(*May 13, 2022*)

15. Euler, Raphson, Newton, Puiseux, Riemann, Hurwitz, Hensel

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[This document is
http://www.math.umn.edu/~garrett/m/complex/notes_2021-22/15_ERNPRHH.pdf]

This is a sketch of useful devices due to many, many people. A few, not quite in chronological order: Leonard Euler, Joseph Raphson, Isaac Newton, Victor Puiseux, Peter Dirichlet, Bernard Riemann, Adolf Hurwitz, Kurt Hensel, Giuseppe Levi.

In modern terminology, and suggesting that the idea fits into a larger context: a *Riemann surface* is a (complex-) one-dimensional complex manifold. The discussion here will focus on more detailed ideas specific to the (complex-) one-dimensional case.

Riemann approximately proved that every compact, connected Riemann surface is a *projective algebraic curve*, but the *Dirichlet (minimum) principle* he invoked was literally incorrect. The literal falsity amounts to the fact that a convex, closed subset of a *Banach* space need not have a unique element of least norm: it may have none, or infinitely-many. This minimum principle is *true* in a *Hilbert* space, as was observed, in effect, by Giuseppe (Beppo) Levi in 1906, who created a Hilbert space to capture aspects of the differentiability of functions, a forerunner of Sobolev spaces.

The arguably most-natural spaces of continuous functions or k-fold differentiable functions on a compact differentiable manifold have natural structures of Banach spaces, so it is not surprising that these natural structures were thought to have the properties for applications. After Levi's 1906 work, we have understood the advantages of Hilbert-space re-constitution of more naive notions.

Motivated by granting Riemann's result, we limit our attention to *(complex) plane curves* X, that is, point sets in $\mathbb{C}^2$ defined by a single polynomial equation:

$$X \;=\; \{(z,w) \in \mathbb{C}^2 \;:\; P(z,w) \;=\; 0\} \qquad\qquad (P \text{ irreducible in } \mathbb{C}[z,w])$$

or in complex *projective* (complex) two-space $\mathbb{P}^2$ defined by a single *homogeneous* polynomial equation:

$$X \;=\; \{(z,w,t) \in \mathbb{P}^2 \;:\; P(z,w,t) \;=\; 0\} \qquad\qquad (P \text{ homogeneous, irreducible in } \mathbb{C}[z,w,t])$$

We will also have use for compactifications of curves $X \subset \mathbb{C} \times \mathbb{C}$ inside $\mathbb{P}^1 \times \mathbb{P}^1$.

An incidental issue is that plane curves defined this way can have *singularities*, such as *self-intersections*. This is *not* the same phenomenon as *ramification*. Ramification is not a property of a curve itself, but is a property of *maps* $X \to Y$ *between* curves.

1. *Planar algebraic curves as ramified covers of* $\mathbb{C}$

A natural, basic construct is the *(affine) planar algebraic curve* given as the zero-set of a polynomial:

$$Y \;=\; \{(z,w) \in \mathbb{C}^2 : f(z,w) = 0\} \qquad\qquad (\text{suitable } f(z,w) \in \mathbb{C}[z,w])$$

Without much loss of generality, we suppose that f is *irreducible* in $\mathbb{C}[z,w]$: if f factors as $f(z,w) = g(z,w) \cdot h(z,w)$, then the zero set of f is the union of the zero-sets of g and of h. The curve Y is also known as the (affine) *Riemann surface* associated to f, despite the possibility that it has non-smooth points, such as self-intersections.

Given $Y = \{(z,w) \in \mathbb{C}^2 : f(z,w) = 0\}$, the corresponding *(ramified) cover* of $\mathbb{C}$ is $\pi : Y \to \mathbb{C}$ by $\pi(z,w) = z$. Or, of course, it could as well be $\pi(z,w) = w$, but often z is considered the primary coordinate, and w somehow secondary. But that convention has no mathematical content.

The polynomial f can be thought of as an element of $\mathbb{C}(z)[w]$, that is, as a polynomial in w with coefficients in the field $\mathbb{C}(z)$ of rational functions in z. Let n be the degree of f in w. The *degree* of $\pi : Y \to \mathbb{C}$ is also n, a terminology justified by:

[1.1] Claim: For all but finitely-many $z_o \in \mathbb{C}$, the equation $f(z_o, w) = 0$ has exactly n roots, and they are distinct (meaning that there are no multiple roots).

Proof: Away z_o from the zeros of the top-degree coefficient, $f(z_o, w)$ is of degree n in w. Thus, *including multiplicities*, $f(z_o, w) = 0$ will have n roots w for every other $z_o \in \mathbb{C}$. The issue is multiplicities. By Gauss' lemma, since f is monic in w, it is irreducible in $\mathbb{C}[z][w] \approx \mathbb{C}[z,w]$ if and only if it is irreducible in $\mathbb{C}(z)[w]$.

From polynomial algebra in one variable over a field, we know that a polynomial P has a double (or higher) multiple root w_o if and only if w_o is a root of P *and* a root of its derivative P'. Since $f \in \mathbb{C}(z)[w]$ is irreducible, f and f_w have no non-trivial common factor $g(w) \in \mathbb{C}(z)[w]$. That is, the extended Euclidean algorithm in $\mathbb{C}(z)[w]$ produces $A(z,w), B(z,w) \in \mathbb{C}(z)[w]$ such that $A(z,w)f(z,w) + B(z,w)f_w(z,w) = 1$. Since the coefficients of A, B are in $\mathbb{C}(z)$, we can multiply through by a (not-identically-zero) polynomial $g(z)$ so that $a(z,w)f(z,w) + b(z,w)f_w(z,w) = g(z)$ with $a, b \in \mathbb{C}[z,w]$ and $g \in \mathbb{C}[z]$.

For $z_o, w_o \in \mathbb{C}$ such that $f(z_o, w_o) = 0$ and $f_w(z_o, w_o) = 0$, necessarily $g(z_o) = 0$. Thus, multiple roots of $f(z_o, w) = 0$ can only occur when $g(z_o) = 0$. ///

In the notation of the proof:

[1.2] Corollary: *(of proof)* The only points z_o where $\pi : Y \to \mathbb{C}$ fails to be n-to-1 are *among* the zeros of $g(z)$, where $a(z,w)f(z,w) + b(z,w)f_w(z,w) = g(z)$. ///

A *covering map* or *cover* $\pi : Y \to X$ of topological spaces is a local homeomorphism at every point $y_o \in Y$, that is, there is be a neighborhood U of y_o so that $\pi|_U$ is an isomorphism (of whatever type is under discussion) to its image. Hence the modifier *ramified* in our current discussion.

[1.3] Claim: Given a ramified cover $\pi : Y \to \mathbb{C}$ associated to a polynomial f, let Y' be Y with the finitely-many bad points removed. Then π restricted to Y' *is* a covering map.

