Math 500.02—Galois Groups and Fundamental Groups

David Meredith
Department of Mathematics
San Francisco State University
E-mail: meredith@sfsu.edu
URL: online.sfsu.edu/~meredith

December 14, 1999

Contents

Chapter 1

Syllabus

Instructor: Dr. David Meredith,
Office: TH 933
Phone: (415) 338-2199/2251
Fax: (415) 338-1461
E-mail: meredith@sfsu.edu
URL: online.sfsu.edu/~meredith

Time and Location: MWF 12-1 HH 831

Office Hours: MWF 11-12

Textbooks: Stewart, *Galois Theory,* Chapman and Hall, New York, 1989
Kuga, *Galois' Dream,* Birkhauser, Boston, 1993
Texts provided *gratis* to enrolled students.

Grading: There will be weekly assignments, class presentations and a final. They will count toward the grade as follows.

Assignments	50%
Class Presentations	30%
Final	20%.

Homework: There will be weekly homework assignments.

1. Assignments must be written in mathematical English, with complete sentences and paragraphs.
   (a) Begin each part with a statement of what you will prove or do.
   (b) Define all terms not in general currency in the mathematical world. Just because a symbol has appeared on the blackboard in class doesn't mean that you can use it without explanation.
   (c) A good test of the completeness of your work is that an advanced student not in this class should be able to read and understand your paper.
   (d) This would be a good time to begin to learn mathematical word-processing. I try not to be prejudiced against hand-written papers, but I usually fail.
2. You are expected to use the library if necessary. For example, the first assignment has some complex number calculations. You may want to refer to an elementary complex analysis text, and the library has many.
3. It is not expected that you will solve every problem completely. It is expected that your work will be complete and correct as far as it goes.

(a) If you cannot solve a problem, solve a simpler problem, or do an example, or at least explain very clearly what you can prove and what you cannot prove.

(b) Mathematicians almost never solve the big problem they set out to solve, but they solve a lot of smaller problems along the way. That's the way you should work.

4. Assignments can be completed by teams of up to three students. Teams should turn in a single copy of the assignment signed by all team members.

5. Because homework will be discussed in class the day it is due, late assignments cannot be accepted.

   (a) Do as much as you can on each assignment, always allowing enough time to write up your results.

6. The purpose of all these rules is two-fold: to help you learn mathematics better and to help you develop skills needed for your careers. Careful writing leads to complete understanding, and in your professional lives the most important skills are reliability (your work can be counted on to be correct), resourcefulness (get a good-enough answer), communication (explaining yourself orally and in writing), and teamwork.

Class Presentation: About once each week I will ask a student or team of students to present a topic in class, often the solution to a homework problem.

Final: The final exam is on Wednesday, December 15: 10:45-1:15. You may bring two pages of notes to the final.

Lectures: I will lecture about two days each week, counting days when guest lecturers visit from MSRI. Lecture notes will be available from my web site before the lectures are given, usually (I hope) by 10:00PM the previous evening. You should download them and bring printed copies to class to help you follow the material. This will reduce the need for notetaking and assure that the notes you do take are more accurate.

Description of the Course

This course brings together two areas of mathematics that each concern symmetry – symmetry in algebra, in the case of Galois theory; and symmetry in geometry, in the case of fundamental groups. In each of these two situations, mathematical objects can be studied by examining the forms that their symmetries can take. This course will consider how these two situations can interact, so that algebra can be used in the service of geometry, and vice versa, in order to study problems that would otherwise be intractable.

The course will be taught in conjunction with the fall Special Program on Symmetry at the Mathematical Sciences Research Institute (MSRI) in Berkeley. The class will visit the Institute and hear lectures at SFSU from leading researchers in the field. The course is part of the CIRE collaboration between MSRI and SFSU.

Prerequisites are at least one course in algebra and analysis, e.g. Math 320 and 370.

Chapter 2

Overview and Introduction to Complex Polynomials

1. Greetings (Hello) and rules of the road
   (a) Read the syllabus
   (b) Homework must be in correct mathematical English
   (c) Late homework will not be accepted
   (d) Questions are always in order
2. Overview
   (a) This course is about a deep connection between "arithmetic" and "geometry"
      1. Arithmetic means algebraic number theory, particularly the study of algebraic numbers over $\mathbb{Q}$
      2. Geometry means the study of Riemann surfaces, surfaces with complex-valued functions
         1. non-compact: Plane, cylinder
         2. compact: sphere, torus, many-handled torus
   (b) This connection has many parallels in 19th and 20th century mathematics
      1. Analytic number theory studies algebraic numbers as a subset of the complex numbers
      2. We can also study the "algebraic" subset of a Riemann surface
         1. Mordell's Theorem
         2. Fermat's Last Theorem
   (c) Analytic geometry (and calculus) connect geometry and analysis, a connection taken for granted in this course. The interesting idea is to extend the connection to arithmetic.
   (d) The connection we will study was conjectured by Alexander Grothendieck and proven by G. V. Belyi in 1979. It says that if a Riemann surface carries a certain kind of function ($\exists a, b, c \in \mathbb{C}$ such that $f'(x) = 0 \Longrightarrow f(x) \in \{a, b, c\}$ then:
      1. the Riemann surface can be defined by equations with algebraic number coefficients.
      2. Associated with the Riemann surface and the function f is a group related to the "Galois group" of the algebraic numbers required to define the surface.
      3. Also associated is a "dessin d'enfant"—a graph (in the sense of graph theory) that completely characterizes the function and the Riemann surface.
      4. The history is in the handout from Schneps, *The Grothendieck Theory of Dessins d'Enfants*
3. Complex numbers
   (a) The set of expressions $\{a + bi : a, b \in \mathbb{R}\}$. Represented by the complex plane.

(b) A field.

1. Add and subtract

$$(a+bi) \pm (c+di) = (a \pm c) + (b \pm d)\, i$$

2. Multiply

$$(a+bi)\,(c+di) = (ac-bd) + (ad+bc)\, i$$

1. So $i^2 = -1$, which is what makes $\mathbb{C}$ different from $\mathbb{R}$

3. Divide

$$\begin{aligned} \frac{a+bi}{c+di} &= \frac{a+bi}{c+di} \times \frac{c-di}{c-di} \\ &= \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} \\ &= \frac{(ac+bd)}{c^2+d^2} + \frac{(bc-ad)}{c^2+d^2} i \end{aligned}$$

(c) You can define all the transcendental functions with complex arguments and complex values, but we don't need all of them.

1. Number one on the all-time equation chart for mathematicians is Euler's identity

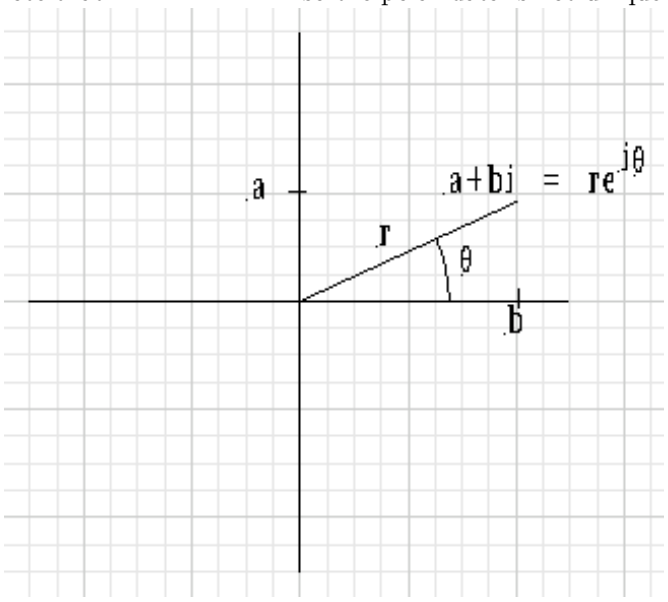
$$e^{\pi\, i} + 1 = 0$$

(d) The polar data for $z = a + bi$ is a length $r = \sqrt{a^2+b^2}$and angle $\theta = \arctan(a, b)$.

1. Sometimes the polar data is used in the form

$$z = re^{i\theta}$$

1. Note that $re^{i\theta} = re^{i(\theta+2\pi)}$ so the polar data is not unique



.

2. Conversely, given the polar data r, θ you can recover $a = r\cos\theta$ and $b = r\sin\theta$.
3. Multiplication is especially nice in polar form:

$$\left(re^{i\theta}\right)\left(se^{i\varphi}\right) = (rs)e^{i(\theta+\varphi)}$$

4. To find the n^{th} roots of a complex number z, you can use the polar form $z = re^{i\theta}$. Let $w^n = z$ and assume $w = se^{i\varphi}$. Then

$$\begin{aligned} \left(se^{i\varphi}\right)^n &= re^{i\theta} \\ s^n e^{i(n\varphi)} &= re^{i\theta} \\ s &= r^{1/n} \\ \varphi &= \frac{\theta + 2k\pi}{n}\ ,\ k = 0, \ldots, n-1 \end{aligned}$$

   1. There are n solutions, all distinct and symmetric about the origin.
   2. Example: the cube roots of $1 + i$. The polar data is $r = \sqrt{2}$ and $\theta = \frac{\pi}{4}$. Thus $s = \sqrt[6]{2} \approx 1.1225$ and $\varphi = \frac{\pi}{12}, \frac{3\pi}{4}, \frac{17\pi}{12}$

(e) *Mathematica* and *X(PLORE)* calculate with complex numbers.

4. Complex polynomials

(a) Using addition, subtraction and multiplication, you can define complex polynomials: $\alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n$ and complex polynomial functions $f(z) = \alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n$.

   1. These can be identified.
   2. The set is denoted $\mathbb{C}[z]$.

(b) Form a ring—can be added, subtracted and multiplied

(c) The degree of $f \neq 0$ is $\deg f$, the order of the highest non-zero term. The degree of 0 is not defined.

   1. If $f, g, f + g \neq 0$ then $\deg(f + g) \leq \max\{\deg f, \deg g\}$
   2. If $f, g \neq 0$ then $\deg(fg) = \deg f + \deg g$

(d) Have division with remainder: for any $f, g \in \mathbb{C}[z]$ there exists $q, r \in \mathbb{C}[z]$ such that $f = gq + r$ where $r = 0$ or $\deg r < \deg g$.

   1. Actually finding q and r is a good job for the computer. Consider

$$\frac{8 - 6z + 4z^2 - 2z^3 + 5z^4 + 3z^5}{3 + 2z - 4z^2}$$

   Apply "divide", get

$$-\frac{3}{4}z^3 - \frac{13}{8}z^2 - \frac{7}{8}z - \frac{85}{32} + \frac{\frac{511}{32} + \frac{31}{16}z}{3 + 2z - 4z^2}$$

   which means:

$$8 - 6z + 4z^2 - 2z^3 + 5z^4 + 3z^5 = \left(3 + 2z - 4z^2\right)\left(-\frac{3}{4}z^3 - \frac{13}{8}z^2 - \frac{7}{8}z - \frac{85}{32}\right) + \left(\frac{511}{32} + \frac{31}{16}z\right)$$

   2. Important special case: $g = z - a$. Then for any polynomial f we have

$$f = (z - a)q + r$$

   where $r = 0$ or $\deg r < 1$. That means $r = 0$ or r is a non-zero constant. In either case r is a complex number and $f(a) = r$

$$\begin{aligned} a \text{ is a root of } f &\iff r = 0 \\ &\iff z - a \text{ divides } f \text{ evenly} \\ &\iff f = (z - a)\, q \text{ for some polynomial } q. \end{aligned}$$

(e) But when does a polynomial have a root?

"ALWAYS" : Gauss

1. Every non-zero complex polynomial can be completely factored.
2. If $\deg f = n$ then $f = a(z - r_1)\cdots(z - r_n)$ for a unique set of roots $\{r_1, \ldots, r_n\}$ and unique coefficient a (the coefficient of z^n) .

(f) How can the roots be found, given the coefficients. Is there a constructive method?

1. If $\deg f = 1$ then $f = az + b$ and the root is $-b/a$
2. If $\deg f = 2$ then $f = az^2 + bz + c$ and the roots are $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
3. If $\deg f = 3, 4$ formulas are known.
4. if $f = z^n - a$ then the method above uses transcendental functions. It was not an exact, algebraic solution.
    1. Usually one accepts solutions involving radicals $\sqrt[n]{\text{expression}}$ like the quadratic formula.
5. In general, if $\deg f > 4$ then the answer is:

"NO" : Galois

(g) Are these answers inconsistent? Does it make sense to say that a polynomial "has" a root when there is no way to find it?

1. Platonism vs. constructivism in mathematics

(h) Roots can always be approximated by numerical methods. Your software can do this very well. Given $3z^4 - 4z^3 - z^2 + 3z + 1 = 0$ the approximate solutions are

$1.134\,7 + .540\,71i$
$1.134\,7 - .540\,71i$
$-.378\,29$
$-.557\,74$

5. Polynomials as maps

(a) A polynomial is a function $f : \mathbb{C} \longrightarrow \mathbb{C}$.

1. If $n = \deg f$ then f is almost n to 1 .
2. At least we can say that for any point $b \in \mathbb{C}$,
    1. $f^{-1}(b)$ is not empty by Gauss
    2. $f^{-1}(b)$ is a set of no more than n points, the solutions to $f - b = 0$

(b) To draw a picture of this map, you could try to stretch and fold the domain so that each point was above its image in the range. Good luck.

1. Show picture for x^2. Can't really be drawn in $\mathbb{R}^3$.

6. Local analysis on the domain—what happens at one point of the domain

(a) We say f is *non-singular* or *analytic* at a if $f'(a) \neq 0$. Otherwise we say that f is *singular* at a.

(b) If f is non-singular at a then f is non-singular in a neighborhood of a (because f' is continuous) and 1-1.

1. In fact f "preserves angles": If two curves pass through a non-singular point a then their images pass through $f(a)$ and the tangents meet at the same angles.

(c) A polynomial can be expanded about a point. Given a polynomial

$$f(z) = \alpha_0 + a_1 z + \cdots \alpha_n z^n$$

and $a \in \mathbb{C}$, we can find unique coefficients β_i such that

$$f(z) = \beta_0 + \beta_1 (z - a) + \cdots + \beta_n (z - a)^n$$

1. This is the power series for $f(z)$ about $z = a$
2. The easy way to calculate the coefficients β_i is to compute $f(z+a)$ and collect the coefficients of z, which will be the β_i. Example

$$\begin{aligned} f(z) &= 2z^3 - 9z^2 + 12z - 4 \\ a &= 1 \\ f(z+1) &= 2(z+1)^3 - 9(z+1)^2 + 12(z+1) - 4 \\ &= 1 - 3z^2 + 2z^3 \\ f(z) &= 1 - 3(z-1)^2 + 2(z-1)^3 \end{aligned}$$

(d) Obviously, if you expand a polynomial f about $z = a$, the coefficients β_i satisfy

$$\beta_i = \frac{f^{(i)}(a)}{i!}$$

1. This is a formula from power series theory, but the proof for polynomials is direct. In the expanded form,

$$\begin{aligned} f^{(i)}(z) &= i!\beta_i + \frac{(i+1)!}{1}\beta_{i+1}(z-a) + \cdots \\ &\quad + \frac{(i+j)!}{j!}\beta_{i+j}(z-a)^j + \cdots \\ &\quad + \frac{n!}{(n-i)!}\beta_n(z-a)^{n-i} \\ f^{(i)}(a) &= i!\beta_i \end{aligned}$$

(e) The *multiplicity* of f at a is the smallest integer $i \geq 1$ such that $\beta_i \neq 0$ (ignore β_0). In the example, the multiplicity of f at 1 is 2.

1. $f'(a) = 0 \Longleftrightarrow$ the multiplicity of f at a is greater than 1 .
2. f is non-singular at $a \Longleftrightarrow$ the multiplicity of f at a is 1.
3. Suppose $f(a) = b$. Draw little neighborhoods N_a and N_b about a and b in the domain and range respectively. You can restrict f to a map $f : N_a \longrightarrow N_b$. The big idea is that, the restricted function f "behaves like" the function $\beta_1 z + \cdots + \beta_n z^n$ that maps $0 \longrightarrow 0$.
4. Suppose the multiplicity of f at a is m. Then f "behaves like" $\beta_m z^m + \cdots + \beta_n z^n$. The smaller the neighborhoods, the more this last map is just a minor perturbation of the simple map $\beta_m z^m$, which is just like z^m. So locally all complex polynomials "behave like" z^m for some m .

7. Local analysis on the range—what happens above one point of the range

(a) Theorem: $f^{-1}(a)$ has n points $\Longleftrightarrow$ the equations $f(z) = a$ and $f'(z) = 0$ have no common roots. That is $\Longleftrightarrow f(z) = a \Longrightarrow f'(z) \neq 0$.

1. The proof is the product role. Suppose

$$f - a = c(z - r_1)\cdots(z - r_n)$$

Then

$$\begin{aligned} f' &= c\sum_{j=1}^{n}\left(\prod_{\substack{k=1 \\ k\neq j}}^{n}(z - r_k)\right) \\ f'(r_i) &= c\prod_{\substack{k=1 \\ k\neq i}}^{n}(r_i - r_k) \end{aligned}$$

The r_i are distinct if and only if $f'(r_i) \neq 0$ for all i.

(b) $f^{-1}(a)$ has n points $\Longleftrightarrow$ f is non-singular at every point of $f^{-1}(a)$

(c) Otherwise we say that f is *branched* above a.

(d) More generally, if $f^{-1}(a)$ has distinct points $r_1, \ldots, r_k$ with multiplicities $t_1, \ldots, t_k$, then $t_1 + \cdots + t_k = n$

8. Global analysis

(a) Suppose f is a polynomial of degree n. Since $\deg f' = n-1$, f has as most $n-1$ singular points and is branched above at most $n-1$ points.

(b) Example: $f(z) = 2z^3 - 9z^2 + 12z - 4$. Then $f'(z) = 6z^2 - 18z + 12 = 6\left(z^2 - 3z + 2\right)$. The singular points of f are $z = 1$ and $z = 2$; both have multiplicity 2. The branch points are $f(1) = 1$ and $f(2) =: 0$. For all values of $b \neq 1, 2$, $f^{-1}(b)$ consists of three points. At the special points $f^{-1}(1) = \left\{1, \frac{5}{2}\right\}$ and $f^{-1}(0) = \left\{2, \frac{1}{2}\right\}$. For both these sets, the sums of the multiplicities is 3.

Assignment due Sept. 1, 1999

1. Let $f(z) = z^4 - az^3 + bz^2 + cz - d$, where a, b, c, d are a sequence of digits selected from your Social Security number.

(a) Use software to graph your polynomial. How many real roots does it have? How many complex roots?

(b) Use software to find all the approximate roots r_i of your polynomial.

1. Calculate $\prod_i (z - r_i)$. How close is this to your original polynomial?

(c) Find all the (approximate) singular points and branch points for your polynomial.

(d) For each branch point b_j, find all the solutions to the equation $f(z) = b_j$. What is the multiplicity of each solution? (The singularities should add up to 4?)

Your answer will have a lot of data. Organize them into tables so they can be understood clearly.

2. Do the same problem for $f(z) = 6z^5 - 15z^4 + 10z^3$, but this time find exact answers for all parts.

3. Suppose $f(z)$ is a polynomial such that $f(3) = 5$ and $f(4) = -2$. Find a new polynomial $g(z) = \alpha f(z) + \beta$ such that $g(3) = 0$ and $g(4) = 1$.

4. Suppose $f(z)$ is a polynomial such that $f(3) = 0$ and $f(4) = 1$. Find a new polynomial $g(z) = f(\alpha z + \beta)$ such that $g(0) = 0$ and $g(1) = 1$.

5. Let f be a complex polynomial and $b \in \mathbb{C}$. Prove that the set $f^{-1}(b)$ consists of points $a_1, \ldots, a_t$ with multiplicities $m_1, \ldots, m_t$ if and only if

$$f(z) - b = c(z - a_1)^{m_1} \cdots (z - a_t)^{m_t}$$

(a) Special case: $f^{-1}(0)$ consists of points $a_1, \ldots, a_t$ with multiplicities $m_1, \ldots, m_t$ if and only if f can be factored into

$$f(z) = c(z - a_1)^{m_1} \cdots (z - a_t)^{m_t}$$

Chapter 3

Belyi Polynomials and Dessins

1. A *Belyi polynomial* is a complex polynomial ramified over at most 0 and 1
   (a) If $f(x)$ is a polynomial that is ramified over at most two points then, by a trivial change in the function (don't change degree or location, number and multiplicity of singular points) we can turn it into a Belyi polynomial
      1. If ramification points are a and b , replace $f(x)$ with $\dfrac{f(x)-a}{b-a}$
      2. We can also fix things so that one of the vertices above 0 is 0 and one of the vertices above 1 is 1.
   (b) Theorem (Simple version of Belyi's Theorem): If $f(x)$ is a Belyi polynomial then the coefficients of $f(x)$ are algebraic numbers.
      1. Examples: $x+3$, x^2-2x+1, $\dfrac{x^3-3x+2}{4}$, $\dfrac{x^3+3x+2i}{4i}$
      2. This is hard to prove
   (c) Associated with every Belyi polynomial is a *dessin d'enfant (children's drawing),* or simply a *dessin.*
      1. It is the pre-image of the interval $[0,1]$.
      2. Depending on the polynomial, it can be easy or difficult to find.
      3. Examples: x^2, x^3, x^n, $2x^3-3x^2$, $\dfrac{x^3-3x+2}{4}$, $\dfrac{x^3+3x+2i}{4i}$
      4. The dessin for a polynomial is always a tree—a graph (vertices connected by edges with no cycles), and the vertices can be alternately labeled 0 and 1.
      5. The degree of the polynomial is the number of edges
      6. The *valency* of a vertex is the number of edges that come out of it. The valency is the multiplicity of the polynomial at the vertex.
      7. We have a Mathematica function for drawing dessins: Poly to Dessin.nb
   (d) Conversely, associated with every dessin without cycles is a polynomial.
      1. This was Grothendieck's great discovery, so
         1. *...there is a profound identity between the combinatorics of finite maps on the one hand and the geometry of algebraic curves defined over number fields on the other.* This deep result, together with the algebraic-geometric interpretation of maps, opens the door into a new, unexplored world—within reach of all, who pass by without seeing it. he says in his *Esquisse d'un Programme* (1984)
      2. Alexandre Grothendieck is one of the twentieth century's most influential mathematicians.
         1. About 1970 he stopped publishing and exiled himself to a provincial university in France. After 1980 he decided he wanted to return to the principal French research institute (IHES–Institute des Hautes Études Scientifiques), and he wrote a 30 page research proposal known as "Esquisse d'un Programme" (published in Schneps, ed. *Geometric Galois*

Actions, Cambridge U..Press, Cambridge, 1997). In it he founded the subject we are studying.

2. When I get the material organized, I'll tell you more about him and his work. If you want, you can look up a sketch of his life in *Notices of the AMS,* March 1999, Vol. 46, No. 3, pp.332.

