Newton polygons.

Over $\mathbb{C}$, an upper bound on the absolute values of the coefficients of a polynomial (in one variable) gives an upper bound on the absolute values of its roots.

In the non-archimedean situation, we get something even better: a precise formula for the absolute values of the roots in terms of the a.v. of the coefficients.

R = complete DVR with uniformizer $\pi$

K = fraction field of R

$\nu : K^x \to \mathbb{Z}, \quad \nu(\pi^m u) = m$

if $u \in K^x$, $m \in \mathbb{Z}$

If $\bar{K}$ is an algebraic closure of $K$, we get an extension $\bar{\nu} : \bar{K}^x \to \mathbb{Q}$, given by

$\bar{\nu}(\bar{x}) = \nu(\text{Norm}_{K(\bar{x})/K(\bar{x})}, \frac{1}{\deg_{\bar{K}}(\bar{x})})$

Remark: This does not rely on $k = R/(\pi)$ being perfect.
§7.3. Now consider a monic polynomial
\[ f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} + \ldots + (-1)^n a_n, \]
where \( a_n \neq 0 \), \( a_j \in K \). Write
\[ f(x) = \prod_{i=1}^{n} (x - \lambda_i), \quad \lambda_i \in \overline{K}, \]
with \( \nu(\lambda_1) \leq \nu(\lambda_2) \leq \ldots \leq \nu(\lambda_n) \).

Furthermore, let us write
\[ (\nu(\lambda_1), \ldots, \nu(\lambda_n)) = (c_1, \ldots, c_1, \ldots, c_d, \ldots, c_d), \]
with \( r_1 \) times \( c_1 \) and \( r_d \) times \( c_d \)
where \( c_1 < c_2 < \ldots < c_d \) and \( r_j \in \mathbb{N} \).

Consequently: for any \( 1 \leq r \leq n \),
\[ a_r = \sum_{i_1 < \ldots < i_r} \lambda_{i_1} \lambda_{i_2} \ldots \lambda_{i_r} \]
\[ \Rightarrow \nu(a_r) \geq \min \{ \nu(\lambda_{i_1} \ldots \lambda_{i_r}) \} \]
\[ = \nu(\lambda_1) + \ldots + \nu(\lambda_r). \]

In addition: If \( r \) is of the form \( r = r_1 + r_2 + \ldots + r_k \) for some \( 1 \leq k \leq d \),
then it is clear that equality is forced:
\[ \nu(a_1 + \ldots + a_k) = \nu(a_1) + \nu(a_2) + \ldots + \nu(a_{r_1} + \ldots + a_{r_k}) \]
\[ \nu(a_{r_1} + \ldots + a_{r_k}) = r_1 c_1 + r_2 c_2 + \ldots + r_k c_k. \]
\[ c_k = \frac{1}{v_k} \left( v(a_{r_1+\ldots+r_k}) - v(a_{r_1+\ldots+r_{k-1}}) \right). \]

§7.4. Geometric interpretation.

With the same notation as above, plot the following points in the Euclidean plane:

\[(0, v(a_0)) = (0, 0),\]
\[(1, v(a_1)), (2, v(a_2)), \ldots, (n, v(a_n)),\]

where by convention we ignore those points \((j, v(a_j))\) for which \(a_j = 0\). This gives a finite subset \(S \subset \mathbb{R}^2\). Now form the lower convex envelope of \(S\), i.e., the smallest set \(C\) containing \(S\) and having the properties that \(C\) is convex and \((x, y) \in C, t > 0 \Rightarrow (x, y + t) \in C\).

Now write

\[ \partial C = E_1 \cup E_2 \cup \ldots \cup E_k \cup V_0 \cup V_n, \]

where \(V_0, V_n\) are the two vertical sides of \(\partial C\) and \(E_1, E_2, \ldots, E_k\) are the line segments which are the edges of \(C\) that have finite length.
On the other hand, consider the subset of $S$ defined as

$$S_1 = \{ (0,0), (r_1, v(a_{r_1})), (r_1 + r_2, v(a_{r_1+r_2})), \ldots, (n, v(a_n)) \}.$$ 

Then $E_1, \ldots, E_k$ are precisely the line segments joining the consecutive points of $S_1$.

