ an absolute value, and $C \in[1, \infty)$. Then the following are equivalent:
(i) $\forall x \in k,|x| \leq 1 \Longrightarrow|x+1| \leq C$.
(ii) $\forall x, y \in k,|x+y| \leq C \max (|x|,|y|)$.

Proof. Assume (i) and let $x, y \in k$. Without loss of generality we may assume that $0<|x| \leq|y|$. Then $\left|\frac{x}{y}\right| \leq 1$, so $\left|\frac{x}{y}+1\right| \leq C$. Multiplying through by $|y|$ gives

$$
|x+y| \leq C|y|=C \max (|x|,|y|) .
$$

Now assume (ii) and let $x \in k$ be such that $|x| \leq 1$. Then

$$
|x+1| \leq C \max (|x|,|1|)=C \max (|x|, 1)=C
$$

Lemma 2. Let $k$ be a field and $\|$ an absolute value with Artin constant $C$. Then || is a norm iff $C \leq 2$.

Proof. $(\Longrightarrow)$ Let $|\mid$ be a norm on $k$, and let $x \in k$ be such that $| x \mid \leq 1$. Then

$$
|x+1| \leq|x|+|1|=|x|+1 \leq 1+1=2 .
$$

$(\Longleftarrow)$ Suppose $C \leq 2$. Let $x, y \in k$. Without loss of generality, we may assume that $0<|x| \leq|y|$. Then $\left|\frac{x}{y}\right| \leq 1$, so $\left|1+\frac{x}{y}\right| \leq C \leq 2$. Multiplying through by $y$, we get $|x+y| \leq 2|y|=2 \max (|x|,|y|)$. Applying this reasoning inductively, we get that for any $x_{1}, \ldots, x_{2^{n}} \in k$ with $0<\left|x_{1}\right| \leq \ldots \leq\left|x_{2^{n}}\right|$, we have

$$
\left|x_{1}+\ldots+x_{2^{n}}\right| \leq 2^{n} \max _{i}\left|x_{i}\right| .
$$

Let $r$ be an integer such that $n \leq 2^{r}<2 n$. Then

$$
\begin{equation*}
\left|x_{1}+\ldots+x_{n}\right|=\left|x_{1}+\ldots+x_{n}+0+\ldots+0\right| \leq 2^{r} \max _{i}\left|x_{i}\right| \leq 2 n \max _{i}\left|x_{i}\right| \tag{1}
\end{equation*}
$$

Applying this with $x_{1}=\ldots=x_{n}=1$ gives that $|n| \leq 2 n$. Moreover, by replacing the max by a sum, we get the following weakened version of (1):

$$
\left|x_{1}+\ldots+x_{n}\right| \leq 2 n \sum_{i=1}^{n}\left|x_{i}\right| .
$$

Finally, let $x, y \in k$ be such that $0<|x| \leq|y|$. Then for all $n \in \mathbb{Z}^{+}$,

$$
\begin{aligned}
&|x+y|^{n}=\left|\sum_{i=0^{n}}\binom{n}{i} x^{i} y^{n-i}\right| \leq 2(n+1) \sum_{i=0}^{n}\left|\binom{n}{i}\right||x|^{i}|y|^{n-i} \\
& \leq 4(n+1) \sum_{i=0}^{n}\binom{n}{i}|x|^{i}|y|^{n-i}=4(n+1)(|x|+|y|)^{n} .
\end{aligned}
$$

Taking $n$th roots and the limit as $n \rightarrow \infty$ gives $|x+y| \leq|x|+|y|$.
Why absolute values and not just norms?
Lemma 3. Let $\left|\mid: k \rightarrow \mathbb{R}^{\geq 0}\right.$ be an absolute value with Artin constant $C$. Put

$$
\left.\left|\left.\right|^{\alpha}: k \rightarrow \mathbb{R}^{\geq 0}, x \mapsto\right| x\right|^{\alpha} .
$$

a) The map $\left|\left.\right|^{\alpha}\right.$ is an absolute value with Artin constant $C^{\alpha}$.
b) If $\left.|\mid$ is a norm, $|\right|^{\alpha}$ need not be a norm.

Exercise 1.6: Prove Lemma 3.
This is the point of absolute values: the set of such things is closed under the operation of raising to a power, whereas the set of norms need not be.

Moreover, Lemma 3 suggests a dichotomy for absolute values. We say an absolute value is non-Archimedean if the Artin constant is equal to 1 (the smallest possible value). Conversely, if the Artin constant is greater than one, we say that the Artin constant is Archimedean.

For example, on $k=\mathbb{Q}$, $p$-adic norm $\left|\left.\right|_{p}\right.$ is non-Archimedean, whereas the standard absolute value $\left.\right|_{\infty}$ is Archimedean with Artin constant 2.

Exercise 1.7:
Let || be an absolute value on $l$, and let $k$ be a subfield of $l$.
a) Show that the restriction of $\|$ to $k$ is an absolute value on $k$.
b) If $\|$ is a norm on $l$, then the restriction to $k$ is a norm on $k$.

### 1.3. Equivalence of absolute values.

Two absolute values $\left|\left.\right|_{1},| |_{2}\right.$ on a field $k$ are equivalent if there exists $\alpha \in \mathbb{R}^{>0}$ such that $\left.\left|\left.\right|_{2}=| |_{1}^{\alpha}\right.$. When convenient, we write this as $|\right|_{1} \sim| |_{2}$.

By a place on a field $k$, we mean an equivalence class of absolute values. ${ }^{2}$ It is easy to check that this is indeed an equivalence relation on the set of absolute values on a field $k$. Moreover, immediately from Lemma 3 we get:

Corollary 4. Each absolute value on a field is equivalent to a norm.
Theorem 5. Let $\left|\left.\right|_{1},| |_{2}\right.$ be two nontrivial absolute values on a field $k$. TFAE:
(i) There exists $\alpha \in \mathbb{R}^{>0}$ such that $\left|\left.\right|_{1} ^{\alpha}=| |_{2}\right.$.
(ii) $\forall x \in k,|x|_{1}<1 \Longrightarrow|x|_{2}<1$.
(iii) $\forall x \in k,|x|_{1} \leq 1 \Longrightarrow|x|_{2} \leq 1$.
(iv) $\forall x \in k$, all of the following hold:

$$
\begin{aligned}
& |x|_{1}<1 \Longleftrightarrow|x|_{2}<1, \\
& |x|_{1}>1 \Longleftrightarrow|x|_{2}>1, \\
& |x|_{1}=1 \Longleftrightarrow|x|_{2}=1 .
\end{aligned}
$$

[^2]Remark: This may seem like a strange way to organize the equivalences, but it will be seen to be helpful in the proof, which we give following [Wei, Thm. 1-1-4].