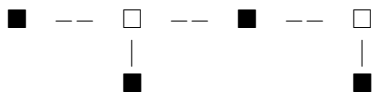
3. A dessin is a graph such that the vertices can be labeled with two symbols and vertices on the ends of any edge are differently labeled.
4. Finding the polynomial f is a job, and there is some ambiguity since the location of the vertices is not specified.
5. Here's a method for finding f that is easy to state but possibly hard to implement without some electronic assistance.
   1. Choose a vertex of maximum valency, and assume (1) it is at 0; and (2) it maps to 0. At this point the destination of all the other vertices are determined.
   2. Name any other vertices with valency > 1 that map to 0 as $p_2, p_3, \ldots, p_s$.
   3. If there are any vertices mapping to 1 with valency > 1, assume the first one is at 1 and the remaining ones are at $q_2, \ldots, q_t$.If no singular vertex maps to 1, then you can assume that $p_2 = 1$.
   4. Make a table of the singular vertices

vertex	0	p_2	$\cdots$	p_s	1	q_2	$\cdots$	q_t
valency	m_1	m_2	$\cdots$	m_s	n_1	n_2	$\cdots$	n_t

   Each $m_i > 1$ and $n_i > 1$. T
   5. The derivative of the desired Belyi polynomial will have the form

$$\frac{df}{dz} = c\, z^{m_1-1} (z-p_2)^{m_2-1} \cdots (z-p_s)^{m_s-1} (z-1)^{n_1-1} \cdots (z-q_t)^{n_t-1}$$

   Note that we are using only the singular nodes of the dessin. Nodes of valency or multiplicity 1 are not used in the calculation.
   6. The desired Belyi polynomial f will be the integral of df with zero constant term. The equations $f(p_2) = 0$, ..., $f(p_t) = 0$, $f(1) = 1$, $f(q_2) = 1$, ..., $f(q_t) = 1$ is a system of equations for the unknown values $c, p_2, \ldots, p_s, q_2, \ldots, q_t$..
6. **Example**: the dessin is



We label the vertices with valency > 1:

   1. The table is

vertex	0	p_2	1
valency	3	2	2

   Thus the derivative of the desired polynomial is:

$$f' = cz^2 (z-1)(z-p_2)$$

   Therefore, integrating and setting the constant of integration to 0:

$$\begin{aligned} f &= \int cz^2 (z-1)(z-p_2)\, dx \\ &= c\left(\frac{1}{5}z^5 + \frac{1}{4}(-1-p_2) z^4 + \frac{1}{3}p_2 z^3\right) \end{aligned}$$

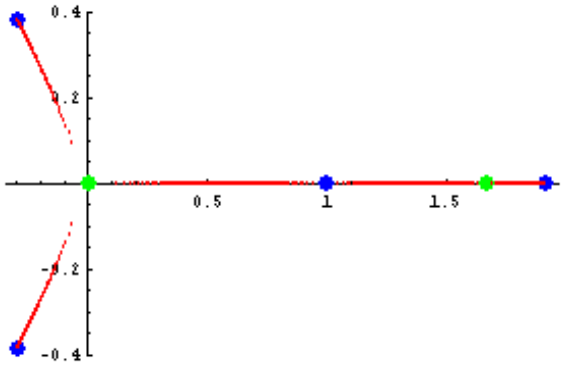
First write the equations at the singular points only and solve them:

$$\begin{aligned} f(p_2) &= c\left(\frac{1}{5}p_2^5 + \frac{1}{4}(-1-p_2)p_2^4 + \frac{1}{3}p_2 p_2^3\right) \\ &= -\frac{1}{20}p_2^5 + \frac{1}{12}p_2^4 = 0 \\ f(1) &= c\left(\frac{1}{5} + \frac{1}{4}(-1-p_2) + \frac{1}{3}p_2\right) \\ &= \frac{1}{60}c(-3+5p_2) = 1 \end{aligned}$$

Some of the solutions involve $p_2 = 0$, which is not useful for us since we know $p_2 \neq 0$. The only useful solution is $p_2 = \frac{5}{3}$, $c = \frac{45}{4}$,. Thus the desired Belyi polynomial is

$$f = \frac{9}{4}z^5 - \frac{15}{2}z^4 + \frac{25}{4}z^3$$

As a check, here's the dessin (drawn by Mathematica) for this polynomial



:

7. Mathematica examples: Dessin to Poly.nb
8. Schneps, in "Dessins d'Enfants", *The Grothendieck Theory of Dessins d'Enfants* (ed. Schneps) Cambridge U. Press, Cambridge, 1994, offers another approach that leads to simpler equations by using more sophisticated analysis.
   1. Alternately assign the vertices "plus" and "minus". Assign a vertex with most common valency to be "plus" (from which all other assignments follow), and assume that this vertex is located at 0.
   2. Make "valency lists" that list the *number of vertices of each valence,* $\{u_1, \ldots, u_s\}$ for the positive vertices, $\{v_1, \ldots, v_t\}$ for the negative vertices.
   3. For $u_i \neq 0$ and $v_i \neq 0$, construct polynomials

$$\begin{aligned} p_i &= z^{u_i} + c_{i,u_i-1}z^{u_i-1} + \cdots + c_{i,1}z + c_{i,0} \\ q_i &= z^{v_i} + d_{i,v_i-1}z^{v_i-1} + \cdots + d_{i,1}z + d_{i,0} \end{aligned}$$

   4. Let u_{i_0} be the largest u_i (i_0 not necessarily unique). Replace p_{i_0} with $p_{i_0} - c_{i_0 0}$. That is, erase the constant term of p_{i_0}
   5. Define $P = \prod p_i^i$ and $Q = \prod q_i^i$.
   6. Solve for c_{ij} and d_{ij} so that $P = Q + 1$.
   7. The resulting polynomial P, with the solutions replacing the literal coefficients d_{ij}, is the desired Belyi polynomial.;.
9. **Example:** For the dessin above, assuming the double point maps to 0, the u_i are $\{3, 1\}$ and the v_i are $\{0, 1, 1\}$. Thus

$$\begin{aligned} p_1 &= z^3 + p_{12}z^2 + p_{11}z + p_{10} \\ p_2 &= z + p_{20} \\ q_2 &= z + q_{20} \\ q_3 &= z + q_{30} \end{aligned}$$

Modify p_1 to $p_1 = z^3 + p_{12}z^2 + p_{11}z$ .Then

$$\begin{aligned} P &= p_2^2 p_3^3 \\ &= \left(z^3 + p_{12}z^2 + p_{11}z\right)(z + p_{20})^2 \\ &= z^5 + (2p_{20} + p_{12})\, z^4 \\ &\quad + \left(p_{20}^2 + 2p_{12}p_{20} + p_{11}\right) z^3 \\ &\quad + \left(p_{12}p_{20}^2 + 2p_{11}p_{20}\right) z^2 \\ &\quad + p_{11}zp_{20}^2 \end{aligned}$$

$$\begin{aligned} Q &= q_2^2 q_3^3 + 1 \\ &= (z + q_{20})^2 (z + q_{30})^3 + 1 \\ &= z^5 + (2q_{20} + 3q_{30})\, z^4 \\ &\quad + \left(q_{20}^2 + 6q_{20}q_{30} + 3q_{30}^2\right) z^3 \\ &\quad + \left(3q_{20}^2 q_{30} + 6q_{20}q_{30}^2 + q_{30}^3\right) z^2 \\ &\quad + \left(3q_{20}^2 q_{30}^2 + 2q_{20}q_{30}^3\right) z \\ &\quad + q_{20}^2 q_{30}^3 + 1 \end{aligned}$$

The equations to be solved are:

$$\begin{aligned} (2p_{20} + p_{12}) &= (2q_{20} + 3q_{30}) \\ \left(p_{20}^2 + 2p_{12}p_{20} + p_{11}\right) &= \left(q_{20}^2 + 6q_{20}q_{30} + 3q_{30}^2\right) \\ \left(p_{12}p_{20}^2 + 2p_{11}p_{20}\right) &= \left(3q_{20}^2 q_{30}^2 + 2q_{20}q_{30}^3\right) \\ p_{11}zp_{20}^2 &= \left(3q_{20}^2 q_{30}^2 + 2q_{20}q_{30}^3\right) \end{aligned}$$

10. Mathematica example: Schneps Tree

(e) A Belyi polynomial f is *clean* if and only if f has multiplicity 2 at every pre-image of 1.

1. That means $f - 1 = h^2$, where h is non-singular at its roots ($\deg h = n \Longrightarrow h$ has n roots)
2. So a clean Belyi polynomial has even degree

(f) A dessin is *clean* if and only if every 1 node has valency 2

1. So you can forget the 1-nodes and just connect the 0-nodes

(g) Any Belyi polynomial g can be turned into a clean Belyi polynomial f via $f = 4g\,(1 - g)$

1. Proof will be on homework
2. Note that $f - 1 = (2ig - i)^2$

Assignment Due September 8, 1999

1. Find the unique tree with one edge. Find its Belyi polynomial.
2. Find the unique tree with two edges. Find its Belyi polynomial
3. Find two trees with three edges (that's all there are). Find the corresponding Belyi polynomials.
4. Find all the trees with four edges and the Belyi polynomials. Use both methods and show they give equivalent results.
5. Referring to Schnep's method, show that all the following quantities are the same:

   (a) the sum of the positive valencies

   (b) the sum of the negative valencies

(c) $\sum iu_i$

(d) $\sum iv_i$

(e) the number of edges

(f) $\deg P$

6. Can you find an example of two different trees with the same valency lists? If so, Schnep's method, which just uses the valency lists, should have two different results for the two trees. Show that this is true for your example.

Chapter 4

Rational Functions and the Riemann Sphere

Rational Functions

1. A rational function (on $\mathbb{C}$) is a quotient of polynomials, which we will always take to be without common factors (*i.e.* without common roots).

$$\frac{x^2-1}{2x} \quad \frac{5x^3-3x^2+\pi x-4}{2x^4-2i}$$

   (a) $\{\text{polynomials}\} \subset \{\text{rational functions}\}$

2. If $f=\frac{p}{q}$is a rational function, then it is NOT a map $\mathbb{C} \longrightarrow \mathbb{C}$ because it is not defined at the roots of q.

   (a) Gauss' theorem also fails. The equation $\frac{x-1}{x}=1$ has no solutions. Rational functions are not onto.

3. In the nineteenth century, somebody (Riemann?) discovered that these irregularities could be eliminated if a point at infinity, denoted ∞, was added to the complex plane. The result—$\mathbb{C}$ with ∞—is called the *Riemann sphere* $\mathbb{P}^1_{\mathbb{C}}$ or just $\mathbb{P}$. In a moment we will see why the term "sphere" is used.

   (a) If $q(z)=0$ then $f(z)=\infty$

   (b) For a rational function $f=\frac{p}{q}$, define

$$f(\infty)=\lim_{z\longrightarrow\infty} f(z)$$

      1. If $\deg p>\deg q$ then $f(\infty)=\infty$
      2. If $\deg p<\deg q$ then $f(\infty)=0$
      3. If $\deg p=\deg q$ and $p=p_0+p_1z+\cdots+p_nz^n$ and $q=q_0+q_1z+\cdots+q_nz^n$ then $f(\infty)=\frac{p_n}{q_n}$
      4. In all cases, if $g(z)=f\left(\frac{1}{z}\right)$ (simplified to a rational function), then $f(\infty)=g(0)$

   (c) $\mathbb{P}^1_{\mathbb{C}}$ means one-dimensional projective space over $\mathbb{C}$. In the context of this course, which is more about algebraic geometry than traditional complex analysis, the chosen symbol is appropriate and widely used.

4. We need to topologize this situation, so that the Riemann sphere is a unified topological entity, not a plane plus a point floating somewhere off it.

(a) The trick is to map the complex plane to the sphere (draw picture) so that the plane is homeomorphic to the sphere with the north pole removed. The north pole then becomes the "point at infinity" on the Riemann sphere.

1. A neighborhood is all the points outside a neighborhood of 0.
2. The definitions I've given make rational functions into continuous maps $\mathbb{P} \longrightarrow \mathbb{P}$

5. We need to calculate the derivative of a rational function

(a) when the argument is ∞

(b) when the value is ∞

But the derivative isn't really defined in these cases. However, all we care about is whether or not the derivative is 0 (whether or not our function is singular at some point), and we can extend the concept of derivative to answer that question in a consistent way.

(a) To find if ∞ is a singular point of f, let $g(z) = f\left(\frac{1}{z}\right)$ and determine if 0 is a singular point of g

(b) If $f(a) = \infty$, to find if a is a singular point of f, determine if a is a singular point of $\frac{1}{f}$

(c) The other singular points are the solutions to $f'(z) = 0$.

1. Note that the solutions to $f'(z) = \infty$ are also singular, but they are the singular points found by considering the solutions to $f(z) = \infty$.

(d) Multiplicities are similarly defined.

1. The multiplicity of f at ∞ is the multiplicity of $f\left(\frac{1}{z}\right)$ at 0
2. If $f(a) = \infty$, then the multiplicity of f at a is the multiplicity of $\frac{1}{f}$ at a.
3. Otherwise the multiplicity of f at a is as before: the least integer $m > 0$ such that $f^{(m)}(a) \neq 0$

(e) Example: $f = \frac{z^2 - 1}{2z}$.

1. $f(0) = f(\infty) = \infty$
2. To find if 0 is a singular point, consider $g = \frac{1}{f} = \frac{2z}{z^2 - 1}$ and $g' = \frac{-2\left(z^2 + 1\right)}{\left(z^2 - 1\right)^2}$. We see that $g'(0) \neq 0$ so 0 is not a singular point of f.
3. to find out if ∞ is a singular point, consider $g = f\left(\frac{1}{z}\right) = \frac{\frac{1}{z^4} - 1}{\frac{2}{z^2}} = \frac{1 - z^4}{2z^2}$ .Then $g(0) = \infty$, so define $h = \frac{1}{g} = \frac{2z^2}{1 - z^4}$. Then $h'(0) = 0$ so g is singular at 0 and f is singular at ∞.
    1. Since $h''(0) \neq 0$, the multiplicity of h at 0 is the multiplicity of g at 0 is the multiplicity of f at ∞ is 2.

(f) The moral of the story:

1. to analyze a function f at ∞ in the domain, analyze $g(z) = f\left(\frac{1}{z}\right)$ at 0
2. to analyze a function f at a point a such that $f(a) = \infty$, analyze $g(z) = \frac{1}{f(z)}$ at a, which you can do since $g(a) = 0$.

6. Suppose $f = \frac{p}{q} : \mathbb{P} \longrightarrow \mathbb{P}$ is a non-constant rational function.

(a) f is onto. Proof:

1. $f(z) = a$ if $p(z) = aq(z)$. Since f is not constant, $p - aq$ is a non-constant polynomial and has a root.
2. $f(z) = \infty$ if $q(z) = 0$ or $\deg p > \deg q$. Since the function is not constant, either $\deg p > \deg q$ or else q is not constant and has a root..

(b) f will be $1-1$ if and only if $f = \dfrac{az+b}{cz+d}$ where $ad - bc \neq 0$. Proof: If $\deg p > 1$ (resp. $\deg q > 1$) then $f = 0$ (resp. $f = \infty$) has multiple solutions. So f is $1-1$ implies that f has the specified form. Conversely, if

$$\frac{az_1+b}{cz_1+d} = \frac{az_2+b}{cz_2+d}$$

then

$$(ad-bc)(z_2 - z_2) = 0$$

so $z_1 = z_2$

1. Such functions are called *fractional linear transformations*
2. The inverse is a fractional linear transformation:

$$\begin{aligned} w &= \frac{az+b}{cz+d} \\ z &= -\frac{dw-b}{cw-a} \end{aligned}$$

3. Given three distinct points $z_1, z_2, z_3 \in \mathbb{P}$ and three more (distinct) points $w_1, w_2, w_3 \in \mathbb{P}$, there is a unique fractional linear transformation mapping z_i to w_i.
   1. It suffices to show that there is a unique fractional linear transformation mapping w_1, w_2, w_3 to $0, 1, \infty$. And it is $L(z) = \left(\dfrac{w_2 - w_1}{w_2 - w_3}\right)\left(\dfrac{z - w_1}{z - w_3}\right)$
4. If f is a rational function and $L = \dfrac{az+b}{cz+d}$ is a fractional linear transformation, then the functions

$$\begin{aligned} g(z) &= (L \circ f)(z) = \frac{af(z)+b}{cf(z)+g} \\ h(z) &= (f \circ L)(z) = f\left(\frac{az+b}{cz+d}\right) \end{aligned}$$

have the same number of singular points, branch points, etc., as f. In particular, the singular points of f and g are the same, and the branch points of f and h are the same.
   1. Proof: let L be a fractional linear transformation. Then $(f \circ L)'(z) = 0$ if and only if $(L \circ f)'(z) = 0$ if and only if $f'(z) = 0$

7. Power series and Laurent series.

(a) Given a rational function $f = \dfrac{p}{q}$ and a point $a \in \mathbb{C}$, we can write

$$\begin{aligned} p &= p(a) + (z-a)^{m_p}\left(p_{m_p} + p_{m_p+1}(z-a) + \cdots + p_{m_p+r}(z-a)^r\right) \\ q &= q(a) + (z-a)^{m_q}\left(q_{m_q} + q_{m_q+1}(z-a) + \cdots + q_{m_q+s}(z-a)^s\right) \end{aligned}$$

where

$$\begin{aligned} m_p &= \text{multiplicity of } p \text{ at } a \\ m_q &= \text{multiplicity of } q \text{ at } a \\ \deg p &= r + m_p \\ \deg q &= s + m_q \\ p_{m_p} &\neq 0,\ q_{m_q} \neq 0 \end{aligned}$$

1. It might simplify matters to note that, since f is reduced, at least one of $p(a)$ and $q(a)$ is non-zero.

(b) The calculation of $f = \frac{p}{q}$ has three cases:

1. $p(a) \neq 0$ and $q(a) \neq 0$ then $f(a) = \frac{p(a)}{q(a)}$ and

$$\begin{aligned} f &= f(a) + (z-a)^t (f_t + f_{t+1}(z-a) + \cdots) \\ \text{if } m_p &\neq m_q \text{ then } t = \min\{m_p, m_q\} \text{ else } t \geq m_p \end{aligned}$$

2. if $p(a) = 0$ and $q(a) \neq 0$ then $f(a) = 0$ and

$$f = (z-a)^{m_p} \left(f_{m_p} + f_{m_p+1}(z-a) + \cdots\right)$$

3. if $p(a) \neq 0$ and $q(a) = 0$ then f has a pole at a and

$$f = (z-a)^{-m_q} \left(f_{m_q} + f_{m_q+1}(z-a) + \cdots\right)$$

(c) To do this analysis at $a = \infty$, do it for $g(z) = f\left(\frac{1}{z}\right)$ at $a = 0$.

(d) In our example above, at $a = 0$, $m_p = 2$ and $m_q = 1$.

$$\begin{aligned} f &= z^{-1}\left(-\frac{1}{2} + \frac{1}{2}z^2\right) \\ f\left(\frac{1}{z}\right) &= z^{-2}\left(\frac{1}{2} - \frac{1}{2}z^3\right) \end{aligned}$$

(e) Every rational function $f = \frac{p}{q} : \mathbb{P} \longrightarrow \mathbb{P}$ is onto, and the sum of the multiplicities at the preimages of any point is equal to $\max\{\deg p, \deg q\}$.

1. The quantity $\{\deg p, \deg q\}$ is the *degree* of f.
2. This generalizes the result that a fractional linear transformation is $1-1$.

8. Given a rational function, it's branch points are the images of its singular points. We say that the function is *ramified* over the branch points. The example above is ramified only over ∞.

(a) A Belyi rational function is a rational function ramified at most over $0, 1, \infty$.

1. A clean Belyi rational function has only double points over 1

1. If $\frac{p}{q}$ is a clean Belyi function, then $\frac{p}{q} - 1 = \frac{p-q}{q}$ has only double roots, so $p - q = r^2$ for some polynomial r.with distinct roots.

2. Given a Belyi rational function f, the function $4f(1-f)$ is a clean Belyi rational function.

9. What does the dessin of a clean Belyi rational function look like.

(a) The dessin is the pullback of $[0, 1]$, and every pullback of 1 is a double point, so we can focus on the pullbacks of 0 and the lines between them.

(b) The result will be a connected graph in $\mathbb{C}$, possibly with cycles. Every finite pullback of ∞ will be in a cycle.

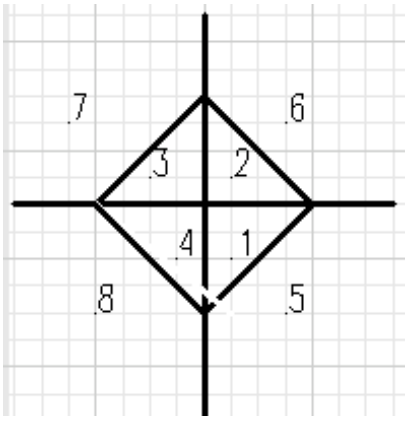
Triangulations

In this section we will use ideas from **algebraic topology** to prove that a dessin is connected and has other desirable properties.

1. Let $f : \mathbb{P} \longrightarrow \mathbb{P}$ be a rational function, and suppose $z \in \mathbb{P}$. Draw lines of two colors coming out of $f(z)$ and consider how these lines pull back to a neighborhood of z.
   (a) If f is non-singular at z, then two colored lines will come out of z
   (b) If f has multiplicity m at z, then $2m$ lines, alternately colored, will come out of z, because the behavior of f near z is like the behavior of z^m near 0.

2. A *triangulation* of the Riemann sphere is a graph drawn on the sphere such that every point is uniquely
   (a) a vertex
   (b) on an edge
   (c) in the interior of a face bounded by three edges
   (d) According to Euler's formula, if V is the number of vertices, E the number of edges and F the number of faces: $V - E + F = 2$

3. A triangulation can be represented on the plane. Here's a triangulation of the Riemann sphere with 8 triangles, 12 edges and 6 vertices, all with valency 4. Euler's formula is satisfied: $6 - 12 + 8 = 2$.



   You can think of this as a octahedron (regular solid with eight triangular faces).

4. For us, the basic triangulaton of the sphere has
   (a) three vertices at 0, 1, ∞, dividing the sphere into two triangles.
   (b) Three edges: the intervals $(0, 1)$, $(1, \infty)$, and $(-\infty, 0)$
   (c) Two faces corresponding to the upper and lower half-planes ($\mathrm{Im}(z) > 0$ and $\mathrm{Im}(z) < 0$).

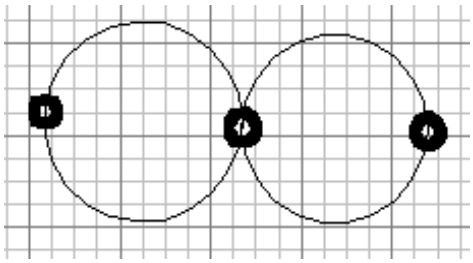
5. We want to study the pre-image of the basic triangulation under a Belyi rational map.
   (a) Let $f : \mathbb{P} \longrightarrow \mathbb{P}$ be a Belyi rational function. Consider the pre-image of the triangulation near a

6. The pre-image of the basic triangulation is a triangulation of $\mathbb{P}$
   (a) This depends on the fact that the only ramification points of the map come at the vertices of the triangulation.
   (b) Proof: use eight colors to color the basic triangle in the range of f three for the vertices, three for the edges and two for the faces. Color the points z on the domain of f so that the color of z is the color of $f(z)$.

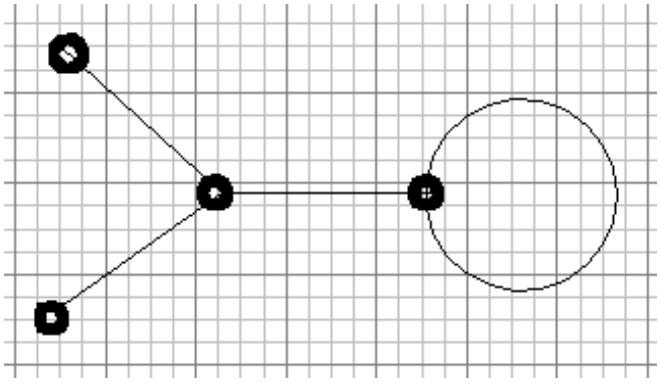
1. If $f(z)$ is not a vertex then f is not singular at z so there exists a small neighborhood U of z such that $f : U \longrightarrow f(U) \subset \mathbb{P}$ is a homeomorphism.
    1. Therefore: every point that maps to a face is surrounded by points mapping to the same face
    2. Every point mapping to an edge is part of a line mapping to the same edge. Moreover the two sides of the line are colored differently–one side maps to the upper half plane, the other side to the lower half plane.
2. If $f(z)$ is a vertex, then emanating from z will be pre-images of edges, colored alternately (so there are $2m$ lines coming out of z, where m is the multiplicity of f at z).
3. Start at a pre-image $z_{\infty,1}$ of ∞ and travel along a pre-image of $(\infty, 0)$ until you get to a pre-image $z_{0,1}$ of 0. Find the next line coming out of $z_{0,1}$ counterclockwise from the line you just traveled, and follow it to $z_{1,1}$, a preimage of 1. Find the next line coming out of $z_{1,1}$ counterclockwise from the line you just traveled, and follow it to $z_{\infty,2}$, a preimage of ∞. I claim $z_2 = z_\infty$, the point you started at.
   To prove this, continue selecting points $z_{0,2}, z_{1,2}, z_{\infty,3}, z_{0,3}, z_{1,3}, \ldots$ until you encounter $z_{i,j} = z_{i,k}$ for some i and $j < k$. Renumbering, you can assume you have points $z_{\infty,1}, \ldots, z_{1,m}, z_{\infty,m+1} = z_{\infty,1}$. If $m > 1$, draw a line from $z_{\infty,1}$to $z_{\infty,2}$: the image of this line under f will be a loop in $\mathbb{P}$ starting and ending at ∞. If you draw the line close to the edges $z_{\infty,1}, z_{0,1}, z_{1,1}, z_{\infty,2}$, you can assume that the loop is entirely in the interior of the triangle $\infty, 0, 1$. As you shrink the image loop, the pre-image line will change too, although it will still connect $z_{\infty,1}$ and $z_{\infty,2}$. But that is impossible, because when the image loop is small enough its primage must be a loop too.