Proof: Away from the finitely-many bad points z_o, at w_o satisfying $f(z_o, w_o) = 0$, we have $f_w(z_o, w_o) \neq 0$. The holomorphic implicit function theorem gives a holomorphic function F on a neighborhood U of z_o such that $F(z_o) = w_o$ and $f(z, F(z)) = 0$. Further, since $f_w(z_o, w_o) \neq 0$, F has a local holomorphic inverse. Thus, π restricted to $F(U)$ is a (local) isomorphism ///

2. *Ramification of $\pi : Y \to \mathbb{C}$ versus singularities of Y*

Given $\pi : Y \to \mathbb{C}$, the previous section produces a finite set S of points in $\mathbb{C}$ such that on $Y' = \pi^{-1}(\mathbb{C} - S)$ the map π is n-to-1. The *bad set* Y' for the map $\pi : Y \to \mathbb{C}$ consists of two types of points. First, there are points at which Y itself is actually not quite a *manifold* (see below), called *singularities*. Second, there are points where the map $\pi : Y \to \mathbb{C}$ aligns awkwardly with the shape of Y, called *ramified* or *branch points*. These features can occur simultaneously.

An easy criterion for (local) non-singularity of a (complex) curve in $\mathbb{C}^2$ defined by a single equation:

[2.1] Claim: Let $Y \subset \mathbb{C}^2$, be defined by $f(z, w) = 0$. At (z_o, w_o) on Y, where the highest-order coefficient in w does not vanish, if $f_w(z_o, w_o) \neq 0$, then Y is non-singular at (z_o, w_o).

Proof: First, the non-vanishing of $f_w(z_o, w)$ at $w = w_o$ assures that w_o is a *simple* root of the equation $f(z_o, w) = 0$. This immediately precludes the possibility of self-intersection, for example. The hypothesis also assures that, by the holomorphic implicit function theorem, there is a *unique* holomorphic F on a sufficiently small neighborhood U of z_o such that $F(z_o) = w_o$ and $f(z, F(z)) = 0$ for $z \in U$. This essentially shows that, on U, the map $\pi : F(U) \to U$ gives a *coordinate map*, fulfilling part of the required properties of a *complex manifold*.

To check the holomorphy of the *transition maps*: let $z_1 \in U_1$ with w_1 and F_1, and and $z_2 \in U_2$ with w_2 and F_2, be two such configurations. *[... iou ...]*(I guess my disregard for this proof is an indication of its inevitability, and, thus, not-so-interestingness... hmm) ///

Reducibility of a planar curve Y is that it is the union of two curves. This is a property of the curve itself, and not of a map $\pi : Y \to \mathbb{C}$. Algebraically, for Y defined via $f \in \mathbb{C}[z, w]$, reducibility of the curve is equivalent to reducibility of the polynomial in (the unique factorization domain) $\mathbb{C}[z, w]$. Reducibility is a bit pathological, and easy to avoid: by Gauss' Lemma: reducibility in $\mathbb{C}[z, w]$ is equivalent to reducibility in the Euclidean ring $\mathbb{C}(z)[w]$. The latter reducibility is equivalent to $f(z, w)$ and $f_w(z, w)$ having a non-trivial greatest common divisor in $\mathbb{C}(z)[w]$. This common divisor can be determined by the Euclidean algorithm. Since $\mathbb{C}(z)[w]$ is Euclidean, it is a principal ideal domain, and Noetherian, so a reducible curve is a *finite* union of *irreducible* curves. The simplest example of a reducible curve is $w^2 = z^2$, which falls apart into two irreducible curves $w = z$ and $w = -z$.

A curve Y that is not reducible is of course called *irreducible*. Irreducibility does *not* preclude non-smoothness/singularities, such as *self-intersection*. As with reducibility/irreducibility, non-smoothness features are features of a curve Y itself, without reference to maps $\pi : Y \to \mathbb{C}$. As a simple example, the reducible curve given by $w^2 = z^2$ can be tweaked to be irreducible, but still *self-intersect* at $(0, 0)$. Namely, modify the example to be Y given by $w^2 = z^2(1 + z)$. By Eisenstein's criterion, using the prime $z + 1$ in $\mathbb{C}[z, w]$, $w^2 - z^2(1 + z)$ is irreducible in $\mathbb{C}[z, w]$. However, the two distinct local solutions near $z = 0$,

$$w_\pm \;=\; \pm z\sqrt{1+z} \;=\; \pm z(1 + \frac{z}{2} + \ldots)$$

intersect at $(0, 0)$. This is a *self-intersection* of the irreducible curve Y.

Manifestly, *any* $\pi : Y \to \mathbb{C}$ of a curve Y (that is, even after reasonable changes of coordinates) for Y having a self-intersection (z_o, w_o), will have anomalous behavior at that point, and such points are included in the set of bad points detected by the method of the previous section.

Ramification is a possible property of a *map* $\pi : Y \to \mathbb{C}$, at a point $z_o \in \mathbb{C}$ and/or at points (z_o, w_o) on Y. Ramification of π at a point does *not* imply singularity of that point on the curve Y. The prototype appears for the curve Y given by $w^n = z$, with $\pi(w, z) = z$. On $\mathbb{C}$, away from $z = 0$, the mapπ is n-to-1. At $z = 0$, the only solution to $w^n = 0$ is $w_o = 0$ (of multiplicity n). We say that $z_o = 0$ is *ramified* or a *branch point*, and/or that $w_o = 0$ is *ramified*, with *ramification degree/index* n.

[2.2] Example: There are more complicated possibilities of ramification. For Y given by $w^5 + w^2 + z = 0$ with $\pi(z, w) = z$, at $z_o = 0$ the equation becomes $w^5 + w^2 = 0$, which has a double root at $w_o = 0$, and three other (distinct) roots, $w_1 = -1, w_2 = e^{\pi i/3}, w_3 = e^{-\pi i/3}$. The derivative $5w^4 + 2w$ is not 0 at any of the latter three points, so by holomorphic implicit function theorem there are holomorphic functions F_1, F_2, F_3 locally for z near $z_o = 0$ such that $F_j(0) = w_j$ for $j = 1, 2, 3$, and $F_j^5(z) + F_j(z)^2 + z = 0$ for z near $z_o = 0$. The point $w_o = 0$ is *ramified* of degree 2 above $z_o = 0$. In summary, above a small-enough neighborhood U of $z_o = 0$, $\pi^{-1}(U)$ breaks into four pieces, one essentially $w \to w^2$, the other three local isomorphisms. We say $z_o = 0$ is ramified. More precisely, there is one ramified point *above* $z_o = 0$, namely w_o, and the three unramified points w_1, w_2, w_3.

Note that this Y is *not* singular at any point $(z, w) \in \mathbb{C}^2$, because $(z, w) \to w$ in fact gives an isomorphism to $\mathbb{C}$, because $z = w^5 + w^2$ throughout.

[2.3] Example: Another example of more complicated ramification: For Y given by $(w+1)(w-1)^3 \cdot w^2 + z = 0$, the only ramified z_o is $z_o = 0$. The resulting equation has a simple root $w = -1$, a triple root $w = 1$, and a double root $w = 0$. That is, there are exactly 3 points above $z_o = 0$, one unramified, one with ramification degree 3, and one with ramification degree 2.