Proof. We shall show (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) $\Longrightarrow$ (i). That (i) $\Longrightarrow$ (ii) (and, in fact, all the other properties) is clear.
(ii) $\Longrightarrow$ (iii): let $x \in k$ be such that $|x|_{1}=1$. We must show that $|x|_{2}=1$. Since $\left|\left.\right|_{1}\right.$ is nontrivial, there exists $a \in k$ with $0<|a|_{1}<1$, and then by (ii) we have $0<|a|_{2}<1$. Then, for all $n \in \mathbb{Z}^{+},\left|x^{n} a\right|_{1}<1$, so $\left|x^{n} a\right|_{2}<1$, so $|x|_{2}<|a|_{2}^{-\frac{1}{n}}$. Taking $n$ to infinity gives $|x|_{2} \leq 1$. We may apply the same argument to $x^{-1}$, getting $|x|_{2} \geq 1$.
(iii) $\Longrightarrow$ (iv): Choose $c \in k$ such that $0<|c|_{2}<1$. Then for sufficiently large $n$,

$$
|x|_{1}<1 \Longrightarrow|x|_{1}^{n} \leq|c|_{1} \Longrightarrow\left|\frac{x^{n}}{c}\right|_{1} \leq 1 \Longrightarrow|x|_{2}^{n} \leq|c|_{2}<1 \Longrightarrow|x|_{2}<1
$$

So far we have shown (iii) $\Longrightarrow$ (ii). As in the proof of (ii) $\Longrightarrow$ (iii) we have $|x|_{1}=1 \Longrightarrow|x|_{2}=1$. Moreover

$$
|x|_{1}>1 \Longrightarrow\left|\frac{1}{x}\right|_{1}<1 \Longrightarrow\left|\frac{1}{x}\right|_{2}<1 \Longrightarrow|x|_{2}>1
$$

This establishes (iv).
(iv) $\Longrightarrow$ (i): Fix $a \in k$ such that $|a|_{1}<1$. Then $|a|_{2}<1$, so

$$
\alpha=\frac{\log |a|_{2}}{\log |a|_{1}}>0 .
$$

We will show that $\left|\left.\right|_{2}=| |_{1}^{\alpha}\right.$. For this, let $x \in k$, and put, for $i=1,2$,

$$
\gamma_{i}=\frac{\log |x|_{i}}{\log |a|_{i}}
$$

It suffices to show $\gamma_{1}=\gamma_{2}$. Let $r=\frac{p}{q}$ be a rational number (with $q>0$ ). Then

$$
\begin{gathered}
r=\frac{p}{q} \geq \gamma_{1} \Longleftrightarrow p \log |a|_{1} \leq q \log |x|_{1} \\
\Longleftrightarrow\left|a^{p}\right|_{1} \geq\left|x^{q}\right|_{1} \Longleftrightarrow\left|\frac{x^{q}}{a^{p}}\right|_{1} \leq 1 \Longleftrightarrow\left|\frac{x^{q}}{a^{p}}\right|_{2} \leq 1 \\
\Longleftrightarrow p \log |a|_{2} \geq q \log |x|_{2} \Longleftrightarrow \frac{p}{q} \geq \gamma_{2} .
\end{gathered}
$$

Exercise 1.8: Let || be an absolute value on a field $k$. Show that || is Archimedean (resp. non-Archimedean) iff every equivalent absolute value is Archimedean (resp. non-Archimedean).

### 1.4. Artin-Whaples Approximation Theorem.

Theorem 6. (Artin-Whaples) Let $k$ be a field and $\left|\left.\right|_{1}, \ldots,| |_{n}\right.$ be inequivalent nontrivial norms on $k$. Then for any $x_{1}, \ldots, x_{n} \in k$ and any $\epsilon>0$, there exists $x \in k$ such that

$$
\forall i, 1 \leq i \leq n,\left|x-x_{i}\right|_{i}<\epsilon .
$$

Our proof closely follows [Art, §1.4].

Proof. Step 1: We establish the following special case: there exists $a \in k$ such that $|a|_{1}>1,|a|_{i}<1$ for $1<i \leq n$.
Proof: We go by induction on $n$. First suppose $n=2$. Then, since $\left.\left|\left.\right|_{1}\right.$ and $|\right|_{2}$ are inequivalent and nontrivial, by Theorem 5 there exist $b, c \in k$ such that $|b|_{1}<1$, $|b|_{2} \geq 1,|c|_{1} \geq 1,\left|c_{2}\right|<1$. Put $a=\frac{c}{b}$.

Now suppose the result holds for any $n-1$ norms, so that there exists $b \in k$ with $|b|_{1}>1$ and $|b|_{i}<1$ for $1<i \leq n-1$. Using the $n=2$ case, there is $c \in k$ such that $|c|_{1}>1$ and $|c|_{n}<1$.
Case 1: $|b|_{n} \leq 1$. Consider the sequence $a_{r}=c b^{r}$. Then for all $r \in \mathbb{Z}^{+}$we have $\left|a_{r}\right|_{1}>1$ while $\left|a_{r}\right|_{n}<1$. For sufficiently large $r,\left|a_{r}\right|_{i}<1$ for all $2 \leq i \leq n$, so we may take $a=a_{r}$.
Case 2: $|b|_{n}>1$. This time, for $r \in \mathbb{Z}^{+}$, we put

$$
a_{r}=\frac{c b^{r}}{1+b^{r}}
$$

Then for $i=1$ and $i=n$,

$$
\lim _{r \rightarrow \infty}\left|a_{r}-c\right|_{i}=\lim _{r \rightarrow \infty}|c|_{i} \frac{\left|b^{r}-\left(1+b^{r}\right)\right|_{i}}{\left|1+b^{r}\right|_{i}}=\lim _{r \rightarrow \infty} \frac{|c|_{i}}{\left|1+b^{r}\right|_{i}}=0
$$

so for sufficiently large $r$ we have

$$
\left|a_{r}\right|_{1}=|c|_{1}>1 \text { and }\left|a_{r}\right|_{n}=|c|_{n}<1
$$

On the other hand, for $1<i<n$,

$$
\left|a_{r}\right|_{i}=\frac{|c|_{i}|b|_{i}^{r}}{\left|1+b^{r}\right|_{i}} \leq|c|_{i}\left|b_{i}\right|^{r}<1
$$