7. Examples.

   (a) Octohedron is homework

   (b) 

$$-\frac{x^4\left(-\sqrt{2}+x\right)^2\left(\sqrt{2}+x\right)^2}{4\left(-1+x\right)^2\left(1+x\right)^2}$$

   (c) 

$$\left(655473\,(-1+x)^3x^3\left(\frac{-1911+\sqrt{21}\,\left(37-48\,I\,\sqrt{3}\right)^{3/2}-74\sqrt{21\,\left(37-48\,I\,\sqrt{3}\right)}}{3822}+x\right)\left(\frac{1}{42}\left(-21-\sqrt{21\,\left(37-48\,I\,\sqrt{3}\right)}\right)+x\right)\right)\Big/$$

$$\left(64\left(-9\,I\sqrt{7\,\left(37-48\,I\,\sqrt{3}\right)}-8\sqrt{21\,\left(37-48\,I\,\sqrt{3}\right)}\right)\left(\frac{-30576-5\sqrt{21}\,\left(37-48\,I\,\sqrt{3}\right)^{3/2}+825\sqrt{21\,\left(37-48\,I\,\sqrt{3}\right)}}{61152}+x\right)\right)$$

8. The edges of the triangulation form a connected graph: Given two vertices, draw a line from one to another. To travel on the graph from one to another, travel along the edges of the faces that your direct path crosses.

   (a) Any path from a preimage of 0 or 1 to a preimage of 0 or 1 that goes through a preimage of ∞ can be replaced by one that avoids all preimages of ∞, that is a path that only uses pre-images of the edge $(0,1)$.

   (b) **The dessin of the map f is the pre-image of $(0,1)$, which is therefore connected.**

9. Let f have degree n. Then the pre-image of the basic triangulation has $2n$ faces, $3n$ edges and $n+2$ vertices (by Euler).

10. Every dessin can be imbedded in a triangulation

    (a) The multiplicity of f at each vertex is the number of edges (counted locally) emanating from the vertex.

    (b) Every closed loop containing no interior vertices goes around exactly one finite point that goes to ∞.

        1. The multiplicity at the point is half the number of edges in the surrounding face.

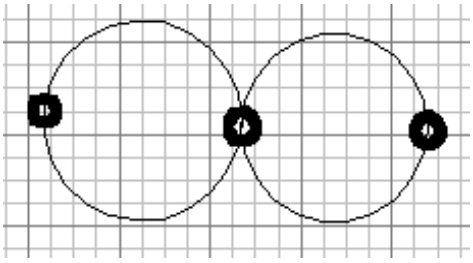
11. If f is a clean Belyi function and we eliminate all lines going through pre-images of 1, we still get a triangulation, and the lines going between pre-images of 0 form the clean dessin.—provided we count correctly.

    (a) The multiplicity at each vertex is the number of lines coming out of the vertex (counted locally)

    (b) Each closed loop in the graph (with no vertices in the interior) surrounds a point that goes to infinity with multiplicity equal to the number of edges.

Calculating Belyi Functions from Clean Dessins

1. This is my method rather than Schneps. I think it is simpler.
2. Suppose we have a clean dessin. We want to find the rational functions $\frac{p}{q}$ that gives the dessin. There may be more than one, corresponding
   (a) to different ways the dessin can be embedded in $\mathbb{C}$
   (b) to different dessins with the same number of vertices and the same multiplicities
3. Each vertex $v_1, \ldots, v_t$ corresonds to a zero of p with multiplicity $m_i$equal to the valence of the vertex, so $p = (x - v_1)^{m_t} \cdots (x - v_t)^{m_t}$
4. Each cycle in the dessin corresponds to a pole w_i of f or a zero of q with multiplicity n_i equal to the number of vertices (pre-images of 0) around the cycle, so $q = c(z - w_1)^{n_1} \cdots (z - w_s)^{n_s}$.
5. Since the dessin is clean $p - q$ is a square polynomial: $p - q = g^2$ were g is a polynomial of degree $1/2$ the degree of p (which will always have even degree because the dessin is clean). By identifying the coefficients of the polynomials $p - q$ and g^2 you find p and q and therefore f.
   (a) You can simplify by assuming that one of the v_i or w_i is 0 and another is 1. You can also assume $c \neq 0$.
6. Example:



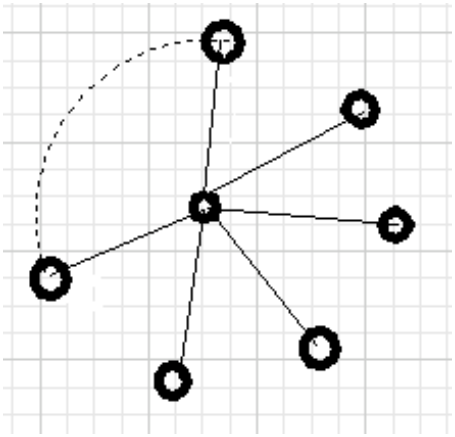
$$\begin{aligned} p &= x^4 (x-a)^2 (x-b)^2 \\ q &= c (x-1)^2 (x-d)^2 \\ g &= x^4 + g_3 x^3 + g_2 x^2 + g_1 x + g_0 \end{aligned}$$

See MySchneps.nb for solution

Some Standard Clean Dessins

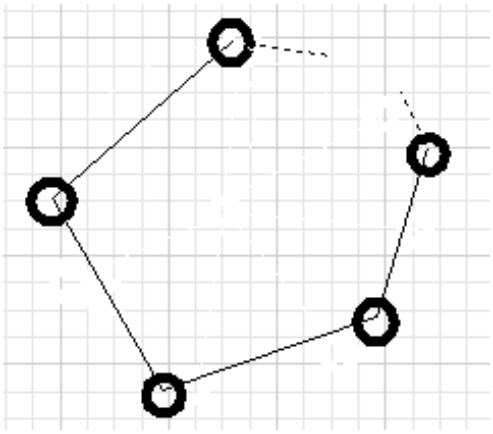
1. Star-shaped dessin—a tree

$$4x^n\left(1-x^n\right)$$



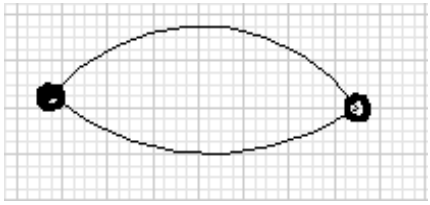
2. Polygon—a cycle

$$\frac{2-x^n-x^{-n}}{4}$$

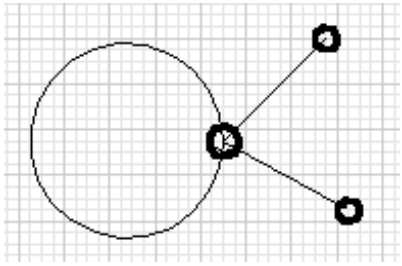


Assignment Due September 24

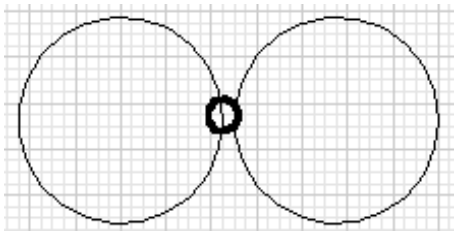
1. Show that the rational function $f(z)=\dfrac{z^2}{4(z-1)}$ is a Belyi function. Find the dessin and the triangulation for it. Is f a clean Belyi function?
2. Could the regular icosahedron be the triangulation for a rational Belyi function?
3. Find clean rational Belyi functions for the following clean dessins (only nodes above 0 are shown):

(a) 

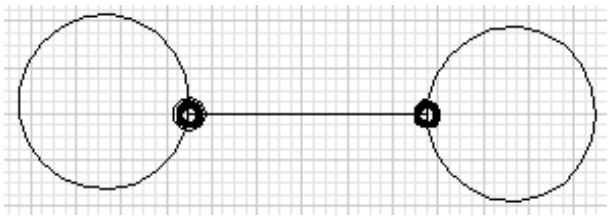
(b)



(c)



(d)



4. Warning: I don't know how hard this problem is. Explain why all dessins drawn in the plane have genus $g = 0$, where:

$$g = 1 - \frac{k_0 + \dot{k}_1 + k_\infty - N}{2}$$

If f is the map for the dessin then $k_i$is the number of distinct points in $f^{-1}(i)$, $i = 0, 1, \infty$, and N is the degree of f (the number of points in $f^{-1}(z)$ when z is not a branch point.

For partial credit, show that the dessins from problem 3 satisfy this rule.

Chapter 5

Covering Spaces and Covering Transformations

Rational Covering of the Thrice-Punctured Riemann Sphere

1. We are not quite ready to define the notion of *covering space* in general, but we can study an important special case. If $\pi : \mathbb{P} \longrightarrow \mathbb{P}$ is a rational Belyi function, consider

$$\pi : \mathbb{P} \tilde{} \ f^{-1}\{0,1,\infty\} \longrightarrow \mathbb{P} \tilde{} \ \{0,1,\infty\}$$

   (a) π is locally bijective

   (b) if $\deg \pi = n$ then $\pi^{-1}(p)$ consists of n points for every $\pi \in \mathbb{P} \tilde{} \ \{0,1,\infty\}$

   (c) $\mathbb{P} \tilde{} \ \{0,1,\infty\}$ is connected (it cannot be divided into disjoint open sets)—intuitively it consists of one piece

2. Whenever we have a covering space $\pi : Y \longrightarrow X$, we want to find the *group of covering transformations* $Aut_X(Y)$ consisting of analytic *automorphisms* $g : Y \longrightarrow Y$ such that the diagram

$$\begin{array}{ccc} Y & \xrightarrow{g} & Y \\ & {\scriptstyle \pi} \searrow \quad \swarrow {\scriptstyle \pi} & \\ & X & \end{array}$$

   commutes

   (a) I think any map that commutes with a Belyi map has to be an automorphism

   (b) First consider covering transformations individually

      1. Any such map interchanges points on fibres.
      2. It is not obvious, but we can prove that if two maps g_1 and g_2 agree at one point ($g_1(p) = g_2(p)$ for one point p then $g_1 = g_2$.
         1. Quick proof: the set of points on which $g_1 = g_2$ is open, closed and not empty. Since Y is connected, $g_1 = g_2$ on all of Y.
      3. Therefore if we pick a fiber $\pi^{-1}(x) = \{y_1, \ldots, y_n\}$, then $Aut_X(Y) \subset Perm(y_1, \ldots, y_n) = S_n$ and $\#Sym_X(Y) \leq n$.

   (c) Now consider the set of covering transformations

      1. It is not empty because it includes the identity map
      2. It is closed under composition.
      3. It is a group
         1. The identity map is the group identity
         2. Each covering transormation is bijective and its function inverse is its group inverse

3. Example 1: Belyi function: $\pi(z) = z^2$

   (a) If g is a covering transformation, then

$$\begin{aligned} \pi \circ g &= \pi \\ g(z)^2 &= z^2 \\ g(z) &= \pm z \end{aligned}$$

   (b) That is, $Aut_X(Y)$ is a group with two elements, so it is isomorphic to $\frac{\mathbb{Z}}{2\mathbb{Z}}$

4. Example 2: Belyi function $\pi(z) = z^n$

   (a) If g is a covering transformation, then

$$\begin{aligned} \pi \circ g &= \pi \\ g(z)^n &= z^n \\ g(z) &= \omega z \text{ where } \omega^n = 1 \end{aligned}$$

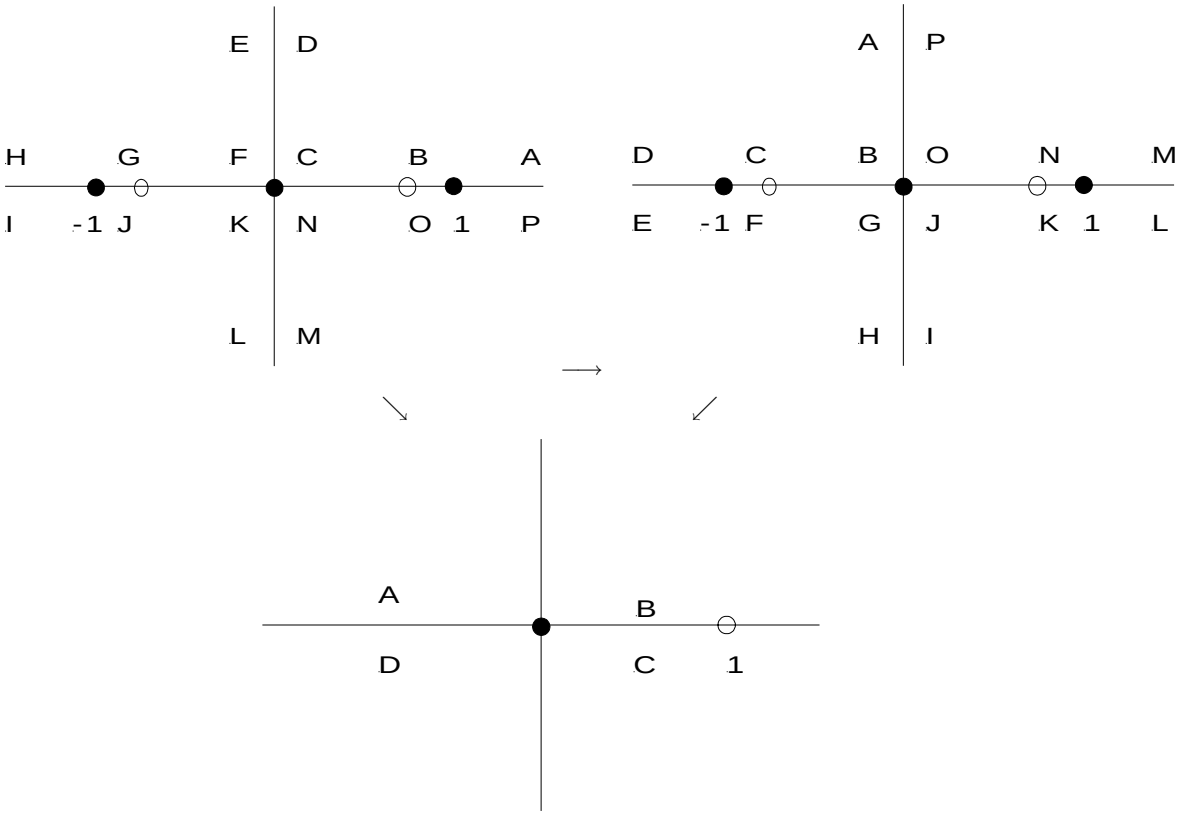
   (b) That is, $Aut_X(Y)$ is a group with n elements, so it is isomorphic to $\frac{\mathbb{Z}}{n\mathbb{Z}}$

5. Example 3: Belyi function $\pi(z) = 4z^2\left(1 - z^2\right)$, the function associated with the clean, star-shaped dessin with two arms

   (a) If g is a covering transformation, then (using the quadratic formula)

$$\begin{aligned} \pi \circ g &= \pi \\ 4g(z)^2\left(1 - g(z)^2\right) &= 4z^2\left(1 - z^2\right) \\ g(z) &= \pm z, \pm\sqrt{1 - z^2} \end{aligned}$$

   (b) That is, $Aut_X(Y)$ is a group with 4 elements is isomorphic to $\frac{\mathbb{Z}}{4\mathbb{Z}}$. The generator is $g(z) = \sqrt{1 - z^2}$, maps quadrants counter-clockwise, but with some complications.


E D
H G F C B A
I -1 J K N O 1 P
L M
A P
D C B O N M
E -1 F G J K 1 L
H I
A B
D C 1

6. Example 4: Belyi function $\pi(z) = 4z^n(1-z^n)$, the function associated with the clean, star-shaped dessin with n arms

   (a) If g is a covering transformation, then (using the quadratic formula)

$$\begin{aligned} \pi \circ g &= \pi \\ 4g(z)^n\left(1-g(z)^n\right) &= 4z^n(1-z^n) \\ g(z) &= \omega z,\ \omega(1-z^n)^{1/n} \text{ where } \omega^n = 1 \end{aligned}$$

   (b) That is, $Aut_X(Y)$ is a group with $2n$ elements is isomorphic to $\dfrac{\mathbb{Z}}{2n\mathbb{Z}}$. The generator is $g(z) = \left(1-z^2\right)^{1/n}$

7. Example 5: Belyi function $\pi(z) = \dfrac{2-z^2-z^{-2}}{4}$, the function associated with a four-sided polygon

   (a) If g is a covering transformation, then (knowing there are at most four automorphisms)

$$\begin{aligned} \pi \circ g &= \pi \\ \frac{2-g(z)^2-g(z)^{-2}}{4} &= \frac{2-z^2-z^{-2}}{4} \\ g(z)^2+g(z)^{-2} &= z^2+z^{-2} \\ g(z) &= \pm z,\ \pm\frac{1}{z} \end{aligned}$$

   (b) That is, $Aut_X(Y)$ is a group with 4 elements isomorphic to $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

8. Example 6: Belyi function $\pi(z) = \dfrac{2-z^n-z^{-n}}{4}$, the function associated with the $2n$-sided polygon.

   (a) If g is a covering transformation, then (knowing there are at most $2n$ automorphisms)

$$\begin{aligned} \pi \circ g &= \pi \\ \frac{2-g(z)^n-g(z)^{-n}}{4} &= \frac{2-z^n-z^{-n}}{4} \\ g(z)^n+g(z)^{-n} &= z^n+z^{-n} \\ g(z) &= \omega z,\ \frac{\omega}{z} \text{ where } \omega^n = 1 \end{aligned}$$

   (b) That is, $Aut_X(Y)$ is the dihedral group D_n with $2n$ elements (non_abelian for $n > 2$)

      1. The automorphisms $g(z) = \dfrac{\omega}{z}$ are of order 2.

9. There is another group associated with a Belyi cover $\pi : Y \longrightarrow X$, where $X = \mathbb{P}^{\tilde{}}\{0,1,\infty\}$? Use the dessins.

   (a) This group determines the Belyi cover

   (b) Before we embark on this calculation, we need to review *permulation groups* S_n.

   (c) S_n consists of *permulations* or *automorphisms* of $\{1,\ldots,n\}$ or of any other set of n distinct symbols.

   (d) The elements of S_n are products of disjoint *cycles* $(s_{i_1},\ldots,s_{i_t})$. where s_{i_j} are distinct and $1 \le s_{i_j} \le n$.

      1. We will read cycles left to right and products right to left.

$$(1,2,4)(2,3) = (2,3,4,1)$$

(e) If $\sigma_1, \ldots, \sigma_t \in S_n$, then the subgroup generated by the σ_i is all possible combinations of the σ_i and their inverses. (all possible *words*)

1. Since S_n is not abelian (commutative), one σ_i may appear at different places in a combination. You cannot reduce a word to $\sigma_1^{n_1} \cdots \sigma_t^{n_t}$.

(f) A subgroup $H \subset S_n$ is called *transitive* if for each i, $1 \leq i \leq n$, there exists $\sigma \in H$ such that $\sigma(1) = i$

1. A transitive subgroup contains elements mapping any i to any j.

10. Now we are ready to calculate the dessin group of a (clean) Belyi cover $\pi : Y \longrightarrow X$

(a) Draw the full dessin with the vertices above 0 and 1.

(b) Label the edges arbitrarily $1, \ldots, n$, where n is the degree of the map.

(c) For each vertex above 0, create a cycle consisting of the edge numbers going counter-clockwise. The product of these (disjoint) cycles is σ_0. Construct σ_1 by going around each vertex above 1 the same way. σ_1 will be a product of transpositions.

(d) We get a transitive subgroup of S_n generated by two elements σ_0 and σ_1.

1. Transitive because any edge can be moved to any other (using connectedness of dessin)

(e) We will see below that this dessin group determines the dessin.

11. Interpret σ_∞ where $\sigma_\infty \sigma_1 \sigma_0 = 1$ or $\sigma_\infty = \sigma_0^{-1} \sigma_1^{-1}$

(a) Go counter-clockwise round each cell, listing edges traversed $0 \longrightarrow 1$. Also go clockwise around outside of dessin, listing edges traversed $0 \longrightarrow 1$. That's σ_∞.

12. Every transitive subgroup of S_n generated by two permutations corresponds to a degree n Belyi cover of $\mathbb{P} - \{0, 1, \infty\}$

(a) Write the generators σ_0 and σ_1 as products of cycles.Include 1-cycles for every number $1..n$ not included in the cycles you already have For each cycle in σ_0 draw a black vertex with edges coming out numbers counterclockwise in the order the numbers appear in the cycle. In the same way create white vertices for the cycles in σ_1. Then each number $1..n$ occurs exactly once as an edge coming out of a black vertex and a white vertex. Connect the edges with the same numbers. That's the dessin associated to the subgroup and generators.

1. Question: if you change the generators but keep the subgroup, how can the dessin change?

(b) But it might not be a rational cover (a cover by an open subset of $\mathbb{P}$), so before we can investigate this relationship, we need to explain more general covers and algebraic curves and Riemann surfaces.

1. A dessin that can be drawn on $\mathbb{P}$ will have genus 0. All non-negative integral geni are possible. The same surface can carry many functions and many dessins, but all will have the same genus, which is the genus of the surface.
2. Torus has genus 1.
3. n-holed torus has genus n.
4. That's all there is, but the same surface can carry many different complex structures and so there are many non-equivalent tori for example.

(c) Nevertheless we can now state with some understanding Grothendieck's observation: (up to certain unstated equivalences) there is a 1-1 correspondence between

1. covers of $\mathbb{P}$ ramified at three points
2. dessins d'enfant
3. transitive subroups of S_n with two generators.
4. Many proofs have been published: one of the clearest is Burch "Non-congruence Subgroups" in Schneps (ed.), *The Grothendieck Theory of Dessins d"Enfants,* Cambridge University Press, Cambridge, 1994.

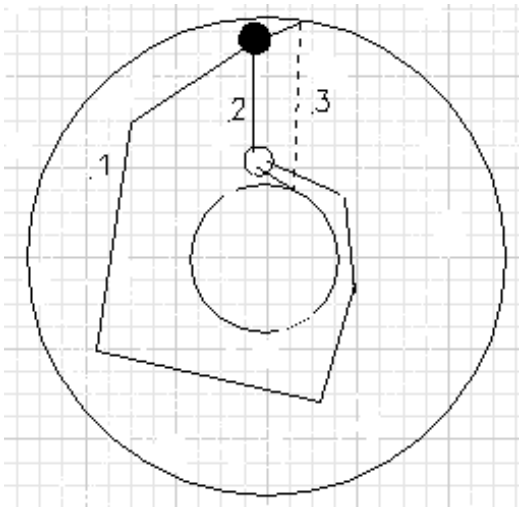
(d) Finding the cover from the group (or the dessin) can be very hard unless the genus is 0. Even then it can be tedious and difficult.