[2.4] Example: A simple family of examples is *hyperelliptic curves*, given by $w^2 = f(z)$ with $f \in \mathbb{C}[z]$. To avoid self-intersections in $\mathbb{C}^2$, we restrict attention to f square-free. At z_o such that $f(z_o) \neq 0$, there are two *distinct* square roots $\pm w_o \neq 0$ of $f(z_o)$, and the derivative $\frac{\partial}{\partial w}(w^2 - f(z_o)) = 2w$ does not vanish at $w = w_o$. Thus, by the holomorphic inverse function theorem, there are two *holomorphic* square roots $\sqrt{f(z)}$ near $z = z_o$. In particular above z_o with $f(z_o) \neq 0$ there is *no ramification*.

At z_o with $f(z_o) = 0$, there is just one w_o satisfying $w_o^2 = f(z_o)$, but this in itself is not quite proof of ramification, since we might have the misfortune of having a *self-intersection*. Fortunately, hyper-elliptic curves do not have self-intersections in the finite part $\mathbb{C}$ of $\mathbb{P}^1$:

Letting $f(x) = (x - x_1) \dots (x - x_n)$ with the x_j distinct, near x_1 the *other* factors *have* two distinct, holomorphic square roots. Thus, the equation can be rewritten

$$\Big(\frac{y}{\sqrt{(x - x_2)(x - x_3) \dots (x - x_n)}} \Big)^2 \;=\; x - x_1$$

which shows that there is ramification of index 2 above x_1.

[2.5] Example: **Fermat Curves:** These are curves $Y \subset \mathbb{C}^2$ defined by $z^n + w^n = 1$. Rewriting this as $w^n = 1 - z^n$, since there are n distinct n^{th} roots unless $1 - z^n = 0$, the only bad points are n^{th} roots of unity, and those points have ramification degree n.

---

3. *Compactification/projectivization of algebraic curves*

Centuries ago, and certainly by Riemann's time, it was understood that *points at infinity*, suitably interpreted, should be included as a genuine part of curves, to have the best versions of theorems. For example, *E. Bezout's theorem* would assert that the number of intersections of two planar curves, of degrees m and n, is the product mn. This is not correct without counting multiplicities and intersection points at infinity.

We should add *points at infinity* to the curve $Y \subset \mathbb{C}^2$ to make it *compact*. One way to do this is to *compactify/projectivize* it to a *projective* curve in $\mathbb{P}^2$. Another is to compactify it to a curve in $\mathbb{P}^1 \times \mathbb{P}^1$.

The $\mathbb{P}^1 \times \mathbb{P}^1$ compactification $\widetilde{Y}$ has the advantage that the maps $\pi : Y \to \mathbb{C}$ always extend to maps $\widetilde{Y} \to \mathbb{P}^1$. The $\mathbb{P}^2$ compactification does not always admit such an extension. On another hand, the $\mathbb{P}^1 \times \mathbb{P}^1$ compactification has the disadvantage that it most often has self-intersections at infinity. The $\mathbb{P}^2$ compactification is better behaved in that regard.

Recall that $\mathbb{P}^2 = (\mathbb{C}^3 - (0,0,0))/\mathbb{C}^\times$, and $\mathbb{C}^2 \subset \mathbb{P}^2$ by $(z,w) \to (z,w,1)\cdot\mathbb{C}^\times$. The added *points at infinity* are

$$(\text{points at } \infty \text{ on } \mathbb{P}^2) \;=\; \{(z,w,0) : z,w \text{ not both } 0\}/\mathbb{C}^\times \;\approx\; \mathbb{P}^1$$

In contrast, the points at infinity on $\mathbb{P}^1 \times \mathbb{P}^1$ are $\{\infty\} \times \mathbb{P}^1 \cup \mathbb{P}^1 \times \{\infty\}$.

To *homogenize* the polynomial f, that is, to define it on homogeneous coordinates (z,w,t) on $\mathbb{P}^2$, replace

$$f(z,w) \;=\; \sum_{t=0}^{n} \Big(\sum_{i=0^t} C_{t,i}\, z^i\, w^{t-i} \Big) \qquad\qquad (\text{constants } C_{t,i})$$

by

$$\widetilde{f}(z,w,h) \;=\; \sum_{t=0}^{n} h^{n-t} \Big(\sum_{i=0^t} C_{t,i}\, z^i\, w^{t-i} \Big)$$

The *projectivization* or *projective compactification* $\widetilde{Y}$ of Y is

$$\widetilde{Y} \;=\; \{(z,w,h) \in \mathbb{C}^3 - \{(0,0,0)\} : \widetilde{f}(z,w,h) = 0\} \;/\; \mathbb{C}^\times \;\subset\; \mathbb{P}^2$$

By design, $\widetilde{Y} \cap \mathbb{C}^2 = Y$.

The natural attempt to extend $\pi : Y \to \mathbb{C}$ to $\pi : \widetilde{Y} \to \mathbb{P}^1$ is

$$\pi(z,w,t) \bmod \mathbb{C}^\times \;=_{???}\; (z,t) \bmod \mathbb{C}^\times \;\in\; \mathbb{P}^1 \qquad\qquad (\text{hopefully mapping } \widetilde{Y} \text{ to } \mathbb{P}^1)$$

However, if the point $(0,*,0)$ lies on $\widetilde{Y}$, the problem is that the point $(0,0)$ in homogeneous coordinates does not exist. So the alleged $\pi(0,*,0)$ does not exist. This non-extendability occurs for hyperelliptic curves, as we see below.

The projectivization/compactification $\widetilde{Y} \subset \mathbb{P}^2$ is also referred to as a *Riemann surface*, and has better behavior than the affine curve Y. The $\mathbb{P}^1 \times \mathbb{P}^1$ compactification is rarely non-singular, but still may be referred to as a Riemann surface. Yes, this usage is in conflict with the idea that Riemann surfaces are *manifolds*. Nevertheless, the typical self-intersections introduced in the $\mathbb{P}^1 \times \mathbb{P}^1$ compactification $\widetilde{Y}$ are easy to *resolve*, in the sense of constructing a generically 1-to-1 surjection $\widetilde{Y}_1 \to \widetilde{Y}$ of another Riemann surface $\widetilde{Y}_1$ which *separates* the self-intersecting points on $\widetilde{Y}$. This is computationally useful.

Surely irreducibility of $Y \subset \mathbb{C}^2$ is equivalent to irreducibility of $\widetilde{Y} \subset \mathbb{P}^2$. At the polynomial-algebra level, this suggests

[3.1] Claim: A polynomial $f(z,w) \in \mathbb{C}[z,w]$ is irreducible if and only if its homogenization is irreducible as a polynomial in 3 variables. *[... iou ...]* ///

Examination of the behavior of $\widetilde{Y} \to \mathbb{P}^1$ at the points at infinity is accomplished through homogenization, for the $\mathbb{P}^2$ compactification, and by coordinates $1/z$ and $1/w$, for the $\mathbb{P}^1 \times \mathbb{P}^1$ compactification.