Therefore we may take $a=a_{r}$ for sufficiently large $r$.
Step 2: We claim that for any $\delta>0$, there exists $a \in k$ such that $\left||a|_{1}-1\right|<\delta$ and $|a|_{i}<\delta$ for $1<i \leq n$.
Proof: If $b$ is such that $|b|_{1}>1$ and $|b|_{i}<1$ for $1<i \leq n$, then the computations of Step 1 show that we may take $a_{r}=\frac{b^{r}}{1+b^{r}}$ for sufficiently large $r$.
Step 3: Fix $\delta>0$. By Step 2, for each $1 \leq i \leq n$, there exists $a_{i} \in k$ such that $\left||a|_{i}-1\right|<\delta$ and for all $j \neq i,\left|a_{i}\right|_{j}<\delta$. Put $A=\max _{i, j}\left|x_{i}\right|_{j}$. Take

$$
x=a_{1} x_{1}+\ldots+a_{n} x_{n} .
$$

Then

$$
\left|x-x_{i}\right|_{i} \leq\left|a_{i} x_{i}-x_{i}\right|_{i}+\sum_{j \neq i}\left|a_{j} x_{j}\right|_{i} \leq A \delta+(n-1) A \delta=n A \delta .
$$

Thus taking $\delta<\frac{\epsilon}{n A}$ does the job.
Remark: Theorem 6 also goes by the name weak approximation. By any name, it is the most important elementary result in valuation theory, playing a role highly analogous to that of the Chinese Remainder Theorem in commutative algebra. On other hand, when both apply the Chinese Remainder Theorem is subtly stronger, in a way that we will attempt to clarify at little later on.

### 1.5. Archimedean absolute values.

In the land of Archimedean absolute values, there is one theorem to rule them all. It is as follows.

Theorem 7. (Big Ostrowski Theorem) Let $k$ be a field and || $\left.\right|_{1}$ an Archimedean absolute value on $k$. Then there exists a constant $\alpha \in \mathbb{R}^{>0}$ and an embedding $\iota: k \hookrightarrow \mathbb{C}$ such that for all $x \in k,|x|_{1}=|\iota(x)|_{\infty}^{\alpha}$. In other words, up to equivalence, every Archimedean absolute value arises by embedding $k$ into the complex numbers and restricting the standard norm.

Theorem 7 is a somewhat annoyingly deep result: every known proof of it from first principles seems to take several pages. It immediately implies all of the other results in this section, and conversely these results - and more! - are used in its proof. Indeed, to prove Big Ostrowski it is convenient to use aspects of the theory of completions, so the proof is deferred until Chapter 2. (In fact, the proof of Big Ostrowski was not presented in the 2010 course at all and was only added to these notes in July of 2010. The implicit message here - that this is an important result whose proof may nevertheless be safely skipped on a first reading - seems valid.)

For a field $k$, let $\mathbb{Z} \cdot 1$ be the additive subgroup generated by 1 . Recall that if $k$ has characteristic 0 , then $\mathbb{Z} \cdot 1$ is isomorphic to the integers, whereas if $k$ has characteristic $p>0, \mathbb{Z} \cdot 1 \cong \mathbb{F}_{p} .{ }^{3}$

Proposition 8. Let $\|$ be an absolute value on a field $k$. TFAE:
(i) || is non-Archimedean.
(ii) $|\mathbb{Z} \cdot 1|$ is bounded.

Proof. The implication (i) $\Longrightarrow$ (ii) follows from the remark preceding the statement of Proposition 8. Now suppose (ii): for specificity, suppose that there exists $M>0$ such that $|n \cdot 1| \leq M$ for all $n \in \mathbb{Z}$. Let $a, b \in k$ and $n \in \mathbb{Z}^{+}$. Then

$$
|a+b|^{n}=\left|(a+b)^{n}\right|=\left|\sum_{i=0}^{n}\binom{n}{i} a^{i} b^{n-i}\right| \leq M \sum_{i=0}^{n}|a|^{i}|b|^{n-i} \leq M \max (|a|,|b|)^{n}
$$

Taking $n$th roots of both sides and $\lim _{n \rightarrow \infty}$ gives the desired result.
Corollary 9. An absolute value on a field of positive characteristic is non-Archimedean.
Lemma 10. (Ostrowski Lemma) Every Archimedean absolute value on $\mathbb{Q}$ is equivalent to the standard Archimedean norm $\left|\left.\right|_{\infty}\right.$.

Proof. Let || be an Archimedean absolute value on $\mathbb{Q}$. By Proposition 8, || is unbounded on the integers, so we may define $N$ to be the least positive integer such that $|N|>1$. Let $\alpha \in \mathbb{R}^{>0}$ be such that $|N|=N^{\alpha}$. Our task is to show that $|n|=n^{\alpha}$ for all $n \in \mathbb{Z}$. We show separately that $|n| \leq n^{\alpha}$ and $|n| \geq n^{\alpha}$.

Step 1: For any $n \in \mathbb{Z}^{+}$, consider its base $N$ expansion:

$$
n=\sum_{i=0}^{\ell} a_{i} N^{i}
$$

[^3]with $0 \leq a_{i}<N, a_{\ell} \neq 0$. (Of course $\ell$ depends on $n$ and $N$.) Then
$$
|n| \leq \sum_{i=0}^{\ell}\left|a_{i}\right| N^{\alpha i}
$$

Note that $n \geq N^{\ell}$. Also, by definition of $N$, we have $\left|a_{i}\right| \leq 1$ for all $i$. So

$$
|n| \leq \sum_{i=0}^{\ell} N^{\alpha i}=N^{\alpha \ell} \sum_{i=0}^{\ell}\left(N^{-\alpha}\right)^{i} \leq n^{\alpha} \sum_{i=0}^{\infty} N^{-\alpha i}=C_{1} n^{\alpha}
$$

where $C_{1}=\sum_{i=0}^{\infty} N^{-\alpha i}$, a constant. Now let $A$ be a positive integer. Applying the above inequality with $n^{A}$ in place of $n$, we get

$$
|n|^{A} \leq C_{1} n^{\alpha A} .
$$

Taking $A$ th roots and the limit as $A$ approaches infinity gives

$$
|n| \leq n^{\alpha}
$$

Step 2: Keeping $N$ and $\ell=\ell(n)$ as above, we have $N^{\ell} \leq n<N^{\ell+1}$. Then

$$
\left|N^{\ell+1}\right|=\left|N^{\ell+1}-n+n\right| \leq\left|N^{\ell+1}-n\right|+|n|
$$

so

$$
\begin{gathered}
|n| \geq\left|N^{\ell+1}\right|-\left|N^{\ell+1}-n\right| \geq N^{\alpha(\ell+1)}-\left(N^{\ell+1}-n\right)^{\alpha} \\
\geq N^{\alpha(\ell+1)}-\left(N^{\ell+1}-N^{\ell}\right)^{\alpha}=N^{\alpha(\ell+1)}\left(1-\left(1-\frac{1}{N}\right)^{\alpha}\right)=C_{2} n^{\alpha}
\end{gathered}
$$

where $C_{2}=1-\left(1-\frac{1}{N}\right)^{\alpha}$, a constant. Arguing as above, we get $|n| \geq n^{\alpha}$.
Theorem 11. (Computation of the Artin constant) Let $k$ be a field and $|\mid$ an absolute value on $k$.
a) The Artin constant $C_{k}$ of $k$ is $\max (|1|,|2|)=\max (1,|2|)$.
b) For any subfield $l$ of $k$, the Artin constant of the restriction of $\left|\mid\right.$ to $l$ is $C_{k}$.