1. As we will see in the homework finding the genus of the cover from the group is easy.
2. Schneps said finding the cover was easy, but she was talking about the topological cover

(e) Let's do her example on the torus: 1 cell, 2 vertices, 3 edges:

$$\begin{aligned} g &= 1 - \frac{k_0 + \dot{k}_1 + k_\infty - N}{2} \\ &= 1 - \frac{1+1+1-3}{2} \\ &= 1 \end{aligned}$$

1. Here's the dessin, drawn on the torus

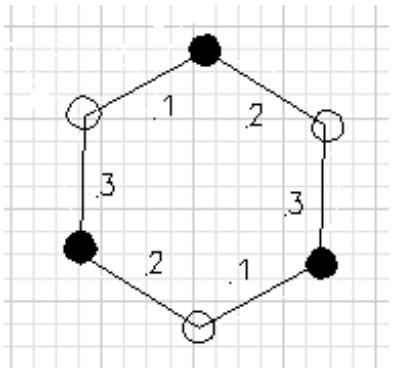


1. The dessin group is

$$\begin{aligned} \sigma_0 &= (1,2,3) \\ \sigma_1 &= (1,2,3) \\ \sigma_\infty &= \sigma_0^{-1}\sigma_1^{-1} \\ &= (1,3,2)\,(1,3,2) \\ &= (1,2,3) \end{aligned}$$

2. The dessin cuts the torus into a single cell with edges

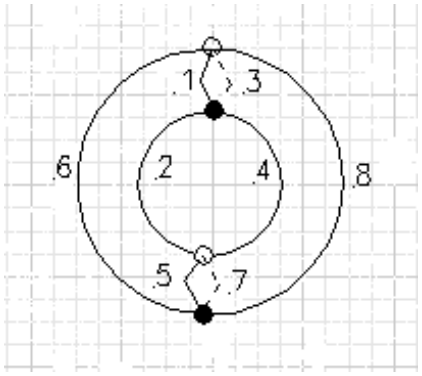
$$1,3,2,1,3,2$$



3. This can be folded up into a torus.

(f) Another example on the torus: 4 vertices, 8 edges, 4 cells

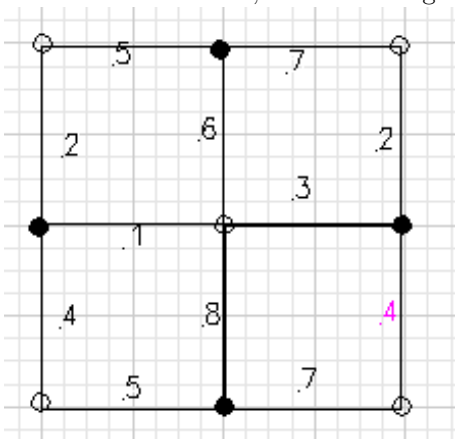
$$\begin{aligned} g &= 1 - \frac{2+2+4-8}{2} \\ &= 1 \end{aligned}$$



1. 8-fold covering of $\mathbb{P}$
2. The dessin group is:

$$\begin{aligned} \sigma_0 &= (1,2,3,4)\,(5,6,7,8) \\ \sigma_1 &= (1,8,3,6)\,(2,5,4,7) \\ \sigma_\infty &= \sigma_0^{-1}\sigma_1^{-1} \\ &= (4,3,2,1)\,(8,7,6,5)\,(6,3,8,1)\,(7,4,5,2) \\ &= (1,5)\,(2,6)\,(3,7)\,(4,8) \end{aligned}$$

3. So there are four cells, each a rectangle



4. These can be assembled into a torus
5. Still have no analytic Belyi function

(g) Try a more analytical example: $x^3 + y^3 = 1$ in $\mathbb{C}^2$

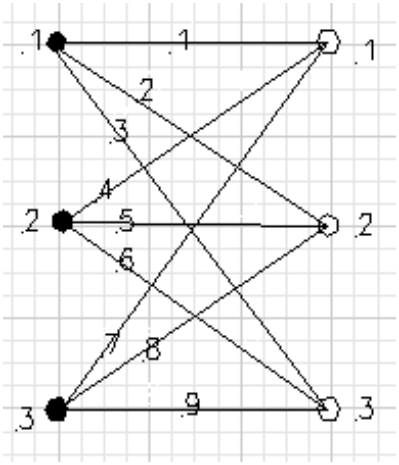
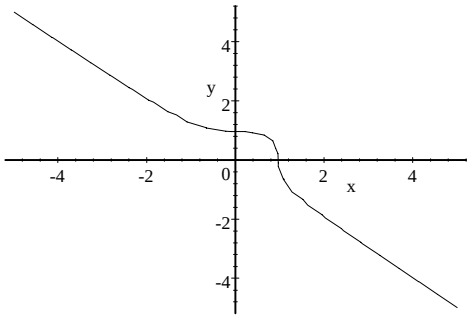


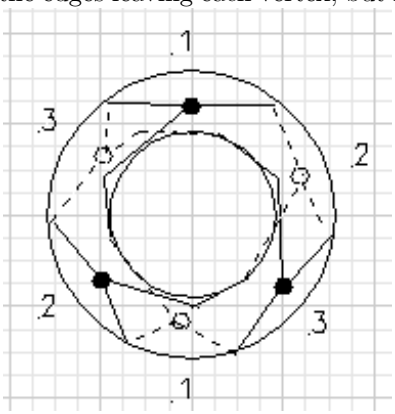
Figure 5.1:



1.
2. This is a *surface* C, in fact a Riemann surface with complex-valued polynomial functions, the restrictions of the polynomials functions of two variables mapping $\mathbb{C}^2 \longrightarrow \mathbb{C}$
    1. It is called C because it is a complex curve.
3. Unfortunately the whole Riemann surface for this equation includes three points "at infinity" which are not in $\mathbb{C}^2$. To describe them better requires using projective space, a compact extension of the affine space $\mathbb{C}^2$ like $\mathbb{P}$ is a compact extension of $\mathbb{C}$.
4. Let ω be a primitive cube root of 1. On the surface is the function x^3 which has singular points at $\left(0, \omega^i\right)$ above 0, $\left(\omega^i, 0\right)$ above 1, and three points above infinity that are off the graph anyway.
    1. Here is an argument suggesting that these are the singular points. The equation $x^3 = a$ has, in general, 9 solutions on our surface so the covering is degree 9. The only equations that have fewer than 9 solutions are $x^3 = 0$ and $x^3 = 1$ (and $x^3 = \infty$, but handling that equation carefully requires more theory) so the singular points must be among these solutions. In fact they are all solutions.
5. The dessin is all 9 lines connecting the three points above 0 to the three points above 1. This is the only possibility.
    1. This cannot be a real picture of the dessin, because the edges cross.
    2. The genus is:

$$\begin{aligned} g &= 1 - \frac{k_0 + k_1 + k_\infty - d}{2} \\ &= 1 - \frac{3+3+3-9}{2} \\ &= 1 \end{aligned}$$

3. I'm not entirely sure how to calculate the dessin group because I'm not sure how to order the edges leaving each vertex, but I have a candidate dessin for this function on the torus.

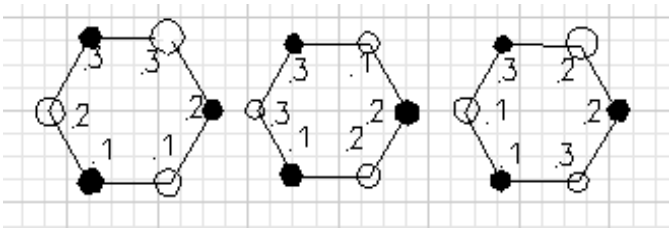


6. Calculate the dessin group.For $1 \leq i, j \leq 3$, number the edges from 0_i to 1_j as $3i + j - 3$. Then the dessin group can be calculated:

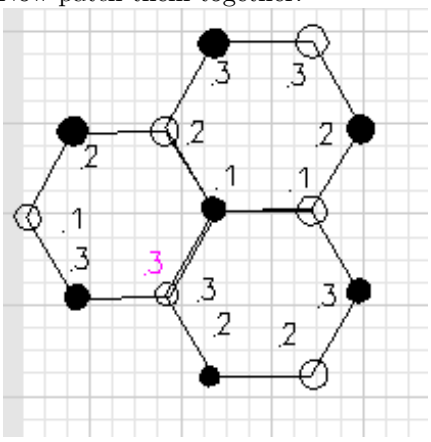
$$\begin{aligned}
\sigma_0 &= (1,2,3)\,(4,5,6)\,(7,8,9) \\
\sigma_1 &= (1,7,4)\,(2,8,5)\,(3,9,6) \\
\sigma_\infty &= \sigma_0^{-1}\sigma_1^{-1} \\
&= (3,2,1)\,(6,5,4)\,(9,8,7)\,(1,4,7)\,(2,5,8)\,(3,6,9) \\
&= (1,6,8)\,(2,4,9)\,(3,5,7)
\end{aligned}$$

1. There are three cells around points above ∞ as stated above.
2. The surface can be reconstructed from the three six-sided cells going around preimages of ∞, whose sides, going counter-clockwise, are

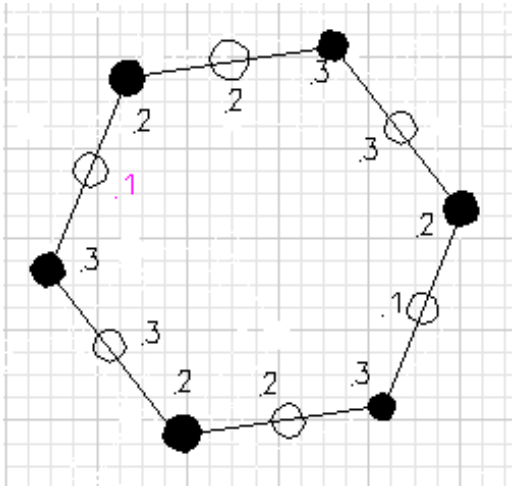
$$\begin{aligned}
(1,6,8) &= b1\ w1\ b2\ w3\ b3\ w2 \\
(2,4,9) &= b1\ w2\ b2\ w1\ b3\ w3 \\
(3,5,7) &= b1\ w3\ b2\ w2\ b3\ w1
\end{aligned}$$



Now patch them together.



Simplify



Assemble into a torus.like Schnep's first example.

Homework Due Monday, October 4, 1999

1. Find the groups of covering transformations for the covers associated with dessins (3b) and (3c) of the previous homework.

2. Find the permutations σ_0, σ_1 and σ_∞ for each of the dessins in problem 3 of the previous assignment. Remember to insert the white vertices first.

3. Draw the dessin associated with the generators $\sigma_0 = (1,2,3)\,(4,5,6)\,(7)\,(8)$ and $\sigma_1 = (1,2)\,(3,4)\,(5,7)\,(6,8)$. Using the genus formula from the previous homework, what is the genus of this dessin?

4. For $\sigma_0 = (1,8,2,5)\,(7,3,6,4)$ and $\sigma_1 = (1,2)\,(3,4)\,(5,6)\,(7,8)$

   (a) Find σ_∞

   (b) Explain why (referring to the genus formula)

      1. k_0 is the number of cycles in σ_0
      2. k_1 is the number of cycles in σ_1
      3. $k_\infty$is the number of cycles in σ_∞
      4. N is the number of distinct values listed being permuted by σ_0 and σ_1 (the smallest N such that $\sigma_0, \sigma_1 \in S_N$).

   (c) Calculate the genus of the dessin associated with this group.

Chapter 6

Galois Theory

Fields

1. A *field* is a set K with two operations: $+$ (addition) and $\cdot$ (multiplication—and the dot is often suppressed) satisfying
   (a) associativity of $+$: $\forall a, b, c \in K, (a + b) + c = a + (b + c)$
   (b) existence of $0 : \exists 0 \in K, \forall a \in K, 0 + a = a + 0 = a$
      1. Theorem: in any system satisfying these two axioms, 0 is unique.
   (c) existence of negatives: $\forall a \in K\ \exists b \in K\ a + b = 0$.
      1. Theorem: in any system satisfying these three axioms, b is uniquely determined by a and is denoted $-a$
      2. With these axioms alone, K is a group with the operation $+$
   (d) commutivity of $+ : \forall a, b \in K, a + b = b + a$
      1. With these axioms alone, K is an abelian group with the operation $+$
   (e) associativity of multiplication: $\forall a, b, c \in K, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
   (f) distributivity of multiplication over addition: $\forall a, b, c \in K, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$
      1. Now K is a ring.
   (g) existence of 1: $\exists 1 \in K, 1 \neq 0, \forall a \in K, a \cdot 1 = 1 \cdot a = a$
      1. Theorem: 1 is unique. Now K is a ring with identity
   (h) commutivity of multiplication: $\forall a, b \in K,\ a \cdot b = b \cdot a$
      1. with all axioms except (g), K is a commutative ring. Will all axioms K is a commutative ring with identity
      2. **Throughout these notes, "ring" means communtative ring with identity.**
   (i) multiplicative inverses: $\forall a \in K, a \neq 0, \exists b \in K, a \cdot b = 1$
      1. Theorem: in any system satisfying these axioms, b is uniquely determined by a and is denoted a^{-1}
      2. A system satisfying all these axioms is a *field.* If axiom (g) is omitted we have a skew-field.
2. Every field, considered with $+$ alone, is an abelian group. If K is a field then $K - \{0\}$ with the operation $\cdot$ is an abelian group.
3. If R is a ring and $a, b \in R$ satisfy $a, b \neq 0$ and $a \cdot b = 0$ then we say that a and b are *zero divisors.* A ring without zero divisors is called an *integral domain.*
   (a) Examples of integral domains: any field, $\mathbb{Z}$
4. Examples of fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$
5. If R is an integral domain, the quotient field of R is a field.

Polynomial and Power Series Rings

Throughout this section, R is an integral domain and K is a field

1. The *power series ring* $R[[t]]$ is the set of infinite sequences $(a_0, a_1, ...) = a_0 + a_1 t + a_2 t^2 + ..., a_i \in R$
   (a) rules for $+, \cdot$
   (b) integral domain
   (c) $u \in R[[t]]$ is a *unit* if and only if a_0 is a unit.
      1. $u \in K[[t]]$ is a unit if and only if $a_0 \neq 0$.
   (d) *order* of a non-zero element f is order of first non-zero coefficient, $ord_t(f)$
      1. $ord(f+g) \geq \min(ord(f), ord(g))$
      2. $ord(fg) = ord(f) + ord(g)$
   (e) In $K[[t]]$
      1. $ord(u) = 0 \iff u$ is a unit.
      2. every element is $f = t^n u$ for some unit u where $n = ord_t(f)$
      3. $K[[t]]$ is a PID and every ideal has a generator of the form t^n, so the only non-zero ideals are $I_n = \{f : ord_t f \geq n\}$
         1. Proof. Let I be an ideal. Choose $f \in I$ with minimal ord. Then $f = t^n u$ and u is a unit, so we can take t^n to be an element of minimal ord. Then t^n divides all elements of I
   (f) $K((t))$ is a field, quotient field of $K[[t]]$, Laurent series or meromorphic functions.

2. The *polynomial ring* $R[t]$ is the subring of eventually 0 series.
   (a) also an integral domain
   (b) degree of a non-zero polynomial is order of highest non-zero term, $\deg_t(f)$
      1. $\deg(f+g) \leq \min(\deg(f), \deg(g))$
      2. $\deg(fg) = \deg(f) + \deg(g)$
      3. f is a unit if and only if $\deg f = 0$ and a_0 is a unit of R.
   (c) A *monic* polynomial is one whose highest order coefficient is 1.

3. Special case: $K[t]$
   (a) Quotient field is $K(t)$, the field of rational functions over K
   (b) Division algorithm for $K[t]$: if $f, g \in K[t]$ and $g \neq 0$ then either $g \mid f$ or $f = gq + r$ where $\deg r < \deg g$
      1. Proof: by induction.on degree f. If $f = 0$ then $g \mid f$. If $\deg f < \deg g$ take $q = 0$, $r = f$. Otherwise let $f = ax^n + l.o.$ and $g = bx^m + l.o.$, where $a, b \neq 0$ and $n = \deg f$ and $m = \deg g$. Thus $m \leq n$ and if $h = f - (ax^{n-m}/b)g$, then either $h = 0$ and $g \mid f$ or $\deg h < \deg f$. In the second case, by induction, either $g \mid h$ or $h = q_1 g + r$ where $\deg r_1 < \deg g$. In the first case $g \mid f$, and in the second case $f = (ax^{n-m}/b + q_1)g + r$. QED
      2. The key to the proof is the ability to divide by the coefficient b, which is where the hypothesis "K is a field" is used.
   (c) $K[t]$ is a PID
      1. Proof: It suffices to show that non-zero ideals are principal. Let I be a non-zero ideal and choose a non-zero element $g \in I$ with minimal degree. Clearly $(g) \subset I$. I claim $I \subset (g)$, which I will prove by showing that every element of I is divisibly by g. Let $f \in I$. If g does not divide f then $f = gq + r$ for some non-zero polynomial r with $\deg r < \deg g$. But then $r \in I$ because $f, g \in I$, which contradicts the assumption that $\deg g$ is minimal for all the non-zero elements of I.

2. Every ideal in $K[t]$ has a unique monic generator, because if two monic polynomials divide each other they must be equal.

(d) A polynomial $f \in K[t]$ is *irreducible* if and only if it cannot be divided into factors of positive degree (non-unit factors).

1. $\deg f = 1 \Longrightarrow f$ is irreducible
2. Two polynomials $f, g \in K[t]$ are said to be *associates* if $f = ug$ for some non-zero constant u. An equivalent condition is $f \mid g$ and $g \mid f$.
3. f is irreducible iff (f) is a *prime* ideal.
    1. Proof: if f is irreducible and $gh \in (f)$ then we must show that $g \in (f)$ or $h \in (f)$. Let $gh = cf$ and assume $g \notin (f)$. We must show $h \in (f)$. Consider the ideal $(f, g) = (k)$ for some polynomial k. Since $(f, g) = (k) \supsetneq (f)$, $k \mid f$ but $f \nmid k$. Since f is irreducible, k is a unit. Moreover $k = af + bg$ for some polynomials a and b. so $1 = k^{-1}af + k^{-1}bg$. Thus $h = k^{-1}afh + k^{-1}bgh = k^{-1}(ah + bc) f \in (f)$..
    Conversely, if (f) is prime and $f = gh$, we must show that g or h is a unit. Since (f) is prime, either $g \in (f)$ or $h \in (f)$. In either case the other factor must have degree 0, or be a unit.
4. Every non-zero polynomial in $K[t]$ is the product of irreducible polynomials which are unique up to order and constant factors. That is, if $f_i, g_j \in K[t]$ are irreducible polynomials, and if $\prod_{i=1}^{n} f_i = \prod_{j=1}^{m} g_j$, then $n = m$ and the sets $\{f_i\}$ and $\{g_j\}$ can be matched up into pairs of associates.
    1. Existence of product: Let $f \in K[t]$ and proceed by induction on $\deg f$. If $\deg f = 0$ then f is a constant. Otherwise either f is irreducible or the product of factors of smaller degree. By induction the factors are products of irreducible polynomials.
    2. Uniquess: suppose $f_i, g_j \in K[t]$ are irreducible polynomials such that $\prod f_i = \prod g_j$. We can divide out associated factors and assume no f_i is associated to any g_j. If both products are empty, the result holds. Otherwise at least one product must be non-empty, in which case both are. But since $\prod f_i \in (f_1)$, we have $\prod g_j \in (f_1)$, a prime ideal. Therefore $g_j \in (f_1)$ for some j. Thus $f_1 \mid g_j$. But f_1 and g_j are both irreducible, so they must be associates, contradicting the removal of all associated pairs from the products.

(e) Polynomials over $\mathbb{Q}$ and $\mathbb{Z}$

1. A monic polynomial with integer coefficients factors into non-unit monic factors in $\mathbb{Q}[t]$ if and only if it factors into non-unit monic factors in $\mathbb{Z}[t]$ ("non-unit" excludes the dumb factorization $f = 1 \cdot f$.)
2. Proof: If f factors in $\mathbb{Z}[t]$ then the same factors work in $\mathbb{Q}[t]$. Conversely, suppose $f = gh$, where g, h are monic polynomials in $\mathbb{Q}[t]$. Multiplying by some integer n, we can obtain $nf = g'h'$, where g', h' are polynomials in $\mathbb{Z}[t]$. We will show that every prime divisor of n divides all the coefficients of either g' or h'. By removing such primes one at a time from either g' or h', we will have factored f into a product of polynomials from $\mathbb{Z}[t]$, which must be monic since their product is monic.
   Let p be a prime divisor of n, and write $g = \sum a_i t^i$ and $h = \sum b_i t^i$. Then p divides every coefficient of gh, and the coefficients are:

$$c_r = \sum_{i=\max(0, r-\deg h)}^{\min\{r, \deg g\}} a_i b_j$$

   $0 \leq r \leq \deg g + \deg h$. If the desired result is false, then there is a minimal $i, j \geq 0$ such that $p \nmid a_i$ and $p \nmid b_j$. Consider the coefficient

$$\begin{aligned} c_{i+j} &= a_i b_j + \text{terms with lower } a's \text{ or lower } b's \\ &= a_i b_j + \text{terms divisible by } p \end{aligned}$$

   Since c_{i+j} is divisible by p, either a_i or b_j is divisible by p, contradicting our assumption and proving the theorem.

3. Eisenstein's criterion: Let $f = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$. If there is a prime p such that $p \nmid a_n$, $p \mid a_i$, $0 \leq i < n$ and $p^2 \nmid a_0$ then f cannot be factored into lower-degree polynomials.
    1. Proof: Suppose $f = gh$. Since the leading coefficient of f is not divisible by p, the leading coefficients of g and h are not divisible by p. Reduce everything modulo p, so we have polynomials $\bar{f} = \bar{g}\bar{h} \in \frac{\mathbb{Z}}{(p)}[t]$. But $\bar{f} = \alpha t^n$ so $\bar{g} = \beta t^r$ and $\bar{h} = \gamma t^{n-r}$ where $\alpha, \beta, \gamma \in \left(\frac{\mathbb{Z}}{(p)}\right)^*$ and $\alpha = \beta\gamma$. Therefore all coefficients but the first in g and h are zero modulo p, or are divisible by p. Therefore the constant term of $f = gh$ is divisible by p^2, contradicting our assumption.

(f) Roots of polynomials

1. Let's do this one right. Suppose $k \subset K$ are fields and $f \in k[t]$. (Then $f \in K[t]$, because $k[t] \subset K[t]$.) A "point" $a \in K$ is a *zero* or *root* of f if and only if $f(a) = 0$.
2. a is a root of f if and only if $t - a$ divides f—in the ring $K[t]$. The coefficients of the other factor will be in K, not necessarily in k.
3. The multiplicity of a root is the number of times $t - a$ divides the polynomial.
4. Over any field $K \supset k$, we can factor a monic polynomial $f = (\prod t - a_i)^{m_i}) f_1(t)$
    1. If you increase K, all the linear factors are retained and others may appear from f_1.
5. The number of roots—even the sum of the multiplicities—is bounded by $\deg f$

(g) Polynomials of several variables

1. If R is a ring, then $R[t_1]$ is the ring of polynomials (in t_1) over R, and $R[t_1][t_2]$ is the ring of polynomials (in t_2) over the ring $R[t_1]$, etc.
2. $R[t_1, \ldots, t_n] = R[t_1][t_2] \cdots [t_n]$
3. A *monomial* in $R[t_1, \ldots, t_n]$ is an expression of the form $r\, t_1^{\mu_1} \cdots t_n^{\mu_n}$; its degree is $\mu_1 + \cdots + \mu_n$.
4. A polynomial is a unique sum of monomials. The degree of a polynomial $f \in R[t_1, \ldots, t_n]$ is the maximum degree of its monomials.
    1. A polynomial is *homogeneous* if all of its monomials have the same degree.
5. A useful generalization: if the variables t_i are assigned degress m_i, then $\deg t_1^{\mu_1} \cdots t_n^{\mu_n} = \mu_1 m_1 + \cdots + \mu_n m_n$
6. You can also define a power series ring $R[[t_1, \ldots, t_n]]$.

(h) Finitely generated subrings

1. Suppose $R \subset S$ are integral domains and $s_1, \ldots, s_n \in S$. Then $R[s_1, \ldots, s_n] \subset S$ is the *R-algebra generated by $s_1, \ldots, s_n$ in S.*, the smallest subring of S containing R and $s_1, \ldots, s_n$, the set of all polynomial expressions in s_i with coefficients from R.
2. We say that $s_1, \ldots, s_t$ are *algebraically independent* or *transcendental* over R is every non-trivial combination of the s_i is non-zero. (The natural map $R[t_1, \ldots, t_n] \longrightarrow R[s_1, \ldots, s_n]$ is an isomorphism.)