**Corollary:** The slope of $E_i$ equals $c_i$.

**Corollary:** The subset $C \subset \mathbb{R}^2$ determines the valuations of all the roots of $f(X)$ counted with their multiplicities.

**8.7.5. Lemma:** Let $A$ be a commutative ring such that $p \cdot A = 0$ for some prime $p$ (i.e., $A$ is a commutative $\mathbb{F}_p$-algebra). Let $I \triangleleft A$ be an ideal such that $I^n = 0$ for some $n \in \mathbb{N}$, and assume that $A/I$ is a perfect field (necessarily of characteristic $p$).

Then $\bigcap_{n=1}^{\infty} A^p = A$ is a subfield of $A$, and the composite $[A] \hookrightarrow A \rightarrow A/I$ is an isomorphism.
Proof: Since $A$ is commutative and $p \cdot A = 0$, a standard argument shows that $A^{p^n}$ is a subring of $A$ for each $n \in \mathbb{N}$, and thus $[A]$ is also a subring of $A$.

Now choose $n \in \mathbb{N}$ so that $p^n > m$. The map $\phi_n: A \rightarrow A$, $\phi_n(a) = a^{p^n}$, is a ring homomorphism which kills $I$, whence it factors through $\overline{\phi}_n: A/I \rightarrow A$. Now $\overline{\phi}_n$ is injective because $A/I$ is a field.

Write $k = A/I$. Since $k$ is perfect, $\overline{\phi}_n(k) \subseteq [A]$. The composition

$\overline{\phi}_n(k) \subseteq [A]$. The composition

$\overline{\phi}_n(k) \subseteq [A]$. The composition

$\overline{\phi}_n(k) \subseteq [A]$.

is also surjective because $k$ is perfect.

Finally, note that the same argument works with $n$ replaced by any $n' \geq n$. This clearly implies that $\overline{\phi}_{n'}(k) = \overline{\phi}_n(k)$, so $[A] = \overline{\phi}_n(k)$ and we are done. //
§7.6. Corollary: Let \( A \) be a commutative \( \mathbb{F}_p \)-algebra, let \( I \subset A \) be an ideal such that \( A \) is \( I \)-adically complete, and suppose that \( k = A/I \) is a perfect field. Then
\[
[A] := \bigcap_{n=1}^{\infty} A^{p^n} \text{ is a subfield of } A
\]
which maps isomorphically onto \( k \).

Proof: The lemma applies to the ring \( A/I^m \) and the ideal \( I/I^m \) for each \( m \in \mathbb{N} \).

Hence the composite
\[
[A/I^m] \rightarrow A/I^m \rightarrow A/I = k
\]
is an isomorphism. We get a diagram
\[
\begin{array}{ccc}
A/I & \xleftarrow{=} & A/I^2 & \xleftarrow{=} & A/I^3 & \xleftarrow{=} & \cdots \\
& \uparrow & & \uparrow & & \uparrow & & \\
[A/I] & \xleftarrow{=} & [A/I^2] & \xleftarrow{=} & [A/I^3] & \xleftarrow{=} & \cdots \\
\end{array}
\]

on which the bottom row consists only of isomorphisms. Let
\[
B = \lim_{\leftarrow m \in \mathbb{N}} [A/I^m] \rightarrow A.
\]

Now \( B \) is a perfect field \( (B \cong k) \), so we must have \( B \leq [A] \). To show equality, observe that \( ([A] + I^m)/I^m \leq [A/I^m] \forall m \in \mathbb{N} \)
§7.7. Corollary: Let $R$ be a complete DVR of characteristic $p > 0$, and assume that the residue field $k$ of $R$ is perfect. Then $R \cong k[[t]]$.

Proof: By Corollary 7.6, we get $k \leftarrow R \rightarrow k$. Let $\pi \in R$ be a uniformizer. We get a homomorphism $k[[t]] \rightarrow R$, $t \mapsto \pi$.