[3.2] Example: For Fermat curves, given by $z^n + w^n = 1$, to examine behavior at infinity, the $\mathbb{P}^2$ compactification works out well, as follows. The homogenized equation is $z^n + w^n = t^n$, and the points at infinity are where $t = 0$, namely, $z^n = w^n$, modulo $\mathbb{C}^\times$, with not both z, w equal to 0. This gives n distinct points at infinity, so the Fermat curves are non-singular at infinity, and have no ramification at infinity. Further, the map $\pi(z,w) = z$ extends to $\pi(z,w,t) = (z,t)$, which is well-defined on the projectivized curve, because not both z, t can be 0 on the projective Fermat curve.

[3.3] Example: For hyperelliptic curves, given by $w^2 = f(z)$, to examine ramification at infinity in the $\mathbb{P}^1 \times \mathbb{P}^1$ compactification, replace w by $1/w$ and z by $1/z$. For example, from $w^2 = z^6 - 1$ in coordinates at infinity, $(1/w)^2 = (1/z)^6 - 1$, which rearranges to $z^6 = w^2(1 - z^6)$ or

$$w^2 \;=\; \frac{z^6}{1 - z^6}$$

The right-hand side has two holomorphic square roots near $z_o = 0$, so there is *no ramification*. However, since both these local square root functions take value 0 at $z_o = 0$, there is a *self-intersection* of the curve.

The local *resolution of singularities* procedure here is to replace w by wz^3, and cancel the common z^6, giving $w^2 = 1/(1 - z^6)$. This is non-singular at infinity, and gives two distinct holomorphic square roots, and there is no ramification.

Similarly, in general, in the $\mathbb{P}^1 \times \mathbb{P}^1$ compactification, for $w^2 = f(z)$ with f square-free and *even* degree n, there is no ramification at infinity, but there is self-intersection, which can be locally smoothed out by replacing w by $wz^{n/2}$.

For f *odd* degree n, there is ramification of index 2 at infinity, as well as self-intersection. The self-intersection can be locally smoothed out, in coordinates at infinity, by replacing w by $wz^{\frac{n-1}{2}}$, leaving $w^2 = zg(z)$ for a polynomial g not vanishing at $z = 0$. While g has two holomorphic square roots near and at $z = 0$, the factor z has *no* holomorphic square root on any neighborhood of $z = 0$, and produces ramification.

The $\mathbb{P}^2$ compactification $\widetilde{Y}$ of the hyperelliptic curve Y given by $w^2 = f(z)$ with square-free f monic of degree n is better behaved at infinity, but does not admit an extension of $Y \to \mathbb{C}$ to $\widetilde{Y}$. First, in homogenous coordinates,

$$\widetilde{Y} \;=\; \{(z, w, t) \in \mathbb{C}^3 - (0, 0, 0) : t^{n-2}w^2 = \widetilde{f}(z, w)\} \bmod \mathbb{C}^\times$$

where $\widetilde{f}$ is the homogenization $\widetilde{f}(z, t) = t^n f(z/t)$. The points at infinity are where $t = 0$, and the equation becomes $0 = z^n$. Thus, $z = 0$ as well, so the only point at infinity is $(0, *, 0)$. There is no difficulty in this, but the purported projection map $\widetilde{Y} \to P^1$ by $(z, w, t) \bmod \mathbb{C}^\times \to (z, t) \bmod \mathbb{C}^\times$ is not defined. The downside of this is that we could not easily use results such as Riemann-Hurwitz about maps of *compact* Riemann surfaces to examine $\widetilde{Y}$. Thus, below, we will use the $\mathbb{P}^1 \times \mathbb{P}^1$ self-intersecting compactification, together with a method of *blowing up* (also called *resolving*) singularities to apply Riemann-Hurwitz to hyperelliptic curves.

[3.4] Example: The $\mathbb{P}^1 \times \mathbb{P}^1$ compactification of the Fermat curve $z^n + w^n = 1$ has self-intersections at infinity. Namely, replacing z by $1/z$ and w by $1/w$, multiplying out, the equation is $w^n + z^n = z^n w^n$, or $w^n = z^n/(z^n - 1)$. Near $z = 0$, there are n distinct holomorphic n^{th} roots of $z^n - 1$, and z^n has n distinct holomorphic n^{th} roots. That is, there are n distinct holomorphic functions w there. However, all these functions take value 0 at $z = 0$, so there is an n-fold self-intersection.

The local resolution of singularities procedure is to replace w by wz, and cancel the factor of z^n, to obtain $w^n = z^n - 1$ near $z = 0$. This eliminates the self-intersection.

---

4. *Real and complex manifolds, Riemann surfaces*

We recall standard terminology and facts. There are minor logical inconsistencies in terminology, which are due to juxtapositions of contexts. This is harmless, and inevitable. Context should clarify.

A *topological manifold* is a topological space in which every point has a neighborhood U homeomorphic to an open in $\mathbb{R}^n$, by a homeomorphism (to the image) $\varphi : U \to \mathbb{R}^n$. These pieces fit together nicely in the sense that, when U, V (with maps φ, ψ) overlap non-trivially, the composite

$$\varphi(U \cap V) \xrightarrow{\varphi|^{-1}_{U\cap V}} U \cap V \xrightarrow{\psi|_{U\cap V}} \psi(U \cap V)$$

is a continuous map from the subset $\varphi(U \cap V) \subset \mathbb{R}^n$ to the subset $\psi(U \cap V) \subset \mathbb{R}^n$. The maps $\varphi : U \to \mathbb{R}^n$ are *coordinate maps* or *charts* or *local coordinates*. The compositions $\psi|_{U\cap V} \circ \varphi^{-1}|_{U\cap V}$ are *transition maps*. The theorem of *invariance of domain*, from basic algebraic topology, proves that the dimension of a topological manifold is well-defined. That is, if $\mathbb{R}^m \approx \mathbb{R}^n$, then $m = n$.

A *(topological) surface* is a two-dimensional (topological) real manifold.

A *smooth (real) manifold* is a topological (real) manifold where the transition maps $\psi|_{U\cap V} \circ \varphi^{-1}|_{U\cap V}$ mapping open subset $\varphi(U \cap V) \subset \mathbb{R}^n$ to another open subset $\psi(U \cap V) \subset \mathbb{R}^n$ are *diffeomorphisms*. That is, the transition maps are smooth maps with smooth inverses. Here *smooth* means indefinitely/infinitely differentiable in the real-variables sense.

A *(smooth) surface* is a (real) two-dimensional smooth manifold.

A *complex manifold* is a topological space in which every point has a neighborhood U homeomorphic to an open in $\mathbb{C}^n$, by a homeomorphism (to the image) $\varphi : U \to \mathbb{C}^n$. These pieces fit together in the sense that, when U, V (with maps φ, ψ) overlap non-trivially, the composite

$$\varphi(U \cap V) \xrightarrow{\varphi|^{-1}_{U\cap V}} U \cap V \xrightarrow{\psi|_{U\cap V}} \psi(U \cap V)$$

is a *complex-differentiable* map from the subset $\varphi(U \cap V) \subset \mathbb{C}^n$ to the subset $\psi(U \cap V) \subset \mathbb{C}^n$. The *complex* dimension of the manifold is n, while the *real* dimension is $2n$.

In this context, a *Riemann surface* is a (complex-) one-dimensional complex manifold. It is a real two-dimensional manifold with extra structure.