(i) Symmetric polynomials

1. A polynomial $f \in R[a_1, \ldots, a_n]$ is *symmetric* if and only if f is unchanged when the variables are permuted.
    1. The set of symmetric polynomials forms a subring of $R[a_1, \ldots, a_n]$
2. Consider the expression $f = (t + a_1) \cdots (t + a_n)$.
    1. If $a_i \in R$ then $f \in R[t]$, but instead write $f = \sum_{i=0}^{n} s_i(a_1, \ldots, a_n)\, t^{n-i}$.
    2. $s_i \in \mathbb{Z}[a_1, \ldots, a_n]$ is a symmetric polynomial, $0 \leq i \leq n$
    3. We call s_i the *i^{th} symmetric polynomial.*
    4. s_i is homogeneous and $\deg s_i = i$
    5. $s_0 = 1$, $s_1 = a_1 + \cdots + a_n$, $s_n = a_1 \cdots a_n$.

3. Obviously $R[s_1, \ldots, s_n] \subset$subring of symmetric polynomials $\subset R[a_1, \ldots, a_n]$. In fact the s_i are algebraically independent and $R[s_1, \ldots, s_n]$ is the subring of .symmetric polynomials. Moreover, every homogeneous symmetric polynomial in $R[a_1, \ldots, a_n]$ is a linear combination of monomials of the same degree in the s_i., so every symmetric polynomial is polynomial of the same degree in the s_i (assuming $\deg s_i = i$).
    1. Example: in $R[a_1, a_2, a_3]$, $a_1^2 + a_2^2 + a_3^2 = s_1^2 - 2s_2$

Homework Due Monday, Oct. 11

1. Consider the Riemann surface X defined by the equations $x^2+y^2 = 1$ in $\mathbb{C}^2$. There is a map $f : X \longrightarrow \mathbb{C}$ given by $f(x, y) = x^2$. Assume that you can add two points at infinity to X resulting in a compact Riemann surface $\bar{X}$. By mapping these points to ∞ in $\mathbb{P}$, you can extend our map to $f : \bar{X} \longrightarrow \mathbb{P}$.
    (a) Show that this map has degree 4.
    (b) Show that the only fibers with fewer than four points lie above $0, 1, \infty$, so f is a Belyi function.
    (c) Draw the dessin for f.
    (d) Calculate the genus of $\bar{X}$.
    (e) Since $\bar{X}$ has genus 0, it is "birationally equivalent" to $\mathbb{P}$. Can you find an algebraic map (a function using just addition, subtraction, multiplication and division and complex constants) from X to $\mathbb{C}$ that is $1-1$ and defined almost everywhere (Hint: find a map from the circle to the line. This is the real-number version of what you are trying to do for all complex points.)
2. Stewart, Chapter 2 (2, 6, 7, 9, 13)

Field Extensions

1. We "know" that every polynomial (with integer coefficients) has a root in the complex numbers $\mathbb{C}$.
    (a) In fact, every polynomial with complex coefficients has a complete factorization into linear factors over $\mathbb{C}$
    (b) This observation leads to a question. (In mathematics, theorem usually spawn questions as much as they answer them): given a polynomial with coefficients in some field, what is the smallest field containing the roots
        1. Important special cases include coefficients in $\mathbb{Q}$, in a finite field.
        2. Finite fields are important because answers to questions there are really approximate answers to Diophantine questions (questions about the integers).
    (c) Galois theory studies the roots of polynomials and the fields containing them. In particular, Galois theory studies the "symmetries of the roots", the question about when permutations of the roots are possible while preserving some property.
2. A *field extension* is a field L and a subfield $K \subset L$.
    (a) More abstractly, a field extension is a homomorphism $\iota : K \longrightarrow L$, which is necessarily $1-1$.
    (b) e.g. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$, $\mathbb{Q} \subset \mathbb{Q}(i)$, $K \subset K(t) \subset K((t))$. $K \subset K(t^n) \subset K(t)$
    (c) If L is a field extension of K, then L is a vector space over K. (At last, a use for abstract linear algebra.)
3. If K is a field and $X \subset K$ then the following are all equivalent:
    (a) Intersection of all subfields of K containing X
    (b) smallest subfield of K containing X

(c) the set of all expressions $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ where $f,g \in \mathbb{Z}[t_1,\ldots,t_n]$ and $x_1,\ldots,x_n \in X$ and $g(x_1,\ldots,x_n) \neq 0$

(d) This is called the subfield of K generated by X

4. The concept of "generated by" is most often encountered like this: Let $K \subset L$ be fields and let $X \in L$. Ofen X is a finite set. The the subfield of L generated by X **over** K, is the subfield of L generated by the union of X and K. This consists of all expressions $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ where $f,g \in K[t_1,\ldots,t_n]$ and $x_1,\ldots,x_n \in X$ and $g(x_1,\ldots,x_n) \neq 0$. This subfield of L is denoted $K(X)$

(a) Example: $\mathbb{Q}(\sqrt{3},\sqrt{5}) \subset \mathbb{C}$.

(b) If $K \subset L$ and there exists a finite subset $X \subset L$ such that $K(X) = L$, then we say that L is finitely generated over K.

(c) If L is a finite dimensional extension of K then L is finitely generated over K. Proof: L is generated by a vector space basis over K.

(d) You cannot write $K(X)$ unless K and X are both contained in some field. $K(t)$ is a field but not the field generated by t over K, because we don't know how to fill in the blank in $K(t)$ is the subfield of *** generated by t over K.

(e) The great mathematician Andre Weil, recently deceased at 90+, imagined a universal domain, a huge field which contained all the fields he wanted to use,to overcome this problem. Serre and Grothendieck use another approach.

5. In $\mathbb{C}$, the fields $\mathbb{Q}(\sqrt{a})$ consists of all expressions of the form $q_0 + q_1\sqrt{a}$, where $q_i \in \mathbb{Q}$.

(a) $b \in \mathbb{Q}(\sqrt{a})$, then

$$b = \frac{c_1 + c_2\sqrt{a}}{d_1 + d_2\sqrt{a}}$$

, where $c_i, d_i, \in Q$. Then there are two possibilities: either $d_1 \neq d_2\sqrt{a}$ and

$$\begin{aligned} b &= \frac{(c_1 + c_2\sqrt{a})(d_1 - d_2\sqrt{a})}{(d_1 + d_2\sqrt{a})(d_1 - d_2\sqrt{a})} \\ &= \frac{e_1 + e_2\sqrt{a}}{d_1^2 - d_2^2 a} \\ &= g_1 + g_2\sqrt{a} \end{aligned}$$

where $g_1, g_2 \in \mathbb{Q}$.

6. Let $K \subset L$ be a field extension and $a \in L$. Suppose there exists a polynomial $q \in K[t]$ such that $q(a) = 0$. In that case we say that a is *algebraic* over K.

(a) If $K \subset L \subset M$ and $a \in M$ is algebraic over K, then a is algebraic over L.

7. If a is algebraic in L over K, then the *minimal polynomial* of a over K is the monic polynomial p of smallest degree in $K[t]$ such that $p(a) = 0$.

(a) This polynomial exists uniquely as the unique monic generator of the ideal $\{q \in K[t] : q(a) = 0\}$.

(b) The minimal polynomial of a over K is irreducible, because if $p = qr$ then either $q(a) = 0$ or $r(a) = 0$.

(c) Any monic irreducible polynomial p such that $p(a) = 0$ is the minimal polynomial for a, because any such polynomial is divisible by the minimal polynomial.

(d) If p is the minimal polynomial of a over K, and if $\deg p = n$, then the elements $1, a, \ldots a^{n-1}$ are linearly independent over K,because otherwise a polynomial of degree less than n would have a as a root.

8. An extension $K \subset L$ is called *simple* if and only if $L = K(a)$ for some $a \in L$.

   (a) $K(t)$ is simple over K

   (b) $K(t)$ is simple over $K(t^n)$.

   (c) $\mathbb{Q}\left(\sqrt{2}\right)$ is simple over $\mathbb{Q}$

9. Let $K \subset L$ and $a \in L$. Then a is algebraic over K if and only if the simple extension $K(a)$ is finite dimensional over K.

   (a) Proof: Suppose $K(a)$ is finite dimensional over K.. Consider the sequence of elements $1, a, a^2, a^3, \ldots$. Eventually it must be linearly dependent, so there exist constants $c_i \in K$, not all 0, such that $c_0 + c_1 a + \cdots + c_n a_n = 0$ for some n. If $p = c_0 + c_1 t + \cdots + c_n t^n \in K[t]$, then $p(a) = 0$.
   Conversely, suppose a is algebraic over K. Let p be the minimal polynomial of a. I claim that if $\deg p = n$ then $1, a, a^2, \ldots, a^{n-1}$ is a basis for L over K. Let $\alpha \in K(a)$, so $\alpha = \dfrac{q(a)}{r(a)}$ for some polynomials q and r such that $r(a) \neq 0$. Divide q and r by by p and let the remainders be q_1 and r_1. Then $q(a) = q_1(a)$ and $r(a) = r_1(a)$, so $\alpha = \dfrac{q_1(a)}{r_1(a)}$. Since $\deg r_1 < \deg p$ and p is irreducible, either r_1 is a constant or r_1 is relatively prime to p. In either case there exist polynomials b, c such that $br_1 + cp = 1$. Moreover, $b(a) r_1(a) = 1$, since $p(a) = 0$. so $\alpha = q_1(a) b(a)$. Divide $q_1 b$ by p and call the remainder q_2. We have $\deg q_2 < n$ and $q_2(a) = \alpha$.so $1, a, \ldots, a^{n-1}$ span L over K.Since p is irreducible it is the minimal polynomial for a and the elements $1, a, \ldots a^{n-1}$ are linearly independent. QED.

10. Let $L = K(a)$ be a simple extension of K. There there is a homomorphism $K[t] \longrightarrow L$ given by $p \longmapsto p(a)$. If the map is $1-1$, then a is transcendental. Otherwise the kernal of the map is the ideal generated by the minimal polynomial p of a. In this case $L \cong \dfrac{K[t]}{(p)}$.

11. Let $K \subset L \subset M$ be a *tower* of extensions. Then $\dim_K M = \dim_K L \dim_L M$.

    (a) Proof: Choose a basis x_i for L over K and y_j for M over L. Then $x_i y_j$ is a basis for M over K. This works for both finite and infinite bases.

12. An extension L of K is said to be *algebraic* if and only if every element of L is algebraic over K.An extension which is not algebraic is *transcendental.* (Mathematicians love colorful words.)

    (a) The extension $\mathbb{Q}\left(\sqrt{2}\right)$ is algebraic over $\mathbb{Q}$

    (b) Infinte dimensional algebraic extensions exists. Consider adjoining all the square roots of numbers to $\mathbb{Q}$, or more generally taking the algebraic closure of $\mathbb{Q}$.

        1. But over $\mathbb{R}$ there are only two algebraic extensions: $\mathbb{R}$ and $\mathbb{C}$., and both are finite dimensional.

    (c) The extension $K(t)$ is transcendental over K, as is $K((t))$. In fact, $K((t))$ is transcendental over $K(t)$.

    (d) $K(t)$ is an algebraic extension of $K(t^n)$.

13. Suppose $K \subset L$. Then L is finitely generated and algebraic over K if and only if L is a finite dimensional vector space over K.

    (a) Proof: If L is a finite dimensional vector space over K, then for every $a \in L$ we have $K(a) \subset L$ is finite dimensional over K, so a is algebraic. We have already shown that a finite dimensional extension of finitely generated.

    (b) Conversely, if L is finitely generated and algebraic, then $L = K(a_1, \ldots, a_t)$ for some elements $a_i \in L$ which are algebraic over K.Then we have the tower of extensions $K \subset K(a_1) \subset K(a_1, a_2) \subset \cdots \subset K(a_1, \ldots, a_n)$, each of which is a simple algebraic extension of its predecessor. Thus each stage is a finite dimensional extension so the top is finite dimensional over the bottom.

14. Corollary: $K(a_1, \ldots, a_n)$ is finitely generated and algebraic over K if and only if a_i is algebraic over K, $1 \leq i \leq t$.

    (a) Proof: If $K(a_1, \ldots, a_n)$ is algebraic over K, then every element, in particular every a_i, is algebraic over K. Conversely, by a theorem above, since a_i is algebraic over $K(a_1, \ldots, a_{i-1})$, $K(a_1, \ldots, a_i)$ is finite dimensional over $K(a_1, \ldots, a_{i-1})$. Therefore $K(a_1, \ldots, a_t)$ is finite dimensional and therefore finitely generated and algebraic over K.

Homework Due October 18

Stewart: 3.6, 3.9, 4.1, 4.13, 4.14
Extra Credit 3.12, 13, 14, 17

Answers

3.9. This problem caused a lot of confusion. Although the answers were basically correct I'm not sure the authors always understood them completely.

Working over $\mathbb{Q}$, let α have minimal polynomial t^2-2 and β have minimal polynomial t^2-4t+2. We have simple extensions $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ in some abstract sense. The best way to think of these extensions is:

$$\begin{aligned}\mathbb{Q}(\alpha) &= \frac{\mathbb{Q}[t]}{(t^2-2)}\\ \mathbb{Q}(\beta) &= \frac{\mathbb{Q}[t]}{(t^2-4t+2)}\end{aligned}$$

You could try to show that these two quotient rings are isomorphic, but a simpler method is to note that $\mathbb{Q}(\alpha)\cong\mathbb{Q}\left(\sqrt{2}\right)\subset\mathbb{C}$ and $\mathbb{Q}(\beta)\cong\mathbb{Q}\left(2+\sqrt{2}\right)\subset\mathbb{C}$. These are isomorphisms between the abstract field extensions and their realizations as subfields of $\mathbb{C}$. It is easy to see that the two subfields of $\mathbb{C}$ are the same, so the two abstract extensions are isomorphic to the same field. Therefore they are isomorphic to each other.

4.13: Suppose $K\subset L\subset M$ are fields and L is algebraic over K and M is algebraic over L. Then M is algebraic over K. The proof involves the idea of "descent". Suppose $m\in M$. Since m is algebraic over L, there exists a polynomial $p(t)=t^n+l_{n-1}t^{n-1}+\cdots+l_0\in L[t]$ such that $p(m)=0$. Here's the key idea: if $L_1=K(l_0,\ldots,l_{n-1})$, then $p(t)\in L_1[t]$ so m is algebraic over L_1. Let $M_1=L_1(m)$. Since m is algebraic over L_1, $[M_1:L_1]<\infty$. But L_1 is finitely generated over K, and every generator l_i is algebraic over K, so $[L_1:K]<\infty$. Therefore $[M_1:K]<\infty$. Since $m\in M_1$, m is algebraic over K.

Given $m\in M$, we have descended from L and M to smaller fields L_1 and M_1 while retaining the relation $m\in M_1$.

Extra Credit

3.12: There exists a field K of characteristic 2 and a quadratic polynomial $p(t)\in K[t]$ that has no roots in the field L, which is obtained by adjoining all the square roots of elements of K to K. Take $K=\mathbb{Z}_2$. Then $L=K$, because adjoining square roots of elements of K to K means adjoining the roots of t^2-0 and t^2-1 to K. But both these polynomials are reducible:

1. $t^2-0=t^2$, and the only root is $t=0$.
2. $t^2-1=(t-1)^2$ and the only root is $t=1$. (Remember, we are working in characteristic 2.)

But the polynomial t^2+t+1 has no root is $\mathbb{Z}_2$ and so is irreducible because any proper factor must be linear and correspond to a root. Therefore adjoing square roots to $\mathbb{Z}_2$ does not create a root of t^2+t+1. Note that this is opposite of the case over $\mathbb{Q}$. If you have square roots of rationals, you can solve any quadratic with rational coefficients using the quadratic formula.

3.13, 3.14: Let K be a field of characteristic 2. If $k\in K$ and if $\sqrt[*]{k}$ is one solution to $t^2+t+k=0$, then $1+\sqrt[*]{k}$ is the other solution. First note that $\sqrt[*]{k}$ and $1+\sqrt[*]{k}$ are not equal, because their difference is not 0. Second, since $\left(\sqrt[*]{k}\right)^2+\sqrt[*]{k}+k=0$, $\left(\sqrt[*]{k}\right)^2=k+\sqrt[*]{k}$ (remember, we are in characteristic 2, so $-a=a$),

$$\begin{aligned}\left(1+\sqrt[*]{k}\right)^2+\left(1+\sqrt[*]{k}\right)+k &= 1+2\sqrt[*]{k}+\left(\sqrt[*]{k}\right)^2+1+\sqrt[*]{k}+k\\ &= \left(k+\sqrt[*]{k}\right)+\sqrt[*]{k}+k\\ &= 0\end{aligned}$$

Now suppose for all $k\in K$

1. the unique solution $\sqrt{k}$ to $t^2+k=0$ is in K
2. the solutions $\sqrt[*]{k}$ and $1+\sqrt[*]{k}$ to $t^2+t+k=0$ are in K.

Then every quadratic equation with coefficients from K has its roots in K. Let $p = t^2 + at + b$ where $a, b \in K$. If $a = 0$ then $\sqrt{b}$ is the unique root of p in K. Otherwise let $\alpha = \dfrac{1}{a}$ and let β be a solution to $\beta^2 + \beta + \alpha^2 b = 0$. We have $\alpha, \beta \in K$. Moreover

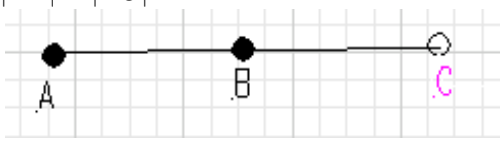
$$\begin{aligned}(\alpha t + \beta)^2 + (\alpha t + \beta) &= \alpha^2 \left(t^2 + \frac{1}{\alpha} t\right) + \beta^2 + \beta \\ &= \alpha^2 \left(t^2 + at\right) + \alpha^2 b \\ &= \alpha^2 p(t)\end{aligned}$$

If we take $\gamma_1 = \dfrac{\beta}{\alpha}$, then $p(\gamma_1) = 0$. The other solution is $\gamma_2 = \dfrac{\beta + 1}{\alpha} = \gamma_1 + a$.

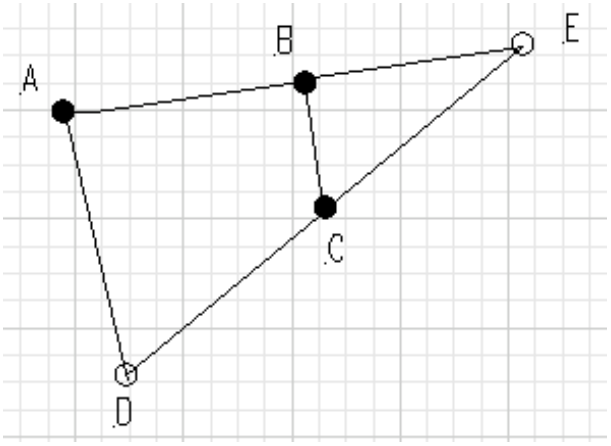
3.17: We will find a field of order 8. I have to apologize here. I thought that the preceeding problems led to a solution of this one, but I was wrong. In fact, if you adjoin a root of $t^2 + t + 1$ to $\mathbb{Z}_2$ you obtain a field K of order 4. Any finite extension of K with have order 4^k for some k, so K cannot be extended to a field of order 8. However the polynomial $t^3 + t + 1$ has no roots in $\mathbb{Z}_2$ and therefore is irreducible over $\mathbb{Z}_2$ (because any factorization would have one linear factor corresponding to a root). Adjoining a root of this polynomial to $\mathbb{Z}_2$ results in a field K of order $2^3 = 8$.

Ruler and Compass Constructions

1. Important notation not introduced earlier: if $K \subset L$ then $[L : K] = \dim_K L$.
2. As the Greeks developed geometry, they found three problems that resisted all efforts:
   (a) Trisecting an angle
   (b) Duplicating a cube
   (c) Squaring the circle
3. Eventually all these operations were shown to be impossible
   (a) Mathematics much profited by the effort
   (b) Nevertheless new solutions are announced to these problems annually, and detailed proofs are sent to math departments throughout the world.
      1. Since no mathematician wants to go down in history with those that initially rejected Ramanujan's work, every one of these proofs is checked for signs of genius.
      2. I have in my office a beautifully illustrated new method of trisecting angles.
   (c) The problems are essentially different, and we will only show that the first two are impossible.
      1. The first two involve algebraic quantities
      2. The last one involves showing that π is transcendental over $\mathbb{Q}$, which we omit.
4. Geometric constructions begin with a given figure and some rules for operating on it
   (a) Figures consist of points, lines and circles
   (b) Operations consist:of:
      1. drawing a line through two points (ruler)
      2. drawing a circle with given center and radius (compass)
         1. For the Greeks this meant given a center and point on the circumference
      3. determining the intersection of two lines, two circles, or a line and a circle
      4. AND any other operation compounded out of these, for example
         1. drawing a perpendicular bisector to a line segment
         2. drawing the circle circumscribed about a triangle
         3. drawing a circle about a point whose radius is equal to the distance between two other points.
            Proof: 1.Given points A and B, we can construct a point C on the line AB such that $|AB| = |BC|$

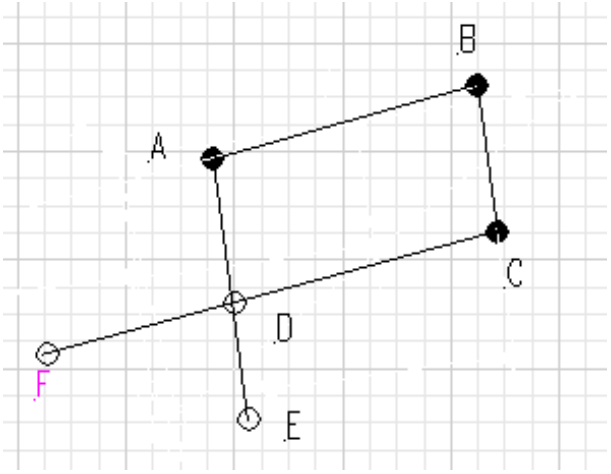
            

            C is the intersection (other than A) of the line AB and the circle with center B passing through A.
            2. Given three points A, B, C, we can construct a line through A parallel to BC



Construct E on the line AB such that $|AB| = |BE|$. Construct D on the line EC such that $|EC| = |CD|$. Then AD is parallel to BC by similar triangles.

3. Given a point A and two points BC, we can construct a point D such that $|AD| = |BC|$



Construct lines $CF \,||\, AB$ and $AE \,||\, BC$. Their intersection D satisfies the requirement, since $ABCD$ is a parallelogram.

The circle with center A passing through D is the circle with center A and radius equal to $|BC|$.

5. Every geometric figure can be interpreted as a finite set of points, and every geometric construction can be interpreted as finding new points from old

   (a) A line is a pair of points

   (b) A circle is a center and one point on the radius

   (c) The intersection of two figures is a point or two points.

   (d) So geometry can be reduced to constructing points from points, but it would be hard to have mental pictures.

6. Nevertheless, thinking this way and adding Cartesian ideas, we make some progress

   (a) Greek concepts alone do not lead to a solution (although I think the solution could be rewritten, in retrospect, entirely in Greek terms)

   (b) A point is a pair of real numbers (a, b)

   (c) A figure is a finite set of pairs of real numbers $\{(a_i, b_i)\}_{i=1\ldots n}$

   (d) The field K associated with a figure is the field $K = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$.

      1. $\mathbb{Q} \subset K \subset \mathbb{R}$

(e) A number is *constructible* from a figure if and only if it is the coordinate of a point constructible from the figure.

1. The definition is sort of one-way. A constructible point has constructible coordinates, but it is not obviously true that a point whose coordinates are constructible is a constructible point. However it is true, as we see below.

7. **The big theorem:** Let K be the field associated with a figure, and suppose $c_1, \ldots, c_t$ are numbers constructible from the figure. If $L = K(c_1, \ldots, c_t) \subset \mathbb{R}$, then $[L : K] = 2^m$ for some m.

(a) As a first step, suppose you have a figure (a finite set of points) and its field K.

1. Any line through two points has an equation $ax + by + c = 0$ with coordinates a, b, c from K
2. Any circle centered at one point through another point has an equation $ax^2 + bx + cy^2 + dy = e = 0$ with coordinates a, b, c, d, e from K.
3. The intersection point of two lines from the figure has coordinates in K
4. The intersection points of a line and a circle from the figure has coordinates in K or a quadratic extension of K (an extension of degree 2).
5. The intersection points of two circles from the figure has coordinates in K or a quadratic extension of K (an extension of degree 2).