Proof. (E. Artin) a) The absolute value || is non-Archimedean iff (Proposition 1.6) $C_{k}=1$ iff $\max (1,|2|)=1$, so we may assume that it is Archimedean. In this case, $k$ contains $\mathbb{Q}$ and by Propsition $1.7|\mid$ restricts to an Archimedean absolute value on $\mathbb{Q}$. If $\left|\left.\right|_{\infty}\right.$ denotes the standard Archimedean norm on $\mathbb{Q}$, then by the Little Ostrowski Theorem (Theorem 1.13), there exists $\beta>0$ such that the restriction of $\left|\left.\right|_{\mathbb{Q}} \text { is }\right|_{\infty}^{\beta}$. On the other hand, let $\alpha>0$ be such that $C_{k}=2^{\alpha}$. Thus the conclusion of part a) is equivalent to $\alpha=\beta$.

Let $a, b, a_{1}, \ldots, a_{m} \in k$. Assuming without loss of generality that $0<|a| \leq|b|$, we get $\left|\frac{a}{b}\right| \leq 1$ so $\left|\frac{a}{b}+1\right| \leq 2^{\alpha}$, hence

$$
|a+b| \leq 2^{\alpha} \max (|a|,|b|)
$$

Indeed, this argument is familiar from the proof of Lemma 1.1. Similarly adapting that proof, we get

$$
\left|a_{1}+\ldots+a_{m}\right| \leq(2 m)^{\alpha} \max _{i}\left|a_{i}\right|
$$

In particular, we have

$$
|a+b|^{m}=\left|(a+b)^{m}\right| \leq(2(m+1))^{\alpha} \max _{i}\left|\binom{m}{i}\right||a|^{i}|b|^{m-i}
$$

Since $\sum_{i=0}^{n}\binom{m}{i}=2^{m}$, we have

$$
\left|\binom{m}{i}\right|=\binom{m}{i}^{\beta} \leq 2^{m \beta}
$$

Thus

$$
|a+b|^{m} \leq(2(m+1))^{\alpha} 2^{m \beta}(\max (|a|,|b|))^{m} .
$$

Taking $m$ th roots and the limit as $m \rightarrow \infty$, we get

$$
|a+b| \leq 2^{\beta} \max (|a|,|b|)
$$

so that $C_{k}=2^{\alpha} \leq 2^{\beta}$. Since

$$
|1+1|=2^{\beta}=2^{\beta} \max (|1|,|1|)
$$

we also have $2^{\beta} \leq 2^{\alpha}$, so $\alpha=\beta$.
b) This follows immediately from part a), as the computation of the Artin constant depends only on the restriction of the absolute value to its prime subring.

### 1.6. Non-archimedean norms and valuations.

Exercise 1.9: Let $(k,| |)$ be a normed field.
a) Show that $\forall a, b \in k,||a|-|b|| \leq|a-b|$.

For the remainder of the exercise, we suppose that the norm is non-Archimedean.
b) Suppose $|a|>|b|$. Show that $|a+b|=|a|$.
c) $\forall n \in \mathbb{Z}^{+}$and $x_{1}, \ldots, x_{n} \in k,\left|x_{1}+\ldots+x_{n}\right| \leq \max _{i}\left|x_{i}\right|$.
d) (Principle of domination) Suppose $x_{1}, \ldots, x_{n} \in k$ and $\left|x_{i}\right|<\left|x_{1}\right|$ for all $i>1$. Show that $\left|x_{1}+\ldots+x_{n}\right|=\left|x_{1}\right|$.

Exercise 1.9 d ) can be restated as: if in a finite collection of elements, there is a unique element of maximal norm, then that element "dominates" in the sense that the norm of it is the norm of the sum. Although this result does not lie any deeper than the non-Archimedean triangle inequality, its usefulness cannot be overstated: if you are trying to prove estimates on the norm of a sum of terms in a non-Archimedean field, always expect to use the principle of domination.

Until further notice, we let $(k,| |)$ be a non-Archimedean normed field.
Exercise 1.10: Define

$$
R=\{x \in k| | x \mid \leq 1\}
$$

and

$$
\mathfrak{m}=\{x \in k| | x \mid<1\} .
$$

Show that $R$ is a ring and that $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{m}$.

Thus $R$ is a local ring, called the valuation ring of $(k,| |)$.
Remark: More generally, an integral domain $R$ is called a valuation ring if for every $x \in k^{\times}$, at least one of $x, x^{-1}$ lies in $R$.

Exercise 1.11: Show that two non-Archimedean norms on a field $k$ are equivalent iff their valuation rings are equal.

Exercise 1.12: Let $R$ be a valuation ring.
a) Show that $R^{\times}$is the set of elements $x \in k^{\times}$such that both $x$ and $x^{-1}$ lie in $R$.
b) Show that $R \backslash R^{\times}$is an ideal of $R$ and hence is the unique maximal ideal of $R$ : $R$ is a local ring.

In the non-Archimedean case it is often fruitful to consider, in place of the norm || itself, its logarithm. This goes as follows:

A (rank one) valuation on a field $k$ is a map $v: k \rightarrow \mathbb{R} \cup\{\infty\}$ such that:
(V1) $v(x)=\infty \Longleftrightarrow x=0$.
(V2) For all $x, y \in k, v(x y)=v(x)+v(y)$.
(V3) For all $x, y \in k, v(x+y) \geq \min (v(x), v(y))$.
Exercise 1.13: Show that $v: 0 \mapsto-\infty, k^{\times} \mapsto 0$ is a valuation on $k$, called trivial.
Two valuations $v$ and $v^{\prime}$ on $k$ are equivalent if there exists $c>0$ such that $v^{\prime}=c v$.
Exercise 1.14: Let $k$ be a field and $v$ a valuation on $k$.
a) Show that $\Gamma:=v\left(k^{\times}\right)$is a subgroup of $(\mathbb{R},+)$. It is called the value group.
b) Show that a valuation is trivial iff its value group is $\{0\}$.