[4.1] Claim: Let $\pi : Y \to \mathbb{C}$ be a ramified cover, with Y the affine Riemann surface attached to a suitable polynomial $f(z, w)$. Let Y' be Y with bad points removed. For $y_o \in Y'$, π restricted to a sufficiently small neighborhood of y_o is a *coordinate map*. The collection of all such makes Y' a (complex-) one-dimensional complex manifold.

Proof: [... iou ...] ///

[4.2] Remark: A better assertion is true, but requires more preparation.

---

5. *Riemann-Hurwitz theorem on ramified coverings*

Let $\pi : Y \to X$ be a ramified cover of a compact connected Riemann surface X by another such Y. The case that $X = \mathbb{P}^1$ and Y is a *projective* planar curve, as above, is the base case.

A geometric characterization of the *genus* g of a compact Riemann surface X as the number of *handles* it has, when modeled topologically as a *sphere with handles*. Genus g can also be characterized as half the dimension of the first homology group $H_1(X, \mathbb{R})$. Further, given a *triangulation* of X, with V vertices, E edges, and F faces, there is the Euler-characteristic description

$$2 - 2g \;=\; V - E + F$$

Evidently this is independent of the specific triangulation. Triangulating the two-sphere as surface of a tetrahedron, we find

$$2 - 2g \;=\; 4 - 6 + 4 \;=\; 2 \qquad \text{(for two-sphere)}$$

indicating that the genus of a sphere is 0. This is consistent with the other characterizations.

In a ramified covering $\pi : Y \to X$, the genus g_Y of Y is related to the genus g_X of X by

[5.1] Theorem: *(Riemann-Hurwitz)*

$$2 - 2g_Y \;=\; n \cdot (2 - 2g_X) - \sum_{\text{ramified } y_o} (e_{y_o} - 1)$$

where the sum is over points $y_o \in Y$ ramified in $\pi : Y \to X$, and e_{y_o} is the ramification index of y_o over $\pi(y_o)$. ///

Since the genus of $\mathbb{P}^1$ is 0,

[5.2] Corollary: For a ramified cover $\pi : Y \to \mathbb{P}^1$,

$$2 - 2g_Y \;=\; 2n - \sum_{\text{ramified } y_o} (e_{y_o} - 1)$$

where the sum is over points $y_o \in Y$ ramified in $\pi : Y \to \mathbb{P}^1$, and e_{y_o} is the ramification index of y_o over $\pi(y_o)$. ///

A sketch of a proof of this can be given via triangulations of X whose 0-simplices include the ramification points of the cover.

[5.3] Example: **Hyperelliptic curves:** The easiest example of computing genus of (ramified) covers is *hyper-elliptic* curves: $y^2 = f(x)$ where f is a square-free polynomial in x. As earlier, the square-free condition avoids *reducibility* and *self-intersection* of the curve in $\mathbb{C}$. For F of odd degree d, there is ramification of degree 2 at infinity: the change of coordinates replacing z, w by $1/z, 1/w$ gives $\frac{1}{w^2} = f(\frac{1}{z})$, or $z^d = w^2 F(z)$ where $F(z) = z^d f(\frac{1}{z})$. Because f is genuinely of degree d, it's highest-degree term is not 0, so $F(0) \neq 0$, and at $z_o = 0$, we have a double root $w_o = 0$. For any degree d, $F(z)$ has two distinct holomorphic square roots for z near 0. Since d is odd, z^d does not have a holomorphic square root on any neighborhood of 0, so there is ramification, of degree 2. For f of even degree d, there is no ramification at infinity, since z^d has holomorphic square roots $\pm z^{d/2}$.

As earlier, at infinity, a change of variables replacing w by $wz^{\frac{n}{2}}$ for even degree n and w by $wz^{\frac{n-1}{2}}$ for odd n eliminates the self-intersection at infinity.

[5.4] Corollary: For hyper-elliptic curves $\pi : Y \to \mathbb{P}^1$ given by $y^2 = f(x)$ with f a square-free polynomial of degree d in x, the Riemann-Hurwitz formula simplifies to

$$2 - 2g_Y \;=\; 2 \cdot (2 - 2 \cdot 0) - d - \begin{cases} 1 & (\text{for } d \text{ odd}) \\ 0 & (\text{for } d \text{ even}) \end{cases}$$

That is,

$$g_Y \;=\; \begin{cases} \dfrac{d-1}{2} & (\text{for } d \text{ odd}) \\ \dfrac{d-2}{2} & (\text{for } d \text{ even}) \end{cases}$$

[5.5] Example: **Fermat curves:** The curve Y given by $z^n + w^n = 1$ has ramification degree n at every n^{th} roots of unity. To understand the situation at infinity, use homogeneous coordinates (z, w, t) and homogenized equation $z^n + w^n = t^n$, and set $t = 0$. This gives $z^n + w^n = 0$, which can be normalized (by adjusting mod $\mathbb{C}^\times$) to gives $1 + w^n = 0$. This has n distinct solutions, so, as earlier, the Fermat curve is smooth at ∞, and there is no ramification. Thus,

$$2 - 2g_Y \;=\; 2n - \sum_{j=1}^{n} (n-1) \;=\; 2n - n(n-1)$$

and

$$g_Y \;=\; \frac{(n-1)(n-2)}{2}$$

---

6. *An analogue of Fermat's last theorem*

[6.1] Theorem: For $n \geq 3$, there are no non-constant rational functions f, g in $\mathbb{C}(z)$ such that

$$f(z)^n + g(z)^n \;=\; 1 \qquad\qquad (\text{for all } z \in \mathbb{C})$$

[6.2] Remark: Of course, for $n = 2$, we have a parametrization for Pythagorean triples:

$$\Big(\frac{z^2-1}{z^2+1}\Big)^2 + \Big(\frac{2z}{z^2+1}\Big)^2 \;=\; 1 \qquad\qquad (\text{for all } z \in \mathbb{C} \text{ except } \pm i)$$

Proof: We invoke the corollary of the Riemann-Hurwitz theorem, that for a non-constant map $\pi : Y \to X$ of compact, connected Riemann surfaces X, Y, the genus of X must be less than or equal that of Y. A parametrization as in the theorem is (extends to) a map $\mathbb{P}^1 \to X$ of $\mathbb{P}^1$ to the compactification/projectivization X of the Fermat curve $z^n + w^n = 1$. From Riemann-Hurwitz, the latter has genus $(n-1)(n-2)/2$. For $n \geq 3$ this is greater than 0. (For $n = 2$ it is 0, so not pretending to disallow the Pythagorean parametrization.) ///

[6.3] Remark: Long ago, I approximately proved something like this by some dubious and excruciating polynomial computations. Luckily, Joe Lipman explained to me that, in a just-slightly-sophisticated context, this result *is obvious*, in the sense that there are conceptual/qualitative, not computational, reasons for its truth. Specifically, *genus* cannot increase under a non-constant map of (compact, connected) Riemann surfaces. An amazing mathematical moment.