(b) If you construct a series of points $(a_i, b_i)_{i=1\cdots t}$ from a figure with field K, each one constructed in one step from the figure and the previous ones, then

$$\begin{aligned} [K(a_1, b_1, \ldots a_i, b_i, a_{i+1}) : K(a_1, b_1, \ldots a_i, b_i)] &\leq 2 \\ [K(a_1, b_1, \ldots a_i, b_i) : K(a_1, b_1, \ldots a_i)] &\leq 2 \end{aligned}$$

Thus

$$[K(a_1, b_1, \ldots, a_n, b_n) : K] = 2^k$$

for $0 \leq k \leq 2t$.

(c) If you have a set of constructible numbers $c_1, \ldots, c_t$, then $[K(c_1, \ldots, c_t) : K] = 2^m$ for some m.

1. Because these numbers are coordinates of constructible points that can be put into a series of points constructible in one step from the figure and the previously constructed points. Thus $K(c_1, \ldots, c_t) \subset L$, where L is the field generated by the coordinates of all the points. Since $[L : K] = 2^k$ for some k, $[K(c_1, \ldots, c_t) : K] = 2^m$ for some $m \leq k$.

(d) In particular, if c is constructible over K then $[K(c) : K] = 2^m$ for some m.

(e) Example: circles of radius 1 centered at $(0, 0)$ and $(0, 1)$ intersect at $\left(\frac{1}{2}, \pm\frac{\sqrt{3}}{2}\right)$, so $\frac{\sqrt{3}}{2}$ is constructible over $\mathbb{Q}$. The intersection of the circle centered at $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ passing through $\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$ with the y-axis, we get a constructible number $c = \frac{1}{2}\sqrt{3} \pm \frac{1}{2}\sqrt{11}$. In this case $[\mathbb{Q}(c) : \mathbb{Q}] = 4$.

8. **Applications of the big theorem to impossibility proofs**

(a) The cube cannot be duplicated:

1. Given a cube of side 1, duplicating it requires constructing a length (coordinate) equal to $\sqrt[3]{2}$. But $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ because the minimal polynomial over $\mathbb{Q}$ of $\sqrt[3]{2}$ is $x^3 - 2$. (If the polynomial factored, there would be a linear factor with constant term $\sqrt[3]{2}$. But $\sqrt[3]{2}$ is not rational, as the Greeks knew. Also, this polynomial is irreducible by Eisenstein's criterion.)

(b) The triangle cannot be trisected

1. It suffices to show that one angle cannot be trisected, so consider the angle $60°$, or the figure with points $(0,0)$, $(1/2,0)$, $\left(1/2,\sqrt{3}/2\right)$. Trisecting the angle would permit constructing the point $(\cos 20, \sin 20)$ on the unit circle. We will show that $\cos 20$ cannot be a constructible number. Everybody knows the formula:

$$\begin{aligned} \cos 3\theta &= 4\cos^3\theta - 3\cos\theta \\ \cos 60 &= 4\cos^3 20 - 3\cos 20 \end{aligned}$$

Thus $\cos 20$ is a root of the polynomial $4x^3-3x-1/2$ so at least $\cos 20$ is algebraic. Simplifying slightly, we see that $\cos 20$ is a root of $p(x) = 8x^3 - 6x - 1$. If $2x - 1 = t$, then

$$\begin{aligned} p(x) &= (t+1)^3 - 3(t+1) - 1 \\ &= t^3 + 3t^2 - 3 \\ &= q(t) \end{aligned}$$

$q(t)$ is irreducible by Eisenstein, so $p(x)$ is irreducible.(Our author often applies Eisenstein's criterion after a linear change of variable.) Since $p(x)$ is irreducible, it is the minimal polynomial of $\cos 20$. Thus $[\mathbb{Q}(\cos 20) : \mathbb{Q}] = 3$ and $\cos 20$ is not constructible.

9. **Applications of the big theorem to possibility proofs**

(a) Suppose you start with the points $(0,0)$ and $(1,0)$, What are the constructible points and the constructible numbers?

(b) x-axis and y-axis can be constructed

(c) If (a,b) is a constructible point, then $(a,0), (0,b), (b,0), (0,a)$, and (b,a) is also constructible

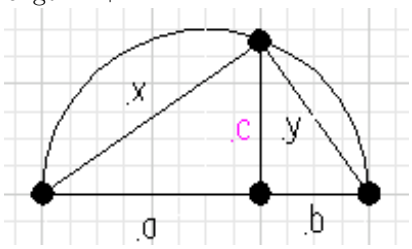
(d) If a is a constructible number than $(a,0)$ and $(0,a)$ are constructible points

(e) If a, b are constructible numbers, then (a,b) is a constructible point.

(f) If a, b are constructible numbers, then so is $a+b$, $a-b$, ab, a/b

(g) If a is constructible then so is $\sqrt{a}$

1. We will show that if a, b are constructible, then so is $\sqrt{ab}$. Taking $b = 1$ gives our result. The following figure is constructible as a circle about the midpoint of the line segment of length $a+b$



$$\begin{aligned} a^2 + c^2 &= x^2 \\ b^2 + c^2 &= y^2 \\ x^2 + y^2 &= (a+b)^2 \\ c^2 &= ab \end{aligned}$$

(h) If a, b are constructible, then so are the solutions to $x^2 + ax + b = 0$ provided they are real.

1. Show that solution to $(x-\alpha)^2 = \beta \geq 0$ is constructible if α, β are constructible.

(i) If $K \supset \mathbb{Q}$ consists entirely of constructible quantities and c is constructible then $K(c)$ is constructible.

(j) If $K \supset \mathbb{Q}$ consists entirely of constructible quantities and if $L \supset K$, $[L : K] = 2$, then L consists entirely of constructible quantities

1. $L = K(c)$ for a solution c to a quadratic polynomial.

(k) Integral coordinates can be placed on the axes

(l) Every rational point $\left(\frac{a}{b}, 0\right)$ and $\left(0, \frac{c}{d}\right)$ and $\left(\frac{a}{b}, \frac{c}{d}\right)$ can be constructed, so $\mathbb{Q}$ is constructible

(m) Suppose $c \in \mathbb{R}$ and, $[\mathbb{Q}(c) : \mathbb{Q}] = 2^m$ for some m. Then c is constructible over $\mathbb{Q}$.

1. To prove this we need to construct a sequence of fields $\mathbb{Q} \subset K_1 \subset \cdots \subset K_{m-1} \subset \mathbb{Q}(c)$ with each step an extension of degree 2. For this, we need Galois theory. We will return to the issue of possible constructions after studying some Galois theory.

Automorphisms of Fields

1. Let $K \subset L$ be fields. Then a *K-automorphism of L* is a homomorphism $\varphi : L \longrightarrow L$ such that $\varphi|_K = id$.

   (a) The set of K-automorphism of L is denoted $\mathrm{aut}_K(L)$.or $\Gamma(L : K)$

   (b) $\Gamma(L : K)$ is a group

   (c) $\Gamma(L : K)$, the *Galois group* of L over K.

2. Examples

   (a) Conjugation is an element of $\mathrm{aut}_{\mathbb{R}} \mathbb{C}$.

   (b) Let $\omega = \frac{-1 + \sqrt{3}i}{2}$, $\omega^3 = 1$. The minimal polynomial of ω is $x^2 + x + 1$ and $\omega^2 = \bar{\omega}$., so if $L = \mathbb{Q}(\omega)$ then conjugation maps $L \longrightarrow L$ and is a $\mathbb{Q}$-automorphism of L

   (c) There are three complex numbers τ_i such that $\tau_i^3 = 2$. All have the same minimal polynomial over $\mathbb{Q}$: $x^3 - 2$., We can take $\tau_2 = \omega\tau_1$, $\tau_3 = \omega\tau_2$.

      1. Let $K_i = \mathbb{Q}(\tau_i)$ and $L = \mathbb{Q}(\tau_1, \tau_2, \tau_3)$.
         1. $K_i = \left\{a + b\tau_i + c\tau_i^2 : a, b, c \in \mathbb{Q}\right\}$
         2. $L = \left\{a + b\tau_i + c\tau_i^2 + d\tau_j + e\tau_i\tau_j + f\tau_i^2\tau_j : a, b, c, d, e, f \in \mathbb{Q}\right\}$
      2. $K_i = \frac{\mathbb{Q}[x]}{(x^3 - 2)}$
      3. Let τ_1 be the real root. $K_1 \subset \mathbb{R}$, $K_2, K_3 \not\subset \mathbb{R}$. Therefore $\Gamma(K_1 : \mathbb{Q}) = (1)$ because $\sigma \in \Gamma(K_1 : \mathbb{Q})$ implies $\sigma(\tau_1) = \tau_i$ and the only $\tau_i \in K_1$ is τ_1.But since all the K_i are isomorphic over $\mathbb{Q}$, $\Gamma(K_i : \mathbb{Q}) = (1)$, $i = 1, 2, 3$.
      4. $\Gamma(L : \mathbb{Q}) = S_3$. any permutation of $\{\tau_1, \tau_t, \tau_3\}$ induces an automophism.of L

   (d) If $K \subset L \subset M$ then $\Gamma(M : L) \subset \Gamma(M : K)$

      1. $\Gamma(L : K_i) \subset \Gamma(L : \mathbb{Q})$ and consists of the identity and the exchange $\tau_j \leftrightarrow \tau_k$ and so is isomorphic to $\frac{\mathbb{Z}}{(2)}$
      2. $\Gamma(L : \mathbb{Q}(\omega)) = \frac{\mathbb{Z}}{(3)}$ and is generated by the permutation $\tau_1 \longrightarrow \tau_2 \longrightarrow \tau_3 \longrightarrow \tau_1$

3. If $H \subset \Gamma(L : K)$ then $L^H = \{\alpha \in L : h(\alpha) = \alpha,\ \forall h \in H\}$ is a field and $K \subset L^H \subset L$., the *fixed field* of H.

   (a) H is the subgroup of S_3 generated by $(2, 3)$. Then in the example $L^H = K_1$. Similarly for the subgroups generated by $(1, 2)$ and $(1, 3)$.

   (b) H is the subgroup of S_3 generated by $(1, 2, 3)$. Then in the example $L^H = \mathbb{Q}(\omega)$.

4. Given $K \subset L$, we have a maps $\{\text{subfields between } K \text{ and } L\} \leftrightarrow \{\text{subgroups of } \Gamma(L : K)\}$

   (a) See example above

(b) The pairing is perfect (1-1 and onto)

(c) The pairing is NOT perfect for K_i over $\mathbb{Q}$

1. This is the situation Grothendieck calls *anabelian*—no symmetries at all.

(d) Galois theory focuses on the situation when the pairing between subspaces and subgroups is $1-1$ and onto.

(e) Both mappings reverse inclusions

1. If $H \subset K \subset \Gamma(L)$ are subgroups then $L^K \subset L^H$
2. If $K \subset M \subset N \subset L$ are subfields then $\Gamma(L,N) \subset \Gamma(L,M)$

5. Whenever you have a map like this, you must ask if the two directions are inverses, or even one sided inverses. Suppose $K \subset L$. Suppose further that $G = \Gamma(L:K)$, $K \subset M \subset L$ is a subfield, and $H \subset G$.is a subgroup.

(a) Is $\Gamma\left(L : M^H\right) = H$

(b) Is $L^{\Gamma(L:M)} = M$

(c) We can show $H \subset \Gamma\left(L : L^H\right)$

$$\begin{array}{ccccccc} (1) & \subset & H & \subset & \Gamma\left(L:L^H\right) & \subset & G \\ & & \searrow & \nearrow & & & \\ L & \supset & L^H & & \supset & & K \end{array}$$

1. $\sigma \in \Gamma\left(L : L^H\right)$ iff $\sigma : L \longrightarrow L$ and $x \in L^H$ implies $\sigma(x) = x$. But $x \in L^H$ iff $\sigma(x) = x$ all $\sigma \in H$, so $H \subset \Gamma\left(L : L^H\right)$.

(d) We can show $M \subset L^{\Gamma(L:M)}$

$$\begin{array}{ccccccc} (1) & & \subset & & \Gamma(L:M) & \subset & G \\ & & \swarrow & & \nwarrow & & \\ L & \supset & L^{\Gamma(L:M)} & \supset & & M & \supset K \end{array}$$

1. $\Gamma(L:M) = \{\sigma : L \longrightarrow L : \sigma(x) = x, \forall x \in M\}$. Thus, if $x \in M$, and $\sigma \in \Gamma(L:M)$, then $\sigma(x) = x$.Thus $M \subset L^{\Gamma(L:M)}$

(e) As we have seen, the results need not be equal, but:

1. $\Gamma(L:M) = \Gamma\left(L : L^{\Gamma(L:M)}\right)$
   Proof: $M \subset L^{\Gamma(L:M)}$ so $\Gamma(L:M) \supset \Gamma\left(L : L^{\Gamma(L:M)}\right)$ by 4(e)2. Conversely $\Gamma\left(L : L^{\Gamma(L:M)}\right) \supset \Gamma(L:M)$ by 5c .
2. $L^H = L^{\Gamma\left(L:L^H\right)}$. The proof is similar.

(f) The text uses inferior notation, because it is too condensed.

$$\begin{aligned} L^H &= H^\dagger \\ \Gamma(L:M) &= M^* \end{aligned}$$

6. One more example: $L = \mathbb{Q}\left(\sqrt{5},\sqrt{7}\right) = \mathbb{Q}\left(\sqrt{5}+\sqrt{7}\right) = \mathbb{Q}\left(\sqrt{5}\right)\left(\sqrt{7}\right) = \mathbb{Q}\left(\sqrt{7}\right)\left(\sqrt{5}\right) = \left\{a+b\sqrt{5}+c\sqrt{7}+d\sqrt{35}\right\}$

(a) $L = \left\{a+b\sqrt{5} : a,b \in \mathbb{Q}\left(\sqrt{7}\right)\right\}$ and $\Gamma\left(L : \mathbb{Q}\left(\sqrt{7}\right)\right) = \left\{id, a+b\sqrt{5} \longrightarrow a-b\sqrt{5}\right\}$

1. In $\Gamma(L:\mathbb{Q})$,the non-trivial automorphism is $\sigma\left(a+b\sqrt{5}+c\sqrt{7}+d\sqrt{35}\right) = a-b\sqrt{5}+c\sqrt{7}-d\sqrt{35}$

(b) $L = \left\{a+b\sqrt{7} : a,b \in \mathbb{Q}\left(\sqrt{5}\right)\right\}$ and $\Gamma\left(L : \mathbb{Q}\left(\sqrt{5}\right)\right) = \left\{id, a+b\sqrt{7} \longrightarrow a-b\sqrt{7}\right\}$

1. In $\Gamma(L:\mathbb{Q})$,the non-trivial automorphism is $\tau\left(a+b\sqrt{5}+c\sqrt{7}+d\sqrt{35}\right) = a+b\sqrt{5}-c\sqrt{7}-d\sqrt{35}$

(c) Thus $\sigma\tau\left(a+b\sqrt{5}+c\sqrt{7}+d\sqrt{35}\right) = a-b\sqrt{5}-c\sqrt{7}+d\sqrt{35}$ and $\Gamma(L:\mathbb{Q}) \cong \dfrac{\mathbb{Z}}{(2)} \oplus \dfrac{\mathbb{Z}}{(2)}$

(d) $L^{<\sigma\tau>} = \mathbb{Q}\left(\sqrt{35}\right)$

Homework Due Monday, October 25

Stewart 5.3, 5.6, 7.1, 7.3, 7.5, 7.6

Note: Stephen Jameyson found a terrific up-to-date biography of Evariste Galois by Tony Rothman at http://wwwrel.ph.utexas.edu/~tonyr/galois.html

Splitting Fields, Normal Extensions and Separability

1. Let K be a field and $f \in K[t]$ be a polynomial. There exists a field $L \supset K$ and $\alpha \in L$ such that $f(\alpha) = 0$

   (a) Lemma: If $K \subset L$ and K is a field and L is an integral domain and $\dim_K L < \infty$, then L is a field. Proof: Suppose $x \in L$, $x \neq 0$. Consider the K-linear map $y \mapsto xy$ mapping $L \longrightarrow L$. This map is $1-1$ because L is an integral domain, so it is onto because L is finite dimensional. Therefore, for some $y \in L$, $xy = 1$. Thus every non-zero element of L is invertible, and L is a field.

   (b) We can assume that f is irreducible since any root of an irreducible factor of f is a root of f. Let

   $$L = \frac{K[t]}{(f)}$$

   Clearly L is a ring containing (an copy of) K and $f(\bar{t}) = 0$ in L. Moreover, as a vector space, L is finite dimensional over K. It remains to show that L is a field.

   To show that L is an integral domain, suppose $\bar{g}\bar{h} = 0$. Then $f \mid gh$, so $f \mid g$ or $f \mid h$. Thus either $\bar{g} = 0$ or $\bar{h} = 0$. L is finite dimensional over K because it has a basis $\bar{1}, \bar{x}, \ldots, \bar{x}^{\deg f - 1}$.But then L is a finite dimensional integral domain over a field, so L is a field.

   (c) Example: if $K = \mathbb{Q}$ and $f{=}t^2 - 2$ then $L = \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{C}$.

2. Let K be a field and $f \in K[t]$ and $L \supset K$ is an extension field. Suppose $\deg f = n$. We say *f splits in L.* if and only if there exist $a_1, \ldots, a_n \in L$ such that $f = (t - a_1) \cdots (t - a_n)$. The a_i need not be distinct..

   (a) In the example above $\pm\sqrt{2} \in L$ and $f = \left(t - \sqrt{2}\right)\left(t + \sqrt{2}\right)$ so f splits in L.

   (b) We say that L is a *splitting field* for f iff f splits in L and $L = K(a_1, \ldots, a_n)$.

   (c) This is equivalent to saying that $K \subset M \subset L$ and f splits in M implies $M = L$

3. Let K be a field and $f \in K[t]$. Then there exists a splitting field L for f.

   (a) By 1, there exists a field $L_1 \supset K$ and element $a_1 \in L_1$ such that $f(a_1) = 0$. Thus, in $L_1[x]$, $f = (x - a_1) f_1$.for some polynomial $f_1 \in L_1[x]$. There exists a field $L_2 \supset L_1$ and $a_2 \in L_2$ such that $f_1(a_2) = 0$. Thus, in $L_2[x]$, $f_1 = (x - a_2) f_2$ for some polynomial $f_2 \in L_2[x]$. Moreover $f = (x - a_1)(x - a_2) f_2$ in $L_2[x]$. Continuing in this way, if $n = \deg f$, we get a field L_n, containing elements $a_1, \ldots, a_n$, and in $L_n[x]$ we have $f = (x - a_1) \cdots (x - a_n)$. Thus f splits in L. The splitting field for f is $K(a_1, \ldots, a_n) \subset L$.

4. Example: the field $\mathbb{Q}\left(\sqrt[3]{2}\right)$ contains a root of $x^3 - 2$ but is not a splitting field for this polynomial. To obtain a splitting field you must adjoin all three cube roots of 2.

5. If L is the splitting field for f over K and $a \in L$ such that $f(a) = 0$ then

   (a) $f = (t - a) f_1$ in $K(a)[t]$

   (b) L is the splitting field for f_1 over $K(a)$

6. How unique is the splitting field? Up to non-unique isomorphism. We have two results.

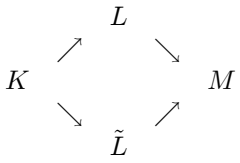
7. Let $K \subset L, \tilde{L} \subset M$ be fields, and suppose L and $\tilde{L}$ are splitting fields for a polynomial $f \in K[t]$. Then $L = \tilde{L}$

   (a) Let $L = K(a_1, \ldots, a_n)$ where the a_i are the roots of f in L, and let $\bar{L} = K(\widetilde{a_1}, \ldots, \widetilde{a_n})$ where $\widetilde{a_i}$ are the roots of f in $\bar{L}$. Then, in $M[t]$, $f = \prod (t - a_i) = \prod (t - \widetilde{a_i})$. By unique factoization, the sets $\{a_i\}$ and $\{\widetilde{a_i}\}$ are the same, so $L = \bar{L}$.

8. Let K be a field and $f \in K[t]$. Let $L \supset K$ and $\tilde{L} \supset K$ be splitting fields for f. Then there exists an isomorphism $\varphi : L \longrightarrow \tilde{L}$ such that $\varphi|_K = id$.

(a) Bad idea: given two splitting fields L and L' generated by roots a_i and a_i' , map L to L' by mapping a_i to a_i' . This might not be an isomorphism. See example later.

(b) Proof very different from one in text. It uses two theorems and two lemmas

1. If R is a commutative ring with identity and $I \subset R$ is an ideal, then $\dfrac{R}{I}$ is a field if and only if I is a maximal ideal.
2. If R is a commutative ring with identity and $I \subset R$ is an ideal, then there exists a maximal ideal $\mathbf{m}$ containing I.
3. If $K \subset L$ is an extension field and T is a set of variables independent of L (*i.e.* $L[T]$ is a pure polynomial ring) and $\mathbf{q}$ is a proper ideal in $K[T]$ then $\mathbf{q}$ generates a proper ideal in $L[T]$. Proof: Otherwise there exists $q_i \in \mathbf{q} \subset K[T]$ and $a_i \in L[T]$ such that $\sum a_i q_i = 1$. Let $\{v_j\}$ be a basis for L over K, and assume $v_1 = 1$. Note that $\{v_i\}$ is also a basis for $L[T]$ over $K[T]$. That is, if $p \in L[T]$ then $p = \sum p_i v_i$ for unique polynomials $p_i \in K[T]$. Write $a_i = \sum \alpha_{ij} v_j$, where $\alpha_{i,j} \in K[T]$., so that
$$\begin{aligned} 1 &= \sum\sum \alpha_{ij} v_j q_i \\ &= \sum \left(\sum \alpha_{ij} q_i \right) v_j \end{aligned}$$
Then for $j > 1$, $\sum \alpha_{ij} q_i = 0$, and $\sum \alpha_{i1} q_i = 1$. But then $\mathbf{q}$ is the unit ideal in $K[T]$ which is a contradiction.
4. Let K be a field and suppose $L \supset K$ and $\tilde{L} \supset K$ are extension fields. Then there exists a field M and a commutative diagram


That is, you can imbed two extensions in a common extension.
Write $L = \dfrac{K[S]}{\mathbf{p}}$, where S is a set of variables and $\mathbf{p}$ is a maximal prime ideal. Similarly write $\bar{L} = \dfrac{K[T]}{\mathbf{q}}$. You can assume that the sets of variables S and T are disjoint. Then in the ring $K[S,T]$ the ideal I generated by $\mathbf{p}$ and $\mathbf{q}$ is not the unit ideal.
   1. To show this, consider the ring $R = \dfrac{K[S]}{\mathbf{p}}[T] \cong L[T]$, a pure polynomial ring. The ideal I is the unit ideal if and only if $\mathbf{q}$ generates the unit ideal in R., which is impossible by 8(b)3.

   In $K[S,T]$ choose a maximal ideal $\mathbf{m} \supset I$., and take $M = \dfrac{K[S,T]}{\mathbf{m}}$.

To prove the theorem, choose a field M containing images of L and $\bar{L}$ over K. Then by 7 the image of L equals the image of $\bar{L}$ in M, so $L \cong \bar{L}$.

9. **Corollary:** If $K \cong \bar{K}$ and the isomorphism carries a polynomial $f \in K[t]$ into $\bar{f} \in \bar{K}[t]$, and if L is a splitting field for f over K and $\bar{L}$ is a splitting field for $\bar{f}$ over $\bar{K}$, then the isomorphism from K to $\bar{K}$ extends to an isomorphism from L to $\bar{L}$ (but the extension need not be unique). To see why, use the map $K \longrightarrow \bar{K}$ to consider $\bar{L}$ as a splitting field for f over K.

10. A field extension $K \subset L$ is *normal* if and only if every irreducible polynomial $f \in K[t]$ with one root in L splits in L. Thus if L contains a root of f then L contains a splitting field for f.

11. **Lemma:** suppose K is a field and:

(a) $K \subset L$ is an extension field

(b) $f \in K[t]$ is irreducible

(c) $a \in L$ such that $f(a) = 0$

Then there exists an isomorphism $\frac{K[t]}{(f)} \longrightarrow K(a)$ that is the identity on K. (a K-isomorphism) .

Proof: $K[t] \longrightarrow K[a] = K(a)$ is onto with kernal (f).

12. Suppose $L \supset K$ is an extension field. Then $[L : K] < \infty$ and L is normal over K if and only if L is the splitting field for some polynomial over K.