A valuation is called discrete if $\Gamma$ is a nontrivial discrete subgroup of $(\mathbb{R},+)$.
c) Show that every discrete subgroup of $(\mathbb{R},+)$ is infinite cyclic.
d) Deduce that every discrete valuation is equivalent to one with value group $\mathbb{Z}$. Such a discrete valuation is said to be normalized.

Exercise 1.15: Let $k$ be a field and $c \in(1, \infty)$.
a) If $\|$ is a non-Archimedean norm on $k$, show $v=-\log _{c}| |$ is a valuation on $k$.
b) If $v$ is a valuation on $k$, then $\left|\mid=c^{-v}\right.$ is a non-Archimedean norm on $k$, with valuation ring $R=\{x \in k \mid v(x) \geq 0\}$.
c) Show that different choices of $c$ yield equivalent norms.

Theorem 12. Let $v$ be a nontrivial valuation on a field $k$ with valuation ring $R$ and maximal ideal $\mathfrak{m}$. TFAE:
(i) $v$ is discrete.
(ii) There is an element $\pi \in R$ such that $\mathfrak{m}=(\pi)$.
(iii) The valuation ring $R$ is a PID.
(iv) $R$ is a Noetherian.

A valuation ring satisfying the equivalent conditions (ii) - (iv) is called a discrete valuation ring or a $\boldsymbol{D V R}$.
Proof. (i) $\Longrightarrow$ (ii): If $v$ is discrete, then by Exercise 1.14 we may as well assume that the value group is $\mathbb{Z}$. Let $\pi \in k$ be such that $v(\pi)=1$. Then it is easily seen that $\mathfrak{m}=(\pi)$.
(ii) $\Longrightarrow$ (i): If $\mathfrak{m}=(\pi)$, then necessarily $\pi$ is an element of minimal positive valuation, so $v$ is discrete.
(ii) $\Longrightarrow$ (iii): This is similar to - but easier than! - the proof that $\mathbb{Z}$ is a PID. Namely, since $(i i) \Longrightarrow(i)$, every ideal contains an element of minimal positive valuation, and one readily shows such an element is a generator.
(iii) $\Longrightarrow$ (iv): a ring is Noetherian iff every ideal is finitely generated, so of course a PID is Noetherian.
(iv) $\Longrightarrow$ (ii): we may assume that $\mathfrak{m}=\left\langle x_{1}, \ldots, x_{n}\right\rangle$ with $v\left(x_{1}\right) \leq \ldots \leq v\left(x_{n}\right)$. Then for all $i \geq 2, v\left(\frac{x_{i}}{x_{1}}\right) \geq 0$, so $\frac{x_{i}}{x_{1}} \in R$, so $x_{1} \mid x_{i}$, so $\mathfrak{m}=\left\langle x_{1}\right\rangle$.

The moral here is that the discrete valuations are by far the easiest to understand. Thus it is natural to wonder whether we really need to bother with non-discrete valuations. The answer is yes, at least in certain circumstances. The following exercise gives an indication of this.

Exercise 1.16: Let $A$ be an abelian group, written additively. Recall that $A$ is divisible if for all $x \in A$ and $n \in \mathbb{Z}^{+}$, there exists $y \in A$ such that $n y=x$. (Equivalently, the multiplication by $n$ map $[n]: A \rightarrow A$ is surjective.)
a) Observe that no nontrivial discrete subgroup of $\mathbb{R}$ is divisible.
b) Show a quotient of a divisible group is divisible.
c) Show that if $k$ is algebraically closed, then $k^{\times}$[which is not written additively: too bad!] is a divisible abelian group.
d) Deduce that an algebraically closed field admits no discrete valuation.

Exercise 1.17: For any field $k$, let $R=k[[t]]$ be the ring of formal power series with $k$-coefficients and $k((t))$ its fraction field, the field of formal Laurent series $\sum_{n=N}^{\infty} a_{n} t^{n}$.
a) Show that for any ring $S$, the units of $S[[t]]$ are precisely the formal power series whose constant term is a unit in $S$.
b) Show that a nonzero $f \in k[[t]]$ may be uniquely written as $f=t^{N} u$ with $u \in R^{\times}$.
c) Show that $f \mapsto N$ is a discrete valuation on $k[[t]]$.

Exercise 1.18: Let $f$ be a field, $F=f((t))$, and $\bar{F}$ an algebraic closure of $F$.
Let $R=F\left[\left\{t^{\frac{1}{n}}\right\}_{n \in \mathbb{Z}^{+}}\right]$and let $k$ be the fraction field of $R$.
a) Show that every element in $R$ (resp. $k$ ) can be written as a formal power series (resp. formal Laurent series) in $t^{\frac{1}{n}}$ for some $n \in \mathbb{Z}^{+}$which depends on $k .^{4}$
b) Show that the units in $R$ are the Puiseux series with nonzero coefficient of $t^{0}$. Deduce that $R$ is a local ring.
c) Show that any nonzero $f \in k$ may be uniquely written as $t^{\frac{p}{q}} \cdot u$ with $u \in R^{\times}$. Deduce that $R$ is a valuation ring. Show that $R$ is not Noetherian, so is not a DVR.
d) Define $\left\|\|: k \rightarrow \mathbb{R}^{>0}\right.$ by $0 \mapsto 0, f=t^{\frac{p}{q}} \cdot u \mapsto 2^{-\frac{p}{q}}$. Show that $\| \|$ is a norm on $k$.

## 1.7. $R$-regular valuations; valuations on Dedekind domains.

Let $R$ be an integral domain with fraction field $k$. We say that a valuation $v$ of $k$ is R-regular if $v(x) \geq 0$ for all $x \in R$, i.e., if $R$ is contained in the valuation ring $R_{v}$ of $v$.

Theorem 13. (Classification of $R$-regular valuations on a Dedekind domain) Let $R$ be a Dedekind domain with fraction field $K$, and let $\mathfrak{p}$ a nonzero prime ideal of $R$. We define a map $v_{\mathfrak{p}}: K \rightarrow \mathbb{Z} \cup-\infty$ as follows: $v_{\mathfrak{p}}(0)=-\infty$. Let $\alpha \in K^{\times}$. Write $\alpha=\frac{x}{y}$ with $x, y \in R \backslash\{0\}$. Let

$$
(x)=\mathfrak{p}^{a} \mathfrak{q},(y)=\mathfrak{p}^{b} \mathfrak{q}^{\prime}
$$

[^4]with $\operatorname{gcd}\left(\mathfrak{p}, \mathfrak{q q}{ }^{\prime}\right)=1$. Put $v_{\mathfrak{p}}=a-b$.
a) The map $v_{\mathfrak{p}}: K \rightarrow \mathbb{Z} \bigcup\{\infty\}$ is a normalized discrete valuation.
b) Conversely, let $v$ be a nontrivial valuation on $K$. If $v$ is $R$-regular - i.e., $v(R) \subset$ $[0, \infty]$ - then $v \sim v_{\mathfrak{p}}$ for a unique nonzero prime ideal $\mathfrak{p}$ of $R$. In particular, any nontrivial $R$-regular valuation on $K$ is discrete.