---

7. *Example of locating bad points*

[7.1] Example: Consider $f(x, y) = y^3 + 3xy + x^3$. At $x = 0$ there is the obvious degeneration, but what else? Applying the Euclidean algorithm in $\mathbb{C}(x)[y]$ to $F(y) = f(x, y)$ and $F'(y) = \frac{\partial F}{\partial y} = 3y^2 + 3x$:

$$F(y) - \frac{y}{3} \cdot F'(y) \;=\; \Big(y^3 + 3xy + x^3\Big) - \frac{y}{3} \cdot \Big(3y^2 + 3x\Big) \;=\; 2xy + x^3$$

Division-with-remainder of $F'(y)$ by a linear (in y) polynomial $y - a$ produces a remainder equal to evaluation of $F'(a)$. Away from $x = 0$, dividing by $2xy + x^3$ will produce the same remainder as dividing by $y + \frac{x^2}{2}$, namely, evaluation at $-x^2/2$:

$$\gcd(F(y), F'(y)) \;=\; F'(x^2/2) \;=\; 3 \cdot ((-x^2/2)^2 + x) \;=\; \frac{3}{4} \cdot x \cdot (x^3 + 4)$$

Thus, in this example, in addition to $x = 0$, the other points over which some ramification occurs are the cube roots of -4.

If we remember the symmetric-function computation determining the *discriminant* of a cubic $y^3 + by + c$ with roots α, β, γ

$$(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 \;=\; -4b^3 - 27c^2$$

then we can check the outcome of the *gcd* computation: for $y^3 + 3xy + x^3$ the discriminant formula gives

$$\text{discriminant } y^3 + 3xy + x^3 \;=\; -4(3x)^3 - 27(x^3)^2 \;=\; -27x^3(4 + x^3)$$

For x a cube root $-\sqrt[3]{4}$ of -4, the equation become $y^3 - 3\sqrt[3]{4}y - 4 = 0$. In fact, the Euclidean algorithm above shows that when x is a cube root of -4, the linear (in y) factor $2xy + x^3 = 2x \cdot (y + \frac{x^2}{2})$ is the common factor of both $f(y)$ and $f'(y)$, meaning that $f(y)$ has a repeated root $y = -x^2/2$, appearing with multiplicity

exactly 2. This computation also checks that the root is *not* of multiplicity 3, unlike the situation at $x = 0$, where the equation degenerates into $y^3 = 0$.

Thus, there are two points y_1, y_2 lying over x_o a cube root of -4, and one of the two has ramification index 2, while the other is unramified.

---

8. *Newtown polygons and ramification*

Newton polygons, described below, subsume *Eisenstein's criterion* for irreducibility as a very special case. More important for our purposes is the information they give about ramification.

To gain information about the ramification of $\pi : Y \to \mathbb{P}^1$ described by a polynomial relation $F(x, y) = 0$ at a point $\pi : (x_o, y_o) \to x_o$, first rewrite the relation as a monic polynomial in $y - y_o$, with coefficients in $\mathbb{C}(x)$:

$$(y - y_o)^n + c_{n-1}(x)(y - y_o)^{n_1} + \ldots + c_2(x)(y - y_o)^2 + c_1(x)(y - y_o) + c_o(x) \qquad (\text{with } c_j(x) \in \mathbb{C}(x))$$

Let $\text{ord}_{x-x_o} f(x)$ be the order of vanishing of a rational function $f(x)$, including the possibility that $f(x)$ has a pole, so the order can be negative.

Consider data points (i, j) with $j = j(i)\text{ord}_{x-x_o} c_{n-i}(x)$, putting $j = j(i) = +\infty$ if $c_{n-i} = 0$. Consider piecewise-linear convex (bending upward) functions P on the interval $[0, n]$ such that for each integer i

$$P(i) \ \leq \ j(i)$$

Let N be the *maximum* among these, and let $i_1 < \ldots < i_m$ be the integer indices where *equality* occurs:

$$N(i_k) \ = \ \text{ord}\, c_{n-(i+k)}(x)$$

The line segements

$$\ell_k \ = \ \text{line segment connecting } N(i_k) \text{ and } N(i_{k+1})$$

form the *Newton polygon* attached to f.

Adjacent segments with the same slope are considered to be parts of a single segment.

For example, at $x_o = 0 = y_o$, the polynomial $y^5 + x^2y^3 + x(x + 1)y + x^2$ has data points $(0, 0)$, $(1, +\infty)$, $(2, +\infty)$, $(3, 2)$, $(4, 1)$, and $(5, 2)$. Thus, the Newton polygon has vertices $(0, 0)$, $(4, 1)$, and $(5, 2)$. The two points with second coordinate $+\infty$ certainly lie strictly above the Newton polygon, but also the point $(3, 2)$ lies above it.

The precise content of the Newton polygon attached to a polynomial $f(x, y)$ will be discussed below. Here, we note some special corollaries in which the Newton polygon gives complete information about ramification. The first is parallel to the situation of Eisenstein's criterion, already generalizing it somewhat:

[8.1] Corollary: If the Newton polygon at x_o consists of a single segment with *rise* (change in vertical coordinate) and *run* (change in horizontal) *relatively prime*, then the covering is *totally ramified* over x_o, of degree equal to the horizontal length. (Proof below.)

For example, $y^5 + x^3y + x^2 = 0$ at $x = 0$ has a Newton polygon of slope $2/5$, so the ramification is *total*, the index is 5.

[8.2] Corollary: Every length-1 segment having *integer slope* indicates an *unramified* point (x_o, y_o) lying over x_o. That is, for each such segment, there is a holomorphic function y of x near x_o such that $y(x_o) = y_o$. (Proof below.)

For example, $y^5 + xy^2 + x^2y + x^4 = 0$ at $x = 0$ has a Newton polygon with three segments, one of length 3 and slope $1/3$, another of length 1 and slope 1, and another of length 1 and slope 2, so from the latter we see that there are two unramified points over $x = 0$.

[8.3] Corollary: Every segment whose *rise* n and *run* m are *relatively prime* indicates a point (x_o, y_o) ramified with index m over x_o. (Proof below.)

Thus, continuing with the previous example, in addition to the two unramified points over $x_o = 0$, there is exactly one other point, and it has ramification index 3.

When the rise and run of a segment are *not* relatively prime, there is ambiguity in the conclusion. For example, for $y^5 + xy^2 + x^3$ at $x = 0$, there is one segment of length 3 and slope $2/3$, indicating a point with ramification index 3, but the other segment has rise 2 and slope 2. Without further effort, we cannot tell whether there are two unramified points lying over x_o, or a further single point with ramification index 2. Via *Hensel's lemma*, below, we can determine that there are two unramified points in addition to the point with ramification index 3. That is, there are two distinct holomorphic functions y of x near x_o satisfying the equation.

---

9. Newton-Raphson/Hensel's lemma

The Newton-Raphson method, in the better form due to Raphson, approximates real roots of polynomials f in $\mathbb{R}[x]$ by iteratively sliding down the tangent from the value $f(x_n)$ at x_n to (what we hope is) an improved approximation

$$x_{n+1} \;=\; x_n - \frac{f(x_n)}{f'(x_n)}$$

In good situations, $\lim_n x_n$ is a root of $f(x) = 0$. In this incarnation, there is no advance assurance that a root *exists*, and even if a root is known to exist, there can be complications due to very small non-zero values, for example.