Check that $k[[t]]/(t^n) \cong R/(\pi^n)$ for all $n \in \mathbb{N}$, which implies that we get an isomorphism after completing:

$$k[[t]] \cong \varprojlim_{n \in \mathbb{N}} R/(\pi^n) \subseteq R.$$ 

§7.8. Corollary: Let $R$ be as above, and let $K$ be the quotient field of $R$. Then $R$ is free as an $R^p$-module, with basis $1, \pi, \ldots, \pi^{p-1}$.


Exercise: This implies that there is a unique purely inseparable extension of $K$ of degree $p^n$ (for each $n \in \mathbb{N}$), namely, this extension is $K^{1/p^n}$. 
Corollary: Let $L/K$ be a finite extension. Then $R_L :=$ integral closure of $R$ in $L$ is finitely generated as an $R$-module.

Proof: Choose $K \subset E \subset L$ purely separable.

Then $L = E^{1/p^m}$ for some $m \geq 0$.

and $R_L$ is a f.g. $R_E$-module by the above.

Upshot: inseparable extensions do not cause any problems. So from now on we will continue studying separable extensions only.

From now on, we stop assuming that $\text{char}(R) = p > 0$. 
§7.10. **Theorem.** Let $R, K, k, \mathfrak{a}$ be as usual, and let $L/K$ be a finite separable field extension. Then there is a unique tower

$$K \subset E \subset L' \subset L,$$

where $E/K$ is unramified,
$L'/E$ is tamely ramified,
and $L/L'$ is wildly ramified.

§7.11. **Terminology.**

$L/K$ is \( \begin{cases} 
\text{tamely ramified} & \Rightarrow \text{L/K is totally} \\
\text{wildly} & \text{ramified, and}
\end{cases} \)

\( \begin{cases} 
\prod p \mid \deg(L/K) & \text{for tamely ramified} \\
\deg(L/K) = p^r & \text{for wildly ramified}
\end{cases} \)

where $p = \text{char}(k)$.

Thus, if $\text{char}(k) = 0$, tamely ramified $\Leftrightarrow$ totally ramified.

§7.12. **Theorem.** $L/K$ finite Galois extension

$E =$ largest unramified extension of $K$ in $L$

$G = \text{Gal}(L/K) \rightarrow \text{Gal}(E/K)$ with

kernel $I = \text{Gal}(L/E) =$ the \text{inertia subgroup}.
Assume that $\text{char}(k) = p > 0$.

If $p$ is a $p$-Sylow subgroup of $I$, then $P$ is normal in $I$ and $I/P$ is cyclic.

Proof: We might as well assume that $E = K$, i.e., $L/K$ is totally ramified.

Let $P_1, P_2 \subset G$ be $p$-Sylow subgroups, and write $L_i = L^{P_i}$ $(i = 1, 2)$. Then $L_1, L_2$ are tamely ramified extensions of $K$ which have the same degree over $K$.

As we proved in the previous lecture, there exists an unramified Galois extension $F/K$ so that $FL_1 \cong FL_2$.

\[ \text{Remark.} \]

\[ \begin{array}{ccc}
F & \rightarrow & FL \\
\downarrow & & \uparrow \\
L & \leftarrow & \text{totally ramified} \\
& & \text{unramified}
\end{array} \]

\[ \Rightarrow \deg(FL/K) = \deg(F/K) \deg(L/K) \]

\[ \Rightarrow F \text{ and } L \text{ are linearly disjoint over } K \]

Use: $\deg(FL/K) \geq e(L/K) \cdot f(F/K)$

\[ = \deg(L/K) \deg(F/K). \]

Consider the Galois extension \( FL/K \). We have an obvious injection

\[
\text{Gal}(FL/K) \hookrightarrow \text{Gal}(F/K) \times \text{Gal}(L/K)
\]

(obtained by restrictions, since \( F/K \) and \( L/K \) are normal extensions).

By Remark 7.13, this is an isomorphism. This map clearly takes

\[
\text{Gal}(FL_i/FL) \cong \{1\} \times P_i
\]

for \( i = 1, 2 \). But \( FL_1 = FL_2 \Rightarrow P_1 = P_2 \).

Thus: We have shown that \( G \) has only one \( p \)-Sylow subgroup, \( P \), which is therefore normal.