Proof. The proof of part a) is straightforward and left to the reader as Exercise 1.19 below. As for part b), let $v$ be a nontrivial $R$-regular valuation on $K$. Let us call its valuation ring $A_{v}$ and its maximal ideal $\mathfrak{m}_{v}$, so by hypothesis $R \subset A_{v}$. Put $\mathfrak{p}:=R \cap \mathfrak{m}_{v}$. Since $\mathfrak{p}$ is nothing else than the pullback of the prime ideal $\mathfrak{m}_{v}$ under the homomorphism of rings $R \hookrightarrow A_{v}$, certainly $\mathfrak{p}$ is a prime ideal of $R$. We claim that it is nonzero. Indeed, $\mathfrak{p}=\{0\}$ would mean that every nonzero element of $R$ is a unit in $A_{v}$. Since every nonzero element of $K$ is a quotient of two nonzero elements of $R$, this would give $A_{v}=K$, contradicting the nontriviality of $v$. Thus $\mathfrak{p}$ is a nonzero prime ideal in the Dedekind domain $R$, hence maximal. Let $R_{\mathfrak{p}}$ be the localization of $R$ at $\mathfrak{p}$, a discrete valuation ring. Since every element of $R \backslash \mathfrak{p}$ is a unit in $A_{v}$, we have an inclusion of nontrivial valuation rings $R_{\mathfrak{p}} \subset A_{v}$. By Theorem 5, this implies that $v_{\mathfrak{p}} \sim v$.

Exercise 1.19: Prove Theorem 13a).
Exercise 1.20: Let $R$ be a Dedekind domain with fraction field $K$. Let $\mathfrak{p}_{1}, \ldots, \mathfrak{p}_{r}$ be distinct nonzero prime ideals of $R, n_{1}, \ldots, n_{r} \in \mathbb{Z}$ and $x_{1}, \ldots, x_{r} \in K$. Show that there exists an element $x \in K$ such that:
(i) For all $1 \leq i \leq r, v_{\mathfrak{p}_{i}}\left(x-x_{i}\right)=n_{i}$ and
(ii) $v_{\mathfrak{q}}(x) \geq 0$ for all nonzero prime ideals $\mathfrak{q}$ different from the $\mathfrak{p}_{i}$ 's.

Note that (i) (at least with $\leq$ in place of $=$; showing that one may demand equality requires a bit more work) is precisely weak approximation applied to the finite set of norms associated to the valuations $v_{\mathfrak{p}_{\mathfrak{i}}}$. However, the additional integrality conditions in (ii) are beyond the scope of the Artin-Whaples approximation theorem (which does not have in its statement an integral domain $R$ ). In the case where $K$ is a global field, this is actually related to the strong approximation theorem, one of the fundamental results of Chapter 6.

### 1.8. Some Classification Theorems.

In this section we give some cases of fields $k$ over which we can classify all norms. The first, and most famous, case is $k=\mathbb{Q}$ :

Theorem 14. (Little Ostrowski Theorem) Up to equivalence, the nontrivial norms on $\mathbb{Q}$ are precisely the standard non-Archimedean norm $\left|\left.\right|_{\infty}\right.$ and the p-adic norms.

Proof. Let || be a nontrivial norm on $\mathbb{Q}$. If || is Archimedean, then by Lemma 10 it is equivalent to $\left|\left.\right|_{\infty}\right.$. Otherwise $| \mid$ is non-Archimedean. Then by Proposition 8 , it is $\mathbb{Z}$-regular on the Dedekind domain $\mathbb{Z}$, so its valuation ring is the localization at a prime ideal of $\mathbb{Z}$, i.e., it is a $p$-adic norm.

To show how little is up our sleeves, let's rephrase the non-Archimedean argument in more concrete terms:

Let || be a nontrivial non-Archimedean norm on $\mathbb{Q}$. By Proposition $8,|\mathbb{Z}| \subset$ $[0,1]$. If $|n|=1$ for every nonzero integer, then by multiplicativity $|\mid$ would be the
trivial norm on $\mathbb{Q}$, so there exists a positive integer $n$ with $|n|<1$. Let $p$ be the least such positive integer; it follows easily that $p$ is prime. By adjusting the norm in its equivalence class, we may assume that $|p|=\frac{1}{p}$, and our task is now to prove that $\left|\left|=| |_{p}\right.\right.$. As a multiplicative group, $\mathbb{Q}^{\times}$is generated by -1 and the primes numbers $\ell$. Certainly $|-1|=|-1|_{p}=1$, so it suffices to show that for all primes $\ell \neq p,|\ell|=|\ell|_{p}=1$. So suppose not, i.e., there exists $\ell>p$ such that $|\ell|<1$. Then there exist integers $x, y$ such that $x p+y \ell=1$, and hence

$$
1=|1|=|x p+y \ell| \leq \max (|x p|,|y \ell|) \leq \max (|p|,|\ell|)<1,
$$

contradiction!
Next we give the "function field analogue" of Theorem 14: namely, we will classify all norms on $\mathbb{F}_{q}(t)$. Recall that by Exercise 1.3, every norm on $\mathbb{F}_{q}(t)$ restricts to the trivial norm on $\mathbb{F}_{q}$. So the following is a more general result:

Theorem 15. Let $k$ be any field and let $K=k(t)$, the field of rational functions over $k$. Then every nontrivial norm on $K$ which is trivial on $k$ is equivalent to exactly one of the following norms:
(i) $\left|\left.\right|_{P}\right.$ for $P \in k[t]$ a monic irreducible polynomial, or
(ii) the norm $\left|\left.\right|_{\infty}\right.$ defined by $\frac{p(t)}{q(t)} \mapsto 2^{\operatorname{deg}(p(t))-\operatorname{deg}(q(t))}$.