In contrast, the analogue for p-adic numbers, *Hensel's Lemma*, works much better! Here, we want an instance of an abstracted version of Hensel's Lemma, applicable to solving equations $F(x, y) = 0$ as above. Although these ideas admit further abstraction, for tangibility we consider a specific setting.

Namely, we consider the ring $\mathbb{C}[[x]]$ of *formal power series* in x. Formal power series are not *formal* in the pejorative sense of allegedly having no genuine meaning, or in any sense of asserted contentless-ness, despite some sources' treatment of them as such. In terms of *notation*, a formal power series in $\mathbb{C}[[x]]$ is of the form

$$a_o + a_1 x + a_2 x^2 + a_3 x^3 + \dots \qquad\qquad (\text{with } a_j \in \mathbb{C})$$

with no conditions on the growth of the coefficients a_j. The notational sense is clear, but the content or meaning is not adequately conveyed by a superficial appraisal of the notation.

One relatively elementary, concrete description of the formal power series ring $\mathbb{C}[[x]]$ as a genuine object is as the *completion* of the polynomial ring $\mathbb{C}[x]$ with respect to the x-adic metric, $|\cdot|_x$, defined by

$$|x^n \cdot f(x)|_x \;=\; 2^{-n} \qquad\qquad (\text{for } f(x) \in \mathbb{C}[x] \text{ prime to } x)$$

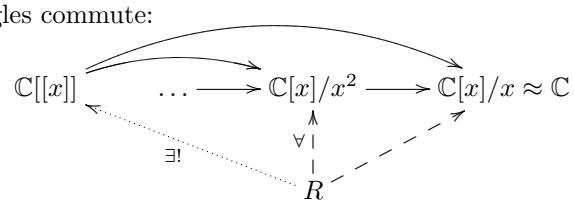
Any other constant > 1 will do in place of the 2. That is, polynomials highly divisible by x are small.

A slightly less elementary characterization, more useful in the long run, is that $\mathbb{C}[[x]]$ is the (projective) *limit* of the quotient rings $\mathbb{C}[x]/x^n \cdot \mathbb{C}[x]$. That is, first, there are commutative ring homomorphisms $\mathbb{C}[[x]] \to \mathbb{C}[x]/x^n$ for all n, sending 1 to 1, and *compatible* in the sense that all triangles commute:

$$\mathbb{C}[[x]] \;\begin{array}{c}\nearrow \\ \searrow\end{array}\; \dots \longrightarrow \mathbb{C}[x]/x^2 \longrightarrow \mathbb{C}[x]/x \approx \mathbb{C}$$

Second, for all *compatible* families of commutative ring homomorphisms $R \to \mathbb{C}[x]/n$ there is a unique

$R \to \mathbb{C}[[x]]$ making all triangles commute:



These two descriptions produce the same object $\mathbb{C}[[x]$.

The field of fractions of $\mathbb{C}[[x]]$, denoted $\mathbb{C}((x))$, is (provably) the ring of *finite-nosed* formal Laurent expansions. In fact, there is only one ring element needing an inverse, x, so

$$\mathbb{C}((x)) \;=\; \mathbb{C}[[x]][\frac{1}{x}]$$

Analogously the ring of p-adic integers $\mathbb{Z}_p$ is a metric completion of $\mathbb{Z}$ with respect to the p-adic metric $|p^n \cdot \frac{a}{b}|_p = p^{-n}$ with a, b prime to p. Also, $\mathbb{Z}_p$ is the limit of quotients $\mathbb{Z}/p^n$. The field of fractions $\mathbb{Q}_p$ is $\mathbb{Z}_p[1/p]$, since p is the only non-unit.

[9.1] Claim: *(Simplest Hensel's lemma)* For monic $f(Y) \in \mathbb{C}[[x]][Y]$, for $y_o \in \mathbb{C}[[x]]$ is such that $f(y_o) = 0 \bmod x$ but $f'(y_o) \neq 0 \bmod x$, the recursion

$$y_{n+1} \;=\; y_n - \frac{f(y_n)}{f'(y_n)}$$

converges in $\mathbb{C}[[x]]$ to a solution y of $f(y) = 0$, and $y = y_o \bmod x$.

Proof: [... iou ...] ///

[9.2] Claim: *(Next-simplest Hensel's lemma)* For monic $f(Y) \in \mathbb{C}[[x]][Y]$, for $y_o \in \mathbb{C}[[x]]$ is such that $|f(y_o)/f'(y_o)^2|_x < 1$ (the denominator is squared!), the recursion

$$y_{n+1} \;=\; y_n - \frac{f(y_n)}{f'(y_n)}$$

converges in $\mathbb{C}[[x]]$ to a solution y of $f(y) = 0$, and $y = y_o \bmod x$.

Proof:

[... iou ...]

///

[9.3] Claim: *(Another Hensel's lemma)* For monic $f(Y) \in \mathbb{C}[[x]][Y]$, if $f(Y) = g_o(Y) \cdot h_o(Y) \bmod x$ for *relatively prime*, monic $g_o(Y), h_o(Y) \in \mathbb{C}[Y]$, then there is a recursion to obtain relatively prime, monic $g(Y), h(Y) \in \mathbb{C}[[x]](Y)$ such that $g(Y) = g_o(Y) \bmod x$, $h(Y) = h_o(Y) \bmod x$, and $f(Y) = g(Y) \cdot h(Y)$

Proof:

[... iou ...]

///

[9.4] Mild pathology

$$y^2(y-1)^2 + xy + x \;=\; 0$$

has no roots y in $\mathbb{C}[[x]]$, because mod x it is

$$y^2(y-1)^2 \;=\; 0 \qquad\qquad (\text{mod } x)$$

Mod x^2, trying $y = ax$, it gives an impossible equation

$$x \;=\; 0 \qquad\qquad (\text{mod } x^2)$$

and similarly for $y = 1 + ax$. If we try to use the simplest form of Hensel's lemma, starting with $y_o = 0$, *[... iou ...]*

---

10. *Proofs about Newton polygons*

[10.1] Corollary: Let m_j be the slope of ℓ_j, and let p_j be the length of the projection of ℓ_j to the horizontal axis. Then there are exactly p_j roots of f in $\mathbb{C}[[x - x_o]]_{\text{sep}}$ with ord equal to m_j.

Proof: Let $\nu_1 < \ldots < \nu_m$ be the distinct ords of the roots, and suppose that there are exactly μ_i roots with ord ν_i. Let σ_j be the j^{th} symmetric function of the roots, so $c_i = \pm\sigma_i$.