    (a) First suppose L is normal and finite over K. Since L is finite, L is algebraic over K and $L = K(a_1, \ldots, a_n)$ for some $a_i \in L$ which are algebraic over K.Let f_i be the minimal polynomial of a_i.over K. Then f_i is irreducible and since L is normal, L contains a splitting field of f_i over K. Thus L contains a full set of roots for f_i. If $f = \prod f_i$ then L contains a full set of roots for f and L is generated over K by the roots. Thus L is a splitting field for f over K. (Note that f need not be irreducible.)

    (b) Next suppose L is a spliting field for $g \in K[t]$. Obviously $[L : K] < \infty$. Suppose $a \in L$ has minimal polynomial $f \in K[t]$. Let $\bar{L}$ be a splitting field for f over K and suppose $L, \bar{L} \subset M$ for some field M. We must show $\bar{L} \subset L$. We know that f has one root $a \in L$. Since the roots of f in M generate $\bar{L}$, it suffices to show that all roots of f contained in M are in L. That is, we must show that $b \in M$ and $f(b) = 0$ implies $b \in L$.

    Note that $L(b)$ is a splitting field for g over $K(b)$ and $L(a) = L$ is a splitting field over $K(a)$ for g. By 11 $K(a) \cong K(b)$, so by Corollary 9 $[L : K(a)] = [L(b) : K(b)]$. Then we have

$$\begin{aligned} [L(b) : L][L : K] &= [L(b) : K(b)][K(b) : K] \\ &= [L(a) : K(a)][K(a)] : K] \\ &= [L(a) : L][L : K] \end{aligned}$$

    But $L(a) = L$ so $L(b) = L$ or $b \in L$.

13. An irreducible polynomial is *separable* if it has no repeated zeros in a splitting field.

    (a) An arbitrary polynomial is separable if all its irreducible factors are separable.

        1. i.e. if it has no repeated roots because distinct irreducible polynomials cannot have a common root.

    (b) An element algebraic over a field is separable if its minimal polynomial is separable.

        1. All the elements in a field are separable over the field.

    (c) An extension is separable if all elements are separable.

    (d) an example of an inseparable (non-separable) polynomial is $x^2 + t$ over $K = \frac{\mathbb{Z}}{(2)}(t)$. Proof: f is irreducible over K because it has no roots in K. Its splitting field is $L = \frac{\mathbb{Z}}{(2)}(s)$ where $s^2 = t$, so $K \subset L$. In L, $f = (x + s)^2$ so f has a repeated root, namely s.(Remember, over $\frac{\mathbb{Z}}{(2)}$ there is no difference between minus and plus.)

    (e) Soon we will see that in characteristic 0 and over finite fields all irreducible polynomials are separable. Thus inseparability requires working over infinite fields of finite characteristic.

    (f) If $K \subset L \subset M$ and M is separable over K then M is separable over L and L is separable over K.

14. Back to calculus. For any field K we have a formal differentiation operator $D : K[t] \longrightarrow K[t]$.

15. **Lemma:** a polynomial $f \in K[t]$ has multiple roots if and only if f and Df are relatively prime in $K[t]$.

(a) Two polynomials $f, g \in K[t]$ are relatively prime if and only if any of the following equivalent conditions holds:

1. they have no common factor in $K[t]$ (except units)
2. they have no common root in any extension field of K
3. the ideal $(f, g) = K[t]$
4. there exist polynomials p, q such that $pf + qg = 1$.

(b) Let $K \subset L$ be a splitting field for f, so for $a_i \in L$ we have $f = \prod (t - a_j)$. Thus $Df = \sum \frac{f}{t - a_j}$. Then $Df(a_i) = \prod_{j \neq i} (a_i - a_j)$, so f and Df have a common root if and only iff f has a multiple root.

16. **Corollary:** a polynomial $f \in K[t]$ is separable if and only if f and Df are relatively prime.

17. **Corollary:** an irreducible polynomial $f \in K[t]$ is separable if and only if $Df \neq 0$.

(a) Proof: if $Df = 0$ then f and Df are not relatively prime. Conversely, if f and Df have a common factor, since f is irreducible, then $Df = 0$.

18. If $char(K) = 0$ then every polynomial $f \in K[t]$ is separable.

(a) We can assume f is irreducible. But $char(K) = 0$ and $Df = 0$ implies $f \in K$. Thus every polynomial $f \in K[t]$ is separable.

19. If $char(K) = p$ and f is irreducible then f is inseperable if and only if $f \in K[t^p]$. I.e. $f = a_0 + a_1 t^p + \cdots + a_n t^{np}$.

20. If K is a finite field then every polynomial over K is separable.

(a) Let $char(K) = p$. Note that the map $K \longrightarrow K$, $x \mapsto x^p$, is a homomorphism, so it is an injection. The image is denoted K^p. If K is finite, the map must also be onto, so every element of K has a unique p^{th} root.

(b) There cannot be an inseperable, irreducible polynomial over K. If f is inseperable then $f = a_0 + a_1 t^p + \cdots + a_n t^{np} = \left(a_0^{1/p} + a_1^{1/p} t + \cdots + a_n^{1/p} t^n\right)^p$ so it is not irreducible.

Homework Due Wednesday, November 3

Stewart 8.1, 8.2, 8.9 (assume characteristic 0), 8.10, 8.11
Extra credit: 8.3, 8.4, 8.13 (think characteristic p)

Some Answers

8.11: Suppose $f \in K[t]$, $\deg f = n$. Let $\sum$ be a splitting field for f over K. Then $[\sum : K]$ divides $n!$.

Proof: We go by induction on n, the statement being obvious for $n = 1$ (in that case $\sum = K$). Assuming the statement is true for polynomials of degree less than n, we first prove it for irreducible polynomials of degree n, and then for all polynomials of degree n. Suppose f is irreducible and $\deg f = n$. Choose one root $\alpha \in \sum$ of f, and in $\sum[t]$ let $f = (t - \alpha) g$. Then

1. $[K(\alpha) : K] = n$
2. $\deg g = n - 1$
3. $\sum$ is a splitting field for g over $K(\alpha)$, and thus $[\sum : K(\alpha)]$ divides $(n-1)!$. Therefore

Therefore $[\sum : K] = [\sum : K(\alpha)][K(\alpha) : K]$ divides $(n-1)!n = n!$.

If f is not irreducible, let $f = gh$ where $\deg g < n$ and $\deg h < n$ and $\deg g + \deg h = n$. Let $\sum'$ be a splitting field for g over K contained in $\sum$. ($\sum$ is generated over K by the roots of f, a set which includes the roots of g. $\sum'$ is the subfield generated by the roots of g.) Then $\sum$ is a splitting for h over $\sum'$ and so $\left[\sum, \sum'\right]$ divides $(\deg h)!$ and $\left[\sum' : K\right]$ divides $(\deg g)!$. But if a and b are non-negative integers then $a!b!$ divides $(a+b)!$ (because the quotient is the binomial coefficient $\binom{a}{b}$). Thus $[\sum : K] = \left[\sum, \sum'\right]\left[\sum' : K\right]$ divides $(\deg h)!(\deg g)!$ which divides $(\deg g + \deg h)! = n!$.

8.13 An example of a non-simple extension. I told you what I would try first. I forgot to tell you that whatever I try first never works. Here's a correct example. Let k be a field of characteristic p, and let $L = k(x, y)$, the rational functions in two variables over k. Let $K = k(x^p, y^p) \subset L$. Then $L = K(x, y)$ but L is not simple. To see that this is true, note that the monomials $x^i y^j$, $0 \le i, j < p$ form a vector space basis for L over K, so $[L : K] = p^2$. Thus if $L = K(\alpha)$ for some $\alpha \in L$, the minimal polynomial for alpha would have to have degree p^2. But if $\alpha \in L$ then $\alpha^p \in K$ so the minimal polynomial for α has degree no more than p.

Field Degrees and Group Orders

1. Suppose $K \subset L$, $K \subset M$. There are two sets of maps

   (a) $\hom_K(L, M)$ is the set of homomorphisms $L \longrightarrow M$ that are the identity on K.

      1. These preserve addition and multiplication.
      2. They are always $1 - 1$ and so are never 0.

   (b) $lin_K(L, M)$ is the set of K-linear maps $L \longrightarrow M$.

      1. They are the identity on K because $\sigma(k) = \sigma(k \cdot 1) = k\,\sigma(1) = k \cdot 1 = k$
      2. They preserve addition and multiplication by elements of K
      3. They form a vector space over M by $(m\sigma)(a) = m(\sigma(a))$ for any $m \in M$ and $a \in L$ and $\sigma \in lin_K(L, M)$

   (c) $\hom_K(L, M) \subset lin_K(L, M)$ is a subgroup under addition but not a subspace.

      1. If $\lambda \in \hom_K(L, M)$ and $m \in M$ then

$$\begin{aligned} (m\lambda)(ab) &= m(\lambda(ab)) = m(\lambda(a)\lambda(b)) \\ ((m\lambda)(a))((m\lambda)(b)) &= m^2\lambda(a)\lambda(b) \end{aligned}$$

         so $m\lambda \notin \hom_K(L, M)$.

2. (Dedekind) If $K \subset L$, $K \subset M$ are fields, then $\hom_K(L, M)$ is a linearly independent.subset of $lin_K(L, M)$

   (a) Example $f \in K(t)$ is irreducible, $L = K(a)$ for a root a of f, M a splitting field of f. There could be many homomorphisms of L into M corresponding to different roots of f .

   (b) Proof: we must show that every finite subset of $\hom_K(L, M)$ ˜ 0 is linearly independent. Let $\lambda_1, \ldots, \lambda_n$ be distinct non-zero homomorphisms, which we know are monomorphisms. Suppose for $a_i \in M$, $\sum_{i=1}^n a_i\lambda_i = 0$ as a linear map $L \longrightarrow M$. Thus, for all $x \in L$,

$$\sum_{i=1}^{n} a_i\lambda_i(x) = 0$$

   Suppose further that there is no linear relation with fewer terms. Note that $n > 1$ because no a_i is zero and (since all $\lambda_i's$ are monomorphisms) a single term $a\lambda(x)$ cannot be zero for all $x \in L$. Choose $y \in L$ such that $\lambda_1(y) \neq \lambda_n(y)$. (Automatically $y \neq 0$.) Then for all $x \in L$:

$$\sum a_i\lambda_i(yx) = \sum a_i\lambda_i(y)\lambda_i(x) = 0$$

   Also for all $x \in L$:

$$\lambda_n(y)\sum a_i\lambda_i(x) = \sum a_i\lambda_n(y)\lambda_i(x) = 0$$

   Subtracting, we have for all $x \in L$:

$$\sum_{i=1}^{n-1} a_i(\lambda_i(y) - \lambda_n(y))\lambda_i(x) = 0$$

   If we let $b_i = a_i(\lambda_i(y) - \lambda_n(y))$, we have $\sum_{i=1}^{n-1} b_i\lambda_i(x) = 0$ for all $x \in L$, so $\sum_{i=1}^{n-1} b_i\lambda_i = 0$ in $lin_K(L, M)$. This is a shorter linear relation than the one we started with, contradicting the minimality of the first one.

3. Let $K \subset L$ be fields, and let G be a finite subgroup of $\Gamma(L : K)$. Then $\#G = \left[L : L^G\right]$.

   (a) Lemma 1: if a linear system of equations have more unknowns than equations, then it has a non-zero solution

(b) If $G = \{g_1, \ldots, g_n\}$. Then $G = \{g_i g_1, \ldots, g_i g_n\}$ for any i, $1 \leq i \leq n$. Note that $g_1, \ldots, g_n \in \hom_K(L, L)$ form a linearly indpendent set in $lin_K(L, L)$.

(c) We show $\left[L : L^G\right] < \#G$ leads to a contradiction. Let $x_1, \ldots, x_m$ be a basis for L over L^G, where $m < n = \#G$. There exists $y_1, \ldots, y_n$, not all 0, such that

$$\sum_{j=1}^{n} g_j(x_i) y_j = 0$$

for $1 \leq i \leq m$. For any $a \in L$ we have $a = \sum_{i=1}^{m} \alpha_i x_i$ for some $\alpha_i \in L^G$, and

$$\begin{aligned}
\sum_{j=1}^{n} g_j(a) y_j &= \sum_{j=1}^{n} \sum_{i=1}^{m} g_j(\alpha_i x_i) y_j \\
&= \sum_{j=1}^{n} \sum_{i=1}^{m} g_j(\alpha_i) g_j(x_i) y_j \\
&= \sum_{i=1}^{m} \alpha_i \left(\sum_{j=1}^{n} g_j(x_i) y_j \right) \\
&= 0
\end{aligned}$$

Thus $\sum_{i=1}^{n} y_i g_i = 0$, contradicting the independence of the g_i.

(d) Finally, we show that $\left[L : L^G\right] > \#G = n$ leads to a contradiction.

1. Suppose you choose elements $x_1, \ldots, x_{n+1} \in L$ that are linearly independent over L^G Then the system of linear equations over L:

$$\sum_{i=1}^{n+1} g_j(x_i) y_i = 0 \quad 1 \leq j \leq n$$

has a non-zero solution.

2. Choose the non-zero solution so the smallest number possible (t) are non-zero, and renumber the x_i so that $y_i \neq 0$ if $i \leq t$ and $y_i = 0$ if $i > t$. Then we have a totally non-zero solution to the system of equations:

$$\sum_{i=1}^{t} g_j(x_i) y_i = 0 \quad 1 \leq j \leq n \tag{6.1}$$

where $t \leq n+1$. We may assume that we have choosen a system with the fewest number of non-zero terms, and that we have renumbered the x_i so that for some t, $2 \leq t \leq n+1$, $y_i \neq 0$ if and only if $i \leq t$.

3. Choose $g \in G$ and multiply all the equations by g. They are still all 0 since $g(0) = 0$ in L.

$$\sum_{i=1}^{t} g g_j(x_i) g(y_i) = 0 \quad 1 \leq j \leq n \tag{6.2}$$

As $j = 1..n$, gg_j traverses all the elements g_k of G exactly once, so the system (3(d)3) is the same as:

$$\sum_{i=1}^{t} g_j(x_i) g(y_i) = 0 \quad 1 \leq j \leq n \tag{6.3}$$

Thus $y_1, \ldots, y_r$ and $g(y_1), \ldots, g(y_r)$ are both solutions to the system (3(d)2).

4. Multiplying $(3(d)2)$ by $g(y_1)$ and $(3(d)3)$ by y_1 and subtracting, we obtain the system

$$\sum_{i=2}^{t} g_j(x_i)(y_1 g(y_i) - y_i g(y_1)) = 0 \quad 1 \le j \le n$$

This system has fewer terms than $(3(d)2)$, so if at least one of the terms is not zero we have the desired contradiction.

5. Otherwise

$$y_1 g(y_i) - y_i g(y_1) = 0 \quad 2 \le i \le t$$

(Note all other possible terms, $i = 1$ and $i > t$, are known to be 0.) Thus

$$y_1 y_i^{-1} = g\left(y_1 y_i^{-1}\right)$$

and this is true for all $g \in G$. Thus $y_1 y_i^{-1} \in L^G$ for $2 \le i \le t$. Let $y_1 y_i^{-1} = z_i^{-1} \in L^G$.

6. Then $y_i = y_1 z_i$, $2 \le i \le t$. If in addition we define $z_1 = 1$ so $y_1 = y_1 z_1$, then $(3(d)2)$ becomes:

$$\sum_{i=1}^{t} g_j(x_i) y_1 z_i = 0 \quad 1 \le j \le n$$

Dividing by the (non-zero) y_1 and taking the equation where $g_j = 1$, we have

$$\sum_{i=1}^{t} z_i x_i = 0$$

But $z_i \in L^G$ and the x_i are linearly lindependent over L^G, so $z_i = 0$ all i, which is not possible since at least $z_1 \neq 0$.

4. If L is finite over K then $\#\Gamma(L:K) \le [L:K]$.

5. We have a useful corollary: If $K \subset L$ is a finite extension and $G = \Gamma(L:K)$ and $H \subset G$ is a subgroup, then

$$\left[L^G : K\right] = \frac{[L:K]}{\#H}$$

6. We've already seen this theorem in action, with the splitting field for $x^3 - 2$ over $\mathbb{Q}$ or the extension $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$.

Where We Are Now

Fix a "ground field" K.

1. Field extensions and algebraic elements. Minimal polynomials. All depend on the choice of ground field.
2. Field homomorphisms and automorphisms. $\Gamma(L:K)$. Fixed fields L^H for $H \subset \Gamma(L:K)$.
3. Splitting field is generated by the roots of one polynomial. Normal extension contains all roots of an irreducible polynomial if it contains one.Finite normal extensions and splitting fields the same.
4. Let $G = \Gamma(L:K)$. Then $\#G = \left[L : L^G\right]$

Homework Due November 17

Stewart 9.1, 9.4, 10.1, 10.2-4

Some Answers

I didn't do a very good job last time on one example. I gave a long, confusing and wrong answer. Two observers made a bet on how it would come out, and the wrong person collected.

1. We want to find the Galois group for the splitting field L of $f = x^4 - 3$ over $\mathbb{Q}$. We will show that this group is isomorphic to D_4, the fourth dihedral group. Let ω be the positive real fourth root of 3.

   (a) $L = \mathbb{Q}(i, \omega)$

      1. The roots of f are ω, $i\omega$, $-\omega$, $-i\omega$, so $L = \mathbb{Q}(\omega, i\omega, -\omega, -i\omega)$. Eliminating redundant generators, we have $L = \mathbb{Q}(\omega, i\omega)$. Since $\frac{i\omega}{\omega} = i$, we have $L = \mathbb{Q}(i, \omega)$.

   (b) $[L : \mathbb{Q}(i)] = 4$

      1. Since $x^4 - 3$ is irreducible over $\mathbb{Q}(i)$ and $L = \mathbb{Q}(i)(\omega)$.

   (c) $[L : \mathbb{Q}] = 8$

      1. $[L : \mathbb{Q}] = [L : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

   (d) $\#\Gamma(L : \mathbb{Q}) = 8$

      1. Because L is a splitting field over $\mathbb{Q}$, L is normal over $\mathbb{Q}$ (and separable because $char(\mathbb{Q}) = 0$) and therefore $\#\Gamma(L : \mathbb{Q}) = [L : \mathbb{Q}] = 8$.

   (e) $\#\Gamma(L : \mathbb{Q}(i)) = 4$

      1. As above, L is normal and separable over $\mathbb{Q}(i)$ because L is normal and separable over $\mathbb{Q}$ and $\mathbb{Q} \subset \mathbb{Q}(i) \subset L$. Thus $\#\Gamma(L : \mathbb{Q}(i)) = [L : \mathbb{Q}(i)] = 4$.

   (f) This is the key point in the argument. Since $L = \mathbb{Q}(i)(\omega)$, if $\sigma_1, \sigma_2 \in \Gamma(L : \mathbb{Q}(i))$ and $\sigma_1(\omega) = \sigma_2(\omega)$ then $\sigma_1 = \sigma_2$.

      1. Every element in L is a polynomial expression in ω with coefficients from $\mathbb{Q}(i)$. We say that $\sigma \in \Gamma(L : \mathbb{Q}(i))$ is *determined by* $\sigma(\omega)$.

   (g) The four elements of $\Gamma(L : \mathbb{Q}(i))$ are given by $\sigma_j(\omega) = i^j\omega$, $j = 0 \ldots 3$. That is $\sigma_0 = id$ and $\sigma_j\sigma_k = \sigma_{(j+k) \bmod 4}$. Note that these maps satisfy $\sigma_j(i) = i$ because these are maps that leave $\mathbb{Q}(i)$ fixed.

      1. We know that there are four automorphisms $\sigma_j \in \Gamma(L : \mathbb{Q}(i))$ and they are determined by four different values $\sigma_j(\omega)$. But $\sigma_j(\omega)^4 = \sigma_j(\omega^4) = \sigma_j(3) = 3$. Thus $\sigma_j(\omega)$ is one of the roots of $x^4 - 3$, and the four possible values are $i^j\omega$, $j = 0 \ldots 3$. NOTE THAT WE DID NOT HAVE TO VERIFY THAT σ_j IS AN AUTOMORPHISM. WE STARTED OUT ASSUMING THAT σ_j WAS AN AUTOMORPHISM AND DEDUCED ITS VALUE ON ω.

   (h) The maps $\sigma_j \in \Gamma(L : \mathbb{Q})$.

      1. Because $\Gamma(L : \mathbb{Q}(i))$ is a subgroup of $\Gamma(L : \mathbb{Q})$.

   (i) Another map in $\Gamma(L : \mathbb{Q})$ is $\tau = conjugation$. Therefore the eight automorphisms in $\Gamma(L : \mathbb{Q})$ are σ_j and $\tau\sigma_j$, $j = 0 \ldots 3$.

   (j) $\Gamma(L : \mathbb{Q})$ is *generated* by $\sigma = \sigma_1$ and τ, elements which satisfy the relations $\sigma^4 = 1$, $\tau^2 = 1$, and $\sigma\tau = \tau\sigma^3$.

1. It is necessary to check only the last relation. We will show $\sigma\tau(\omega) = \tau\sigma^3(\omega)$ and $\sigma\tau(i) = \tau\sigma^3(i)$, which is sufficient to show that $\sigma\tau = \tau\sigma^3$.

$$\begin{aligned}
\sigma\tau(\omega) &= \sigma(\omega) \\
&= i\omega \\
\tau\sigma^3(\omega) &= \tau(-i\omega) \\
&= \tau(-i)\,\tau(\omega) \\
&= i\omega \\
\sigma\tau(i) &= \sigma(-i) \\
&= -i \\
\tau\sigma^3(i) &= \tau(i) \\
&= -i
\end{aligned}$$

(k) $\Gamma(L:\mathbb{Q}) \cong D_4$

1. Because D_4 is a group with two generators satisfying the same relations.

2. We want to find the Galois group for the splitting field L of $f = x^5 - 7$ over $\mathbb{Q}$. The procedure is much the same as above. Let ω be the positive real fifth root of 7.

   (a) $L = \mathbb{Q}(i, \omega)$

      1. Let ζ be a primitive fifth root of 1. The roots of f are $\zeta^j\omega$, $j = 0 \dots 6$. Thus $L = \mathbb{Q}\left(\omega, \zeta\omega, \dots, \zeta^4\omega\right)$. Since $\frac{\zeta\omega}{\omega} = \zeta$, we have $L = \mathbb{Q}(\zeta, \omega)$.

   (b) $[L : \mathbb{Q}(\zeta)] = 5$

      1. Since $x^5 - 7$ is irreducible over $\mathbb{Q}(\zeta)$ and $L = \mathbb{Q}(\zeta)(\omega)$.

   (c) $[L : \mathbb{Q}] = 20$

      1. $[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ because ζ is the root of the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$.

   (d) $\#\Gamma(L : \mathbb{Q}) = 20$

      1. Because L is a splitting field over $\mathbb{Q}$, L is normal over $\mathbb{Q}$ (and separable because $char(\mathbb{Q}) = 0$) and therefore $\#\Gamma(L : \mathbb{Q}) = [L : \mathbb{Q}] = 20$.

   (e) $\#\Gamma(L : \mathbb{Q}(\zeta)) = 5$

      1. As above, L is normal and separable over $\mathbb{Q}(\zeta)$ because L is normal and separable over $\mathbb{Q}$ and $\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset L$. Thus $\#\Gamma(L : \mathbb{Q}(\zeta)) = [L : \mathbb{Q}(\zeta)] = 5$.

   (f) This is the key point in the argument. Since $L = \mathbb{Q}(\zeta)(\omega)$, if $\sigma_1, \sigma_2 \in \Gamma(L : \mathbb{Q}(\zeta))$ and $\sigma_1(\omega) = \sigma_2(\omega)$ then $\sigma_1 = \sigma_2$.

      1. Every element in L is a polynomial expression in ω with coefficients from $\mathbb{Q}(\zeta)$. We say that $\sigma \in \Gamma(L : \mathbb{Q}(\zeta))$ is *determined by* $\sigma(\omega)$.

   (g) The five elements of $\Gamma(L : \mathbb{Q}(\zeta))$ are given by $\sigma_j(\omega) = \zeta^j\omega$, $j = 0 \dots 4$. That is $\sigma_0 = id$ and $\sigma_j\sigma_k = \sigma_{(j+k) \bmod 5}$. Note that these maps satisfy $\sigma_j(\zeta) = \zeta$ because these are maps that leave $\mathbb{Q}(\zeta)$ fixed.