Proof. Let || be a norm on $K$ which is trivial on $k$. Note that since || is trivial on $k$, in particular $|\mathbb{Z} \cdot 1| \subset[0,1]$ so by Proposition $8|\mid$ is non-Archimedean. Let $R=\mathbb{F}_{q}[t]$ - a Dedekind domain with fraction field $K$.
Case 1: If $\|$ is $R$-regular, then by Theorem 13 the associated valuation is $v_{\mathfrak{p}}$ for a unique prime ideal $\mathfrak{p}$ of $R$. This is equivalent to what is stated in (i).
Case 2: Suppose $|R| \not \subset[0,1]$. Since by hypothesis $|k| \subset[0,1]$, we must have $|t|>1$. Adjusting $|\mid$ in its equivalence class we may assume that $| t \left\lvert\,=\frac{1}{2}\right.$, and our task is now to show that $\left|\left|=| |_{\infty}\right.\right.$, for which it is sufficient to show that $\left.| P\right|=2^{\operatorname{deg} P}$ for each polynomial $P(t)=a_{n} t^{n}+\ldots+a_{1} t+a_{0}$. But we know that $\left|a_{i} t^{i}\right|=2^{i}$ for all $i$, so (c.f. Exercise X.X) the leading term dominates and the conclusion follows.

Note the following remarkable similarity between Theorems 14 and 15: in both cases, most of the valuations come from the prime ideals of a particularly nice Dedekind domain (in fact, a PID) with fraction field $k$, but there is one exception, a valuation "at infinity". This is very strange because in the case of $\mathbb{Q}$ this exceptional valuation is Archimedean, whereas in the case of $k(t)$ it is non-Archimedean. In fact, in the latter case the "infinite place" is not intrinsic to the field but just comes from our choice of $R$ : indeed, pulling it back by the automorphism $t \mapsto \frac{1}{t}$ gives us a finite place!

The following exercise is meant to drive home this point:
Exercise 1.21: Suppose $k$ is algebraically closed.
a) Show that the group $G=P G L_{2}(k)$ acts faithfully on $k(t)$. (Hint: linear fractional transformation).
b) Show that the orbit of $\left|\left.\right|_{\infty}\right.$ under $G$ consists of $| \|_{\infty}$ together with all the norms $\left|\left.\right|_{P_{c}}\right.$ where $P_{c}(t)=t-c$ for $c \in k$.
c) Show that $G$ acts transitively on the set of norms of $k(t)$ which are trivial on $k$ iff $k$ is algebraically closed.

In the case of $k=\mathbb{C}$, anyone who has taken a complex analysis or algebraic geometry course will recognize part c) of this exercise as saying that the set of places on $\mathbb{C}(t)$ which are trivial on $\mathbb{C}$ is naturally parameterized by the Riemann sphere, or projective line, $\mathbb{P}^{1}(\mathbb{C})$. Thus the existence of "infinite" valuations can be interpreted expressing the fact that $\mathbb{P}^{1}(\mathbb{C})$ is not affine but projective. This is just the beginning of a deep connection between valuation theory and algebraic geometry (a connection which will, unfortunately, be pursued very little in this course).

Let us now try to extend the above work to finite extension fields. This brings us to some key definitions: a number field is a field $k$ which is a finite extension of $\mathbb{Q}$. A function field is a field which is a finite extension of $\mathbb{F}_{p}(t)$ for some prime $p$. (As a small remark, we would not change the definition of a function field by requiring the extension to be separable: a field which is written as a finite, nonseparable extension of $\mathbb{F}_{p}(t)$ can also be realized as a finite separable extension of $\mathbb{F}_{p}(t)$.) A global field is a field $k$ which is a finite extension either of $\mathbb{Q}$ or of $\mathbb{F}_{p}(t)$.

The side-by-side treatment of number fields and function fields is one of the hallmarks of modern number theory. We must quote André Weil, who eloquently cast it in the language of his day (May, 1967):
"Once the presence of the real field, albeit at infinite distance, ceases to be regarded as a necessary ingredient in the arithmetician's brew, it goes without saying that the function-fields over finite fields must be granted a fully simultaneous treatment with number-fields instead of the segregated status, and at best the separate but equal facilities, which hitherto have been their lot. That, far from losing by such treatment, both races stand to gain by it, is one fact which will, I hope, clearly emerge from this book."

We turn next to the natural question of classifying all norms on an algebraic number field $K$. Much of what we have said before carries over verbatim. We will see that there is a slight subtlety concerning the inequivalent Archimedean norms (which we will not completely resolve at this point but rather return to it in Chapter 2 when we have further tools). Moreover, unlike the case of $R=\mathbb{Z}, K=\mathbb{Q}$, it is not immediately obvious that every valuation on $K$ is regular on the ring of integers. For this, we use the following result:

Proposition 16. Let $L / K$ be a finite degree field extension. Let $R$ be a Dedekind domain with fraction field $K$, and let $S$ be the integral closure of $R$ in $L$. Then:
a) $S$ is a Dedekind domain with fraction field $L$.
b) Let $v$ be a valuation on $L$. Then $v$ is $S$-regular iff its restriction to $K$ is $R$-regular.

Proof. Part a) is a standard result which it is not our purpose to prove here. If $L / K$ is separable, it is easy to prove this and also the important supplementary result that $S$ is a finitely generated $R$-module. If $L / K$ is not separable, then the proof that $S$ is a Dedekind domain becomes more involved - see e.g. [Eis, Thm. 11.13] and the finiteness of $S$ as an $R$-module need not hold!
b) Since $R \subset S$, certainly the $R$-regularity of $\left.v\right|_{K}$ is necessary for the $S$-regularity of $v$. Conversely, let $x$ be an element of $S$. By definition of integral closure, there
exists $n \in \mathbb{Z}^{+}$and $a_{0}, \ldots, a_{n-1} \in R$ such that

$$
x^{n}+a_{n-1} x^{n-1}+\ldots+a_{1} x+a_{0}=0
$$

Seeking a contradiction, we suppose $v(x)=N<0$. Since each $a_{i}$ is in $R$, by hypothesis we have $v\left(a_{i}\right) \geq 0$ for all $0 \leq i<n$, so $v\left(a_{i} x^{i}\right)=i N+v\left(a_{i}\right) \geq i N$, whereas $v\left(x^{n}\right)=n N$. Thus in the sum $x^{n}+a_{n-1} x^{n-1}+\ldots+a_{1} x+a_{0}$ we have a unique term of smallest valuation; by Exercise 1.9c), we get

$$
\infty=v(0)=v\left(x^{n}+a_{n-1} x^{n-1}+\ldots+a_{1} x_{1}+a_{0}\right)=n N,
$$

a contradiction. So $v(x) \geq 0$.
Theorem 17. (Number Field Ostrowski Theorem)
Let $k \cong \mathbb{Q}[t] /\left(P(t)\right.$ be a number field, with ring of integers $\mathbb{Z}_{k}$. Then:
a) Every non-Archimedean absolute value is equivalent to $\left|\left.\right|_{\mathfrak{p}}\right.$ for a unique prime ideal of $\mathbb{Z}_{k}$, the ring of integers of $k$.
b) Every Archimedean embeddding, up to equivalence, is of the form $x \mapsto|\iota(x)|$, where $\iota: k \rightarrow \mathbb{C}$ is a field embedding and $|\mid$ is the standard absolute value on $\mathbb{C}$.
c) Let $r_{1}$ be the number of real roots of the defining polynomial $P(t)$ and let $r_{2}$ be half the number of complex roots. Let $r$ be the number of Archimedean places. Then $0<r<r_{1}+r_{2}$.