Let $\rho_1, \ldots, \rho_{\mu_1}$ be the roots with largest ord. Since

$$\sigma_{\mu_1} = \rho_1 \ldots \rho_{\mu_1} + (\text{other products})$$

where the other products of μ_1 factors have strictly smaller ords. By the ultrametric inequality,

$$\text{ord}(\sigma_{\mu_1}) = \text{ord}(\rho_1 \ldots \rho_{\mu_1}) = \mu_1\nu_1$$

Similarly, let $\tau_1, \ldots, \tau_{\mu_2}$ be the second-largest batch of roots, namely, roots with ord ν_2. Then

$$\sigma_{\mu_1+\mu_2} = \rho_1 \ldots \rho_{\mu_1}\tau_1 \ldots \tau_{\mu_2} + (\text{other products})$$

where all the other products have strictly smaller ord. Again by the ultrametric inequality

$$\text{ord}(\sigma_{\mu_1+\mu_2}) = \text{ord}(\rho_1 \ldots \rho_{\mu_1}\tau_1 \ldots \tau_{\mu_2}) = \mu_1\nu_1 + \mu_2\nu_2$$

Generally,

$$\text{ord}(\sigma_{\mu_1+\ldots+\mu_j}) = \mu_1\nu_1 + \ldots + \mu_j\nu_j$$

Therefore, the line segment connecting $N(n - \mu_1 - \ldots - \mu_j)$ and $N(n - \mu_1 - \ldots - \mu_{j+1})$ has slope $-\nu j + 1$ and the projecting to the horizontal axis has length μ_{j+1}.

On the other hand, for

$$\mu_1\nu_1 + \ldots + \mu_j\nu_j < M < \mu_1\nu_1 + \ldots + \mu_{j+1}\nu_{j+1}$$

by the ultrametric inequality

$$\text{ord}M \geq \min(\text{ord of products of } M \text{ roots}) = \mu_1\nu_1 + \ldots + \mu_j\nu_j + (M - \mu_1 - \ldots - \mu_j)\nu_{j+1}$$

That is, $N(n - M)$ lies on or above the line segment connecting the two points $N(n - \mu_1 - \ldots - \mu_j)$ and $N(n - \mu_1 - \ldots - \mu_{j+1})$. ///

[10.2] Corollary: *(Irreducibility criterion)* Let f be monic of degree n over an ultrametric local field k as above. Suppose that the Newton polygon consists of a single line segment of slope $-a/n$ where a is relatively prime to n. Then f is irreducible in $k[x]$.

Proof: By the theorem, there are n roots of ord a/n. Since a is prime to n, the field $k(\alpha)$ generated over k by any one of these roots has ramification index divisible by n, by the following lemma, for example. But $[k(\alpha) : k] \leq n$, so the field extension degree is exactly n. ///

[10.3] Lemma: Let α belong to the separable closure of the ultrametric field k, and suppose that $\mathrm{ord}\alpha = a/n$ with a relatively prime to n. Then $k(\alpha)$ has ramification index divisible by n (and, thus n divides $[k(\alpha) : k]$).

Proof: Let ϖ be a local parameter in the extension $k(\alpha)$. Then

$$\mathrm{ord}\varpi = \frac{1}{e}$$

where e is the ramification index of the extension. Since α differs by a unit from some integer power of ϖ,

$$\frac{a}{n} = \mathrm{ord}\alpha \in \frac{1}{e} \cdot \mathbb{Z}$$

That is, $ea \in n\mathbb{Z}$. Since a is prime to n, it must be that n divides e, which divides the field extension degree in general. ///

[10.4] Corollary: *(Eisenstein's criterion)* Let f be monic of positive degree over a principal ideal domain R. Let E be the field of fractions of R. Let π be a prime element of R dividing all the coefficients of f (apart from the leading one, that of x^n), and suppose that π^2 does *not* divide the constant coefficient. Then f is irreducible in $E[x]$.

Proof: Let k be the π-adic completion of E, and $\mathfrak{o}$ the valuation ring in k. In fact, f is irreducible in $k[x]$. The hypothesis implies that the Newton polygon consists of a single segment connecting $(0, 1)$ and $(n, 0)$, with slope $-1/n$. Thus, by the previous corollary, f is irreducible in $k[x]$. ///

[10.5] Corollary: In the situation of the theorem, the polynomial f factors over k into polynomials f_i of degrees d_i, where all roots of f_i have ord $-m_i$. Let $m_i = a_i/d_i$, if a_i is relatively prime to d_i then f_i is *irreducible* over k and any root of f_i generates a totally ramified extension of k.

Proof: If α, β are Galois conjugates, then their ords are the same. Thus, the set of roots with a given ord is stable under Galois. That is, the monic factor f_i of f with these as roots has coefficients in the ground field k. If the ord of α is of the form a/M with numerator prime to M then α generates an extension of degree divisible by M, by the lemma above. Thus, f_i is irreducible if in lowest terms $-m_i$ has denominator d_i. ///

[10.6] Remark: In this last corollary there is no conclusion about the irreducibility of the factor f_i if the denominator of $-m_i$ (in lowest terms) is not the maximum possible, d_i. That is, we reach a sharp conclusion only for totally ramified extensions.

---

11. *Newton-Puiseux series*

A *Newton-Puiseux* series is a power series in $z^{1/n}$ for some positive integer n.

[11.1] Theorem: The only (finite) algebraic extensions of $\mathbb{C}((z))$ are obtained by adjoining $z^{1/n}$ for $n = 2, \ldots$. *[... iou ...]*

We will prove this after some examples that illustrate the sort of phenomena that the proof must accommodate.

---

12. *Appendix: Euler characteristics*

For a *triangulated* (connected, compact, oriented) surface with V vertices, E edges, and F faces, the *genus* (number of *handles*) is determined via the *Euler characteristic*

$$2 - 2g \;=\; V - E + F$$

Euler approximately proved something in this direction. Making a precise assertion, and proving it, is non-trivial.

The classification of (compact, connected, oriented) surfaces by their *genus*, is non-trivial. The *idea* is that the surface is a *sphere with handles*, and the genus is the number of handles. It is not obvious that this is an adequate or correct description, although it is plausible, and was proven correct in the early 20th century.

Alternatively, for a compact, connected, oriented surface S, the genus is *half* the dimension of the first homology $H_1(S)$.

The Euler characteristic of a finite sequence of real vector spaces $V_0, V_1, V_2, \ldots$ is the alternative sum of dimensions:

$$\chi(V_0, V_1, V_2, \ldots) \;=\; \dim V_0 - \dim V_1 + \dim V_2 - \dim V_3 + \ldots$$

Letting V_i be the real vector space with basis consisting of i-dimensional simplices in a triangulation of a surface, we recover Euler's formula

$$\chi \;=\; \dim V_0 - \dim V_1 + \dim V_2 \;=\; V - E + F$$

However, one should reasonably worry that different triangulations could give different Euler characteristics. There is a reassuring re-expression of the Euler characteristic making it more clearly intrinsic:

The 0^{th} homology of a reasonable connected space is rank 1, as is the 2^{nd} homology of a compact, connected, oriented surface, and all higher homology is 0. This is not elementary, but granting this, the Euler characteristic of the sequence $H_0(S), H_1(S), H_2(S), \ldots$ can be rewritten as

$$\chi(H_0(S), H_1(S), H_2(S), \ldots) \;=\; \dim H_0(S) - \dim H_1(S) + \dim H_2(S) \;=\; 1 - 2g + 1 \;=\; 2 - 2g$$