      1. We know that there are five automorphisms $\sigma_j \in \Gamma(L : \mathbb{Q}(\zeta))$ and they are determined by five different values $\sigma_j(\omega)$. But $\sigma_j(\omega)^5 = \sigma_j\left(\omega^5\right) = \sigma_j(7) = 7$. Thus $\sigma_j(\omega)$ is one of the roots of $x^5 - 7$, and the five possible values are $\zeta^j\omega$, $j = 0 \dots 4$. NOTE THAT WE DID NOT HAVE TO VERIFY THAT σ_j IS AN AUTOMORPHISM. WE STARTED OUT ASSUMING THAT σ_j WAS AN AUTOMORPHISM AND DEDUCED ITS VALUE ON ω.

   (h) The maps $\sigma_j \in \Gamma(L : \mathbb{Q})$.

      1. Because $\Gamma(L : \mathbb{Q}(\zeta))$ is a subgroup of $\Gamma(L : \mathbb{Q})$.

   (i) Similarly $L = \mathbb{Q}(\zeta)(i)$ and $\Gamma(L : \mathbb{Q}(\omega))$ is a subgroup of $\Gamma(L : \mathbb{Q})$. There are four such maps τ_k, $k = 1 \cdots 4$, and they are determined by their values $\tau_k(\zeta)$. Since $\tau_k(\zeta)$ is conjugate to ζ, $\tau_k(\zeta) = \zeta^{2^k}$ gives the four distinct maps.and $\tau_4 = identity$.because $2^4 = 16 = 1 \mod 5$. These maps satisfy $\tau_j(\omega) = \omega$.and $\tau_j = \tau_1^j$.

   (j) $\Gamma(L : \mathbb{Q})$ is *generated* by $\sigma = \sigma_1$ and $\tau = \tau_1$, elements which satisfy the relations $\sigma^5 = 1$, $\tau^4 = 1$, and $\sigma\tau = \tau\sigma^3$.

      1. It is necessary to check only the last relation. We will show $\sigma\tau(\omega) = \tau\sigma^3(\omega)$ and $\sigma\tau(\zeta) =$

$\tau\sigma^3(\zeta)$, which is sufficient to show that $\sigma\tau = \tau\sigma^3$.

$$\begin{aligned}
\sigma\tau(\omega) &= \sigma(\omega) \\
&= \zeta\omega \\
\tau\sigma^3(\omega) &= \tau\left(\zeta^3\omega\right) \\
&= \tau\left(\zeta^3\right)\tau(\omega) \\
&= \tau(\zeta)^3\,\omega \\
&= \left(\zeta^2\right)^3\omega \\
&= \zeta\omega \\
\sigma\tau(\zeta) &= \sigma\left(\zeta^2\right) \\
&= \zeta^2 \\
\tau\sigma^3(\zeta) &= \tau(\zeta) \\
&= \zeta^2
\end{aligned}$$

Automorphisms, Normal Closures and Separability

Algebraic Closures

1. I think life will be much simpler if we accept a true but difficult theorem: every field K has an algebraic closure $\bar{K}$, that is a field algebraic over Ksuch that, if $[L:K]<\infty$ then there exists a (not-necessarily unique) commutative diagram

$$\begin{array}{ccc} L & \longrightarrow & \bar{K} \\ & \nwarrow \quad \nearrow & \\ & K & \end{array}$$

   (a) $\bar{K}$ is unique up to non-unique isomorphism.

      1. In fact $\Gamma\left(\bar{K}:K\right)$ is a group called the *absolute Galois group* of K. Usually this is a huge group.
      2. If $K\longrightarrow L$ is a homomorphism of fields, then there exists an homomorphism $\bar{K}\longrightarrow\bar{L}$ such that the following diagram commutes:

$$\begin{array}{ccc} \bar{K} & \longrightarrow & \bar{L} \\ \uparrow & & \uparrow \\ K & \longrightarrow & L \end{array}$$

         1. If $K\longrightarrow L$ is bijective, then so is $\bar{K}\longrightarrow\bar{L}$.
         2. In fact, if L is algebraic over K then $\bar{K}\longrightarrow\bar{L}$ is bijective.

      3. **Example**: $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. $\Gamma\left(\mathbb{C}:\mathbb{R}\right)=\{id,conjugation\}\cong\dfrac{\mathbb{Z}}{(2)}$.

   (b) $\bar{K}$ is algebraically closed: *i.e.* if $f\in\bar{K}[t]$ then f splits over $\bar{K}$.

      1. Let $f=f_0+f_1t+\cdots+t^n$. Then f_i are algebraic over K so $L=K\left(f_0,\ldots,f_{n-1}\right)$ is a finite extension of K. The polynomial $f\in L[t]$ so it has a splitting field M over L which is finite over L and therefore finite over K. A copy of M, containing all the roots of f, can be found in $\bar{K}$, and so f splits in $\bar{K}$. This is the descent argument again.

2. Let $K\subset L\subset M\subset\bar{K}$. It is obvious that we have a map $\hom_K\left(M,\bar{K}\right)\longrightarrow\hom_K\left(L,\bar{K}\right)$. What is not obvious is that this map is surjective.

   (a) **Proof:** if $\sigma\in\hom_K(L:\bar{K})$, then there exists a map $\hat{\sigma}:\bar{K}\longrightarrow\bar{K}$ giving a commutative diagram:

$$\begin{array}{ccc} \bar{K} & \xrightarrow{\hat{\sigma}} & \bar{K} \\ \uparrow & & \uparrow \\ L & \xrightarrow{\sigma} & \sigma(L) \end{array}$$

   $\hat{\sigma}$ restricts to a map $\sigma_1\in\hom_K\left(M,\bar{K}\right)$ that is a pull-back of σ.

$$\begin{array}{ccc} \bar{K} & \xrightarrow{\hat{\sigma}} & \bar{K} \\ \uparrow & & \uparrow \\ M & \xrightarrow{\sigma_1} & \sigma_1(M) \\ \uparrow & & \uparrow \\ L & \xrightarrow{\sigma} & \sigma(L) \end{array}$$

   (b) **Terminology:** we say that σ_1*lifts* the map σ.

3. Let K be a field and let $\alpha\in\bar{K}$. The K*-conjugates of* α are the roots of the minimal polynomial for α over K in $\bar{K}$.

   (a) α is a K-conjugate of α.

(b) α is separable over K if and only if the number of K-conjugates of α is equal to the degree of the minimal polynomial for α over K., which is the same as saying that the minimal polynomial of α has no multiple roots.

(c) Let $\alpha, \beta \in \bar{K}$. Then α and β are K-conjugate if and only if there exists $\sigma \in \Gamma\left(\bar{K} : K\right)$ such that $\sigma(\alpha) = \beta$.

1. **Proof**: if $f \in K[t]$ is the minimal polynomial for α, then f is the minimal polynomial for $\sigma(\alpha) = \beta$ so β is conjugate to α.Conversely, we have an isomorphism $K(\alpha) \xrightarrow{\tau} K(\beta)$ and thus an isomorphism $\overline{K(\alpha)} \xrightarrow{\sigma} \overline{K(\beta)}$ such that the following diagram commutes:

$$\begin{array}{ccc} \overline{K(\alpha)} & \xrightarrow{\sigma} & \overline{K(\beta)} \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{\tau} & K(\beta) \\ \nwarrow & & \nearrow \\ & K & \end{array}$$

Since $\bar{K}$ is the algebraic closure of $K(\alpha)$ and $K(\beta)$, σ is the desired isomorphism.

Joins

1. Suppose $K \subset L_1, L_2 \subset \bar{K}$. Then the *join of* L_1 *and* L_2, denoted L_1L_2 is the smallest subfield of $\bar{K}$ containing both L_1 and L_2. It is unique and generated by all products $\alpha\beta$, $\alpha \in L_1$ and $\beta \in L_2$.

   (a) If $L_1$and L_2 are splitting fields of polynomials f_1 and f_2, then L_1L_2 is a splitting field of f_1f_2

   (b) If $L_1$and L_2 are finite normal extensions of K, then L_1L_2 is a finite normal extension of K

   (c) This all extends to finite sets of subfields of $\bar{K}$ over K

Normal Closure

1. Let $\alpha_1, \ldots \alpha_n \in \bar{K}$, and suppose this set is closed under taking of conjugates over K. Then $f = \prod_{i=1}^{n}(t - \alpha_i) \in K[t]$ and $K(\alpha_1, \ldots, \alpha_n)$ is the splitting field for f.

2. Let $K \subset L \subset \bar{K}$ be a finite extension. Then there is a minimal normal extension M of K containing L called the normal closure of L over K. It is generated by the conjugates of a generating set for L over K.

   (a) M is the join of $\left\{\sigma(L) : \sigma \in \Gamma\left(\bar{K} : K\right)\right\}$.

3. An algebraic extension $K \subset M \subset \bar{K}$ is normal if and only if, for all $\sigma \in \hom_K\left(M, \bar{K}\right)$, $\sigma(M) \subset M$. In that case $\sigma(M) = M$ for all σ.

   (a) **Proof:** Every element of $\sigma(M)$ is conjugate to an element of M. If M is normal over K then $\sigma(M) \subset M$ for all $\sigma \in \hom_K\left(M, \bar{K}\right)$. Conversely, if M is not normal, there exists $\alpha \in M$ with a K-conjugate $\beta \notin M$. Then there is a map $\sigma : M \longrightarrow \bar{K}$ with $\sigma(\alpha) = \beta$, so $\sigma(M) \nsubseteq M$.
   If, M is normal and for some σ, $\sigma(M) \neq M$, then $\sigma(M) \subsetneqq M$. Thus $\sigma^{-1}(M) \supsetneqq M$, a contradiction.

   (b) **Corollary:** for any extension $K \subset M$, $\Gamma(M : K) \subset \hom_K(M, \bar{K})$. M is normal over K if and only if $\hom_K(M, \bar{K}) = \Gamma(M : K)$.

4. If $K \subset L$ is a finite extension and $\sigma \in \hom_K\left(L, \bar{K}\right)$. Then $\sigma(L)$ is contained in the normal closure M of L.

   (a) **Proof:** lift σ to a map $\sigma_1 : M \longrightarrow \bar{K}$. Then $\sigma_1(M) = M$ so $\sigma(L) \subset M$.

5. Let $K \subset L$ be a finite extension. Then $\hom_K\left(L, \bar{K}\right)$ is finite.

   (a) **Proof**: Let M be the finite normal closure of L over K. Then $\hom_K\left(M, \bar{K}\right) = \Gamma(M : K)$ is a finite group, and the natural map $\Gamma(M : K) \longrightarrow \hom_K\left(L, \bar{K}\right)$ is surjective.

Separable Algebraic Extensions

1. An irreducible polynomial in $K[t]$ is separable if and only if it factors into distict linear factors in $\bar{K}[t]$. However we can say more for non-separable irreducible polynomials. All irreducible polynomials can be written a particularly regular way. Let $p>0$ be the characteristic of K. If $f \in K[t]$ is irreducible, then $f = g\left(t^{p^r}\right)$ for a separable polynomial $g \in K[t]$. If $\deg g = n$ then the distinct roots of f are $\alpha_1, \ldots, \alpha_n$ where $\alpha_i^{p^r}$ are the distinct roots of g.

   (a) **Proof**: Construct a sequence of polynomials $f_0 = f$, $f_{i+1}(t^p) = f_i(t)$. The sequence continues until we encounter f_r such that $Df_r \neq 0$. Then $f = f_r\left(t^{p^r}\right)$ and f_r is separable.

2. **Lemma**: let $K \subset L \subset M \subset \bar{K}$. Then $\#\hom_L\left(M:\bar{K}\right)\#\hom_K(L:\bar{K}) = \#\hom_K\left(M:\bar{K}\right)$

   (a) **Proof**: Choose a normal closure N/K for M, so we have $K \subset L \subset M \subset N$. Moreover, $\hom_K\left(N,\bar{K}\right) = \Gamma(N:K)$ and $\hom_M\left(N,\bar{K}\right) = \Gamma(N:M)$. We have a commutative diagram of finite sets, some of which are finite groups:

$$\begin{array}{ccccc}
\Gamma(N:M) & \xrightarrow{id} & \Gamma(N:M) & & \\
\downarrow a' & & \downarrow b' & & \\
\Gamma(N:L) & \xrightarrow{c'} & \Gamma(N:K) & \xrightarrow{c} & \hom_K\left(L,\bar{K}\right) \\
\downarrow a & & \downarrow b & & \downarrow id \\
\hom_L\left(M,\bar{K}\right) & \xrightarrow{d'} & \hom_K\left(M,\bar{K}\right) & \xrightarrow{d} & \hom_K\left(L,\bar{K}\right)
\end{array}$$

   First consider the horizontal maps.

   1. The top and middle rows consist of groups and group homomorphisms
   2. The bottom row is a sequence of sets.
   3. c' is $1-1$, c is onto, and $\{\sigma : d(\sigma) = id_L\} = im(c')$
   4. d' is $1-1$, d is onto, and $\{\sigma : d(\sigma) = id_L\} = im(d')$

   Now consider the vertical maps:

   1. a' and b' are injective group homomorphisms
   2. a and b are onto
   3. $\{\sigma : a(\sigma) = id_M\} = im(a')$
   4. $\{\sigma : b(\sigma) = id_M\} = im(b')$

   We will show

   1. $\#\Gamma(N:L) = \#\Gamma(N:M)\,\#\hom_L\left(M,\bar{K}\right)$
   2. $\#\Gamma(N:K) = \#\Gamma(N:M)\,\#\hom_K\left(M,\bar{K}\right)$
   3. $\#\Gamma(N:K) = \#\Gamma(N:L)\,\#\hom_K\left(L,\bar{K}\right)$

   The desired conclusion $\#\hom_L\left(M:\bar{K}\right)\#\hom_K(L:\bar{K}) = \#\hom_K\left(M:\bar{K}\right)$ follows immediately.

   Each of these statements is says the same thing about a tower of three fields where the top field is normal over the bottom, so we will prove the first. For each $\rho \in \hom_L\left(M,\bar{K}\right)$ I claim that $a^{-1}(\rho)$ is a right coset of $\Gamma(N:M)$ in $\Gamma(N:L)$. This proves the result.

   1. If $\sigma,\tau \in \Gamma(N:L)$ and $a(\sigma) = a(\rho)$ then $\sigma|_M = \tau|_M$ so $\tau^{-1}\sigma|_M = id_M$ and $\tau^{-1}\sigma \in \Gamma(N:M)$. Thus σ and τ are in the same right coset of $\Gamma(N:M)$.
   2. If $\sigma, t \in \Gamma(N:L)$ are in the same right coset of $\Gamma(N:M)$.then for some $\rho \in \Gamma(N:M)$ we have $\sigma = \tau\rho$. Then $\sigma|_M = \tau\rho|_M = \tau|_M$ or $a(\sigma) = a(\tau)$.

3. Let $\alpha \in \bar{K}$. Then $\#\hom_K\left(K(\alpha),\bar{K}\right) \leq [K(\alpha):K]$ with equality holding if and only if α is separable over K.

   (a) **Proof:** $\#\hom_K\left(K(\alpha),\bar{K}\right)$ is the number of conjugates of α in $\bar{K}$, and $[K(\alpha):K]$ is the degree of the minimal polynomial of α over K.

4. Let $[L:K]<\infty$. Then $\#\hom_K\left(L,\bar{K}\right)\leq[L:K]$, and L is separable over K if and only if $\#\hom_K\left(L,\bar{K}\right)=[L:K]$.

   (a) **Proof**: We proceed by induction on $[L:K]$, the statement being obvious if $[L:K]=1$. Let $\alpha\in L\tilde{}\ K$. If $K(\alpha)=L$ we are done by the previous result. Otherwise assume $K\subsetneqq K(\alpha)\subsetneqq L$. We first show the inequality. By the previous result, $\#\hom_K\left(K(\alpha),\bar{K}\right)\leq[K(\alpha):K]$. By induction, $\#\hom_{K(\alpha)}\left(L,\bar{K}\right)\leq[L:K(\alpha)]$. Going up two results, we have

$$\begin{aligned}\#\hom_k\left(L,\bar{K}\right) &= \#\hom_{K(\alpha)}\left(L,\bar{K}\right)\#\hom_K\left(K(\alpha),\bar{K}\right)\\ &\leq [L:K(\alpha)]\,[K(\alpha),K]\\ &= [L:K].\end{aligned}$$

   Now we proceed to the second statement. If L is separable over K then L is separable over $K(\alpha)$ and $K(\alpha)$ is separable over K so by the previous argument $\#\hom_K\left(L,\bar{K}\right)=[L:K]$.
   Suppose $\#\hom_K\left(L,\bar{K}\right)=[L:K]$. Then, since $\#\hom_k\left(L,\bar{K}\right)=\#\hom_{K(\alpha)}\left(L,\bar{K}\right)\#\hom_K\left(K(\alpha),\bar{K}\right)$ and $\#\hom_K\left(K(\alpha),\bar{K}\right)\leq[K(\alpha):K]$ and $\#\hom_{K(\alpha)}\left(L,\bar{K}\right)\leq[L:K(\alpha)]$, we have $\#\hom_K\left(K(\alpha),\bar{K}\right)=[K(\alpha):K]$ and $\#\hom_{K(\alpha)}\left(L,\bar{K}\right)=[L:K(\alpha)]$. By induction, $K(\alpha)$ is separable over K and L is separable over $K(\alpha)$, so L is separable over K.

   (b) **Corollary:** if $K\subset L\subset M\subset\bar{K}$ and $[M:K]<\infty$ then M is separable over K if and only if M is separable over L and L is separable over K.

      1. **Proof:** We have that

$$\begin{aligned}[M:K] &= [M:L]\,[L:K]\\ \#\hom_K\left(M,\bar{K}\right) &= \#\hom_L\left(M,\bar{K}\right)\#\hom_K\left(L,\bar{K}\right)\end{aligned}$$

         Moreover each factor on the top is not less than the corresponding factor on the bottom. Thus the right sides are equal if and only if the corresponding terms on the left are equal. QED

   (c) **Corollary:** if $a\in\bar{K}$ is separable over K, then $K(a)$ is separable over K.

      1. **Proof:** By (3) if a is separable over K then $[K(a):K]=\#\hom_K(K(a):K)$.

   (d) **Corollary:** if $a_1,\ldots,a_n\in\bar{K}$ are separable over K, then $K(a_1,\ldots,a_n)$ is separable over K.

      1. **Proof:** a_{i+1} is separable over $K(a_1,\ldots,a_i)$ because its minimal polynomial over $K(a_1,\ldots,a_i)$ divides its minimal polynomial over K. Therefore the minimal polynomial of a_{i+1} over $K(a_1,\ldots,a_i)$ cannot have multiple roots. By the second corollary, $K(a_1,\ldots,a_{i+1})$ is separable over $K(a_1,\ldots,a_i)$. By the first corollary, $K(a_i,\ldots,a_n)$ is separable over K.

   (e) **Corollary:** the set of elements in $\bar{K}$ separable over K form a field denoted $\bar{K}_{sep}$, the separable algebraic closure of K. If $K\subset L$ then $L_{sep}=L\cap\bar{K}_{sep}$ is a field containing K.

5. Suppose $K\subset L\subset\bar{K}$ and $[L:K]<\infty$. Then L is normal and separable over K if and only if $\#\Gamma[L:K]=[L:K]$

   (a) **Proof**: If L is normal and separable, use (4) and (3*b*) . To go backwards, note in general $\#\Gamma[L:K]\leq\#\hom_K\left(L,\bar{K}\right)\leq[L:K]$. If the first two are equal, L is normal over K, and if the second and third are equal then L is separable over K.

6. Suppose $K\subset L\subset\bar{K}$ and $[L:K]<\infty$. Let $G=\Gamma(L:K)$. Then L is normal and separable over K if and only if $L^G=K$.

   (a) **Proof:** L is normal and separable over K if and only if $\#\Gamma[L:K]=[L:K]$. But in general $\#\Gamma[L:K]=\left[L:L^G\right]$, so L is normal and separable over K if and only if $[L:K]=\left[L:L^G\right]$,which holds if and only if $K=L^G$.

David Harbater's Talk

Dr. Habater's talk at MSRI covered a lot of topics. I want to distill them for you. We are going to follow one of his threads, Galois extensions of $\mathbb{C}(t)$, for our last topic of the semester.

We will adopt Harbater's notation for algebraic closure. The algebraic closure of K will henceforth be denoted by $\bar{K}$ rather than $\hat{K}$.

1. Given a field K, the inverse Galois problem is to determine all finite groups that appear as Galois groups for extensions of K.
   (a) We need only consider finite, normal, separable extensions. These are called *Galois* extensions.
2. The inverse Galois problem is solved in three cases (at least):
   (a) If K is a finite field, then the Galois groups over K are the finite cyclic groups
   (b) If $K = \mathbb{C}(t)$, the every finite group is a Galois group
      1. This is proven by the theory of topological covering spaces and fundamental groups together with the Riemann Existence Theorem
   (c) If $K = \bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) then every finite group is a Galois group over $\bar{\mathbb{Q}}(t)$
      1. This is proven by "theory of descent" from $\mathbb{C}(t)$ to $\bar{\mathbb{Q}}(t)$.
3. Two conjectures:
   (a) If K is a field, then every finite group is a Galois group over $K(t)$
   (b) Every finite group is a Galois group over $\mathbb{Q}$
4. The Hilbert rigidity theorem says that every Galois group over $\mathbb{Q}$ is a galois group over $\mathbb{Q}(t)$, and conversely.
   (a) So to study Galois groups over $\mathbb{Q}$, it suffices to study them over $\mathbb{Q}(t)$.
5. For every group G we can find a finite extension $\mathbb{Q} \subset K$ and a finite extension $K(t) \subset L$ such that $G \cong \Gamma(L : K(t))$.
   (a) This follows from the fact that every finite group is a Galois group over $\bar{\mathbb{Q}}(t)$
   (b) If we could elimimate the extension K we would have that every group is a galois group over $\mathbb{Q}(t)$ and therefore over $\mathbb{Q}$
6. It is known that if the group G is "rigid" (and most but not all finite groups are rigid), then G is a Galois group over $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n^{th} root of unity.
   (a) Often we can then show that G is a Galois group over $\mathbb{Q}$

Review of normal and separable

1. **Definition:** a finite field extension $K \subset L$ or L/K is *Galois* if it is normal and separable.
2. Suppose $K \subset L$ is a finite extension
   (a) If $G = \Gamma(L : K)$ then $\#G = \left[L : L^G\right]$
   (b) There exists a minimal normal extension M/K containing L. This is the *normal closure* of L/K.
   (c) $\Gamma(L : K) \subset \hom_K\left(L, \bar{K}\right)$, and L/K is a normal extension if and only if $\Gamma(L : K) = \hom_K\left(L, \bar{K}\right)$
   (d) $\#\hom_K\left(L, \bar{K}\right) \leq [L : K]$, and L/K is a separable extension if and only if $\#\hom_K\left(L, \bar{K}\right) = [L : K]$
   (e) L/K is Galois if and only if $\#\Gamma(L : K) = [L : K]$ if and only if $K = L^{\Gamma(L:K)}$.

(f) If $K \subset M \subset L$ then the natural map $\hom_K\left(L, \bar{K}\right) \longrightarrow \hom_K\left(M, \bar{K}\right)$ is surjective, and $\hom_M\left(L, \bar{K}\right) \subset \hom_M\left(L, \bar{K}\right)$ is the set of elements that map to id_M.

1. If L/K is Galois then L/M is Galois and $\Gamma(L:K) \longrightarrow \hom_K\left(M, \bar{K}\right)$ is surjective, and $\Gamma(L:M) \subset \Gamma(L:K)$ is the set of elements that map to id_M.
2. If L/K and M/K are both Galois we have the exact sequence:

$$1 \longrightarrow \Gamma(L:M) \longrightarrow \Gamma(L:K) \longrightarrow \Gamma(M:K) \longrightarrow 1$$

Fundamental Theorem of Galois Theory

Finally

1. Suppose L/K is a Galois extension. Here's what we already know.
   (a) $\#\Gamma(L:K) = [L:K]$
   (b) Every subgroup $H \subset \Gamma(L:K