Proof. a) Since $\mathbb{Z}_{k}$ is Dedekind, this follows from Theorem 13 and Proposition 16. b) By the Big Ostrowski Theorem, every Archimedean absolute value, up to equivalence, arises from an embedding $\iota: k \hookrightarrow \mathbb{C}$. Since $k / \mathbb{Q}$ is finite separable, there are $[k: \mathbb{Q}]$ embeddings of $k$ into $\mathbb{C}$, obtained by sending $t(\bmod P(t))$ to each of the $[k: \mathbb{Q}]$ complex roots of $P(t)$. Thus there is at least one Archimedean norm.
c) The subtlety is that distinct embeddings $\iota: k \hookrightarrow \mathbb{C}$ may give rise to the same norm: c.f. Exercise 1.4c). Indeed, because complex conjugation on $\mathbb{C}$ preserves the standard norm $|\mid$, the number $r$ of Archimedean places of $k$ is at most the number of orbits of the set of embeddings under complex conjugation, namely $r_{1}+r_{2}$.

Remark: Indeed we always have equality in part c): the number of Archimedean places is precisely $r_{1}+r_{2}$. I looked long and hard to find a proof of this fact using only the tools we have developed so far. I found it in exactly one place: Dino's text [Lor]. But the proof given there is not easy! We will come back to this point in the context of a more general discussion on extension of valuations.

Remark: In particular, if $k=\mathbb{F}_{q}$ or $\overline{\mathbb{F}_{p}}$, then by Exercise 1.3 every norm on $k(t)$ is trivial on $k$, and Theorem 15 classifies all norms on $k(t)$.

Exercise 1.22: Let $k$ be a field, $R=k[t], K=k(t)$, and $L / K$ be a finite separable field extension. Let \| be an absolute value on $L$ which is trivial on $k$.
a) Let $S$ be the integral closure of $k[t]$ in $L .{ }^{5}$ Show that $\left|\left|=| |_{\mathcal{P}}\right.\right.$ for some prime ideal $\mathcal{P}$ of $S$ iff the restriction of $\left.|\mid$ to $k$ is not $|\right|_{\infty}$.
b) Let $\left|\left.\right|_{\mathfrak{p}}\right.$ be an $R$-regular norm on $K$, with corresponding prime ideal $\mathfrak{p}$ of $R$. Express the number of places of $L$ which restrict to \| in terms of the factorization of $\mathfrak{p}$ in $S$.

[^5]c) Suppose that that $L \cong K[t] / P(t)$ for an irreducible polynomial $P(t) .{ }^{6}$ Can you give a more concrete description of the number of places of $L$ which restrict to the finite place $\left|\left.\right|_{\mathfrak{p}}\right.$ of $K$ ?
d) Show that the number of places of $L$ which extend the infinite place $\left\|\|_{\infty}\right.$ of $K$ is positive and at most $[L: K]$. Can you say more?

Let $L / K$ be a finite field extension and || a place of $K$. As we can see from the above results and exercises, with our current vocabulary it is slightly awkward to describe the number of places of $L$ which extend the place $\|$ of $K$. To elaborate: suppose for simplicity that $|\mid$ is a non-Archimedean place whose corresponding valuation is discrete and that $L / K$ is separable. Then the valuation ring $R$ of || is a DVR with fraction field $K$. Let $S$ be the integral closure of $R$ in $L$, so that $S$ is again a Dedekind domain with finitely many maximal ideals (so, in fact, a PID). What we want is precisely to count the number of maximal ideals of $S$. In classical number theory, we do this via the criterion of Kummer-Dedekind: namely, we write $L=K[x] \cong K[t] /(P)$, where $x \in S$ has minimal polynomial $P(t)$, and then we factor $P$ modulo the maximal ideal $\mathfrak{p}$ of $R$. Unfortunately this only works when $S=R[x]$. In the number field case, it is easy to see that this condition holds at least for all but the primes dividing the discriminant of the minimal polynomial $P$, which is usually enough for applications. But now we are in the local case, and as we shall see it is simply not true that $S$ need be monogenic as an $R$-module.

In summary, the fact that ring extensions are more complicated than field extensions is doing us in. What would be fantastic is if the number of maximal ideals of $S$ could be expressed in terms of the factorization of the polynomial $P$ in some field extension. This is exactly what the theory of completions will give us, so we turn to that next.

## References

[Art] E. Artin, Algebraic numbers and algebraic functions. Gordon and Breach Science Publishers, New York-London-Paris 1967 xiii +349 pp.
[AW] E. Artin and G. Whaples, A note on axiomatic characterization of fields. Bull. Amer. Math. Soc. Volume 52, Number 4 (1946), 245-247.
[Bak] M. Baker, Algebraic Number Theory Course Notes (2006), available at http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf
[Eis] D. Eisenbud, Commutative algebra. With a view toward algebraic geometry. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.
[Lor] D. Lorenzini, An invitation to arithmetic geometry. Graduate Studies in Mathematics, 9. American Mathematical Society, Providence, RI, 1996. xvi+397 pp.
[Wei] E. Weiss, Algebraic number theory. Reprint of the 1963 original. Dover Publications, Inc., Mineola, NY, 1998.

[^6]
[^0]:    Thanks to John Doyle, David Krumm and Rankeya Datta for pointing out typos.

[^1]:    ${ }^{1}$ I.e., there exists $k \in \mathbb{Z}^{+}$such that $x^{k}=1$.

[^2]:    ${ }^{2}$ Warning: in more advanced valuation theory, one has the notion of a $K$-place of a field $k$, a related but distinct concept. However, in these notes we shall always use place in the sense just defined.

[^3]:    ${ }^{3}$ Thus either way $\mathbb{Z} \cdot 1$ is a subring of $k$, often called the prime subring.

[^4]:    ${ }^{4}$ Either type of series is called a Puiseux series.

[^5]:    ${ }^{5}$ Recall that $S$ is a Dedekind domain: [Bak, Remark 4.23]. More on this sort of thing later on.

[^6]:    ${ }^{6}$ By the corollary to the Primitive Element Theorem, this certainly occurs if $L / K$ is separable, so e.g. in characteristic 0 .