§7.15. Next, we want to check that \( G/P \) is cyclic. We might as well replace \( K \) by \( L \) and thus assume that \( P = \{1\} \).

In other words, \( p \nmid \deg(4/K) \).

Now play the same game; we know that \( LF/F \) is cyclic, where \( F = K(\sqrt{r}) \), \( r = \deg(4/K) \), and \( F \) is unramified. By the argument above,

\[
\text{Gal}(LF/F) \cong \text{Gal}(4/K).
\]

Q.E.D.
§7.16. Generalities. \[ F \subset F_{\text{sep}} \]

Field \quad \text{separable closure of } F

\begin{align*}
\text{Aut}(F_{\text{sep}}/F) & \overset{\text{def}}{=} \text{Gal}(F_{\text{sep}}/F) \hookrightarrow \text{Gal}(L/F) \\
L & = \text{finite} \\
& \text{Galois extension of } F
\end{align*}

Equip each \( \text{Gal}(L/F) \) with the discrete topology; then the image of \( \text{Gal}(F_{\text{sep}}/F) \) is closed with respect to the product topology, and hence \( \text{Gal}(F_{\text{sep}}/F) \) becomes a compact topological group (in fact, profinite).

From now on we will write \( G_F = \text{Gal}(F_{\text{sep}}/F) \).

We have one-to-one correspondences:

- \( \{ \text{finite extensions of } F \text{ contained on } F_{\text{sep}} \} \)
- \( \{ \text{open subgroups of } G_F \} \)

\[ E \hookrightarrow \text{Gal}(F_{\text{sep}}/E) \subset G_F \]

- \( \{ \text{arbitrary field extensions of } F \text{ contained in } F_{\text{sep}} \} \)
- \( \{ \text{closed subgroups of } G_F \} \)

Examples:

1. \( F = \mathbb{F}_q \) \( \Rightarrow \) \( \hat{\mathbb{Z}} \overset{\alpha}{\twoheadrightarrow} G_F \) via \( 1 \mapsto (x \mapsto x^q) \)

2. \( F = \mathbb{C}(t) \) \( \Rightarrow \) \( G_F \cong \hat{\mathbb{Z}} \), but non-canonically.
§7.17. We are interested in the structure of $G_F$, where $F = K$ and $K$ is as above ($K$ = fraction field of a complete d.v.r. $R$ with perfect residue field $k$).

Remark: $L/K$ finite Galois extension

$E = \text{maximal unramified extension of } K \text{ in } L$

$\rightarrow 1 \rightarrow I(L/K) \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(E/K) \rightarrow 1$

and $1 \rightarrow P(L/K) \rightarrow I(L/K) \rightarrow I_t(L/K) \rightarrow 1$

("$t$" for "toric")

$p$-Sylow subgroup
of $I(L/K)$, where $p = \text{char}(k)$

§7.18. Let $K_{sep}$ be a fixed separable closure of $K$

$K_{nr} = \text{max. unram. ext. of } K \text{ in } K_{sep}$

$1 \rightarrow I \rightarrow \text{Gal}(K_{sep}/K) \rightarrow \text{Gal}(K_{nr}/K) \rightarrow 1$

$I = \lim_{L/K \text{ finite Galois}} I(L/K)$

$P = \lim_{L/K \text{ finite Galois}} P(L/K)$

subgroup
We have:

(1) \( \text{Gal}(K_{\text{sep}}/K) / I \cong \text{Gal}(K_{\text{nr}}/K) \cong \text{Gal}(k_{\text{sep}}/k) = G_k \)

(2) \( I / p \cong \prod l \mathbb{Z}/(1) \) (where \( l \) = prime, \( l \neq p \), but non-canonically)

(3) \( P \) is a pro-\( p \) group, i.e., an inverse limit of finite \( p \)-groups

\[ \text{Notation: Let us write} \]

\[ M_n = \{ x \in K_{\text{sep}} \mid x^n = 1 \} \]

We define

\[ \mathbb{Z}_l(1) := \lim_{\rightarrow} M_n \]

with respect to the obvious homomorphisms

\[ \cdots \rightarrow M_3 \rightarrow M_2 \rightarrow M_1 \rightarrow M_0 \]

given by \( x \rightarrow x^l \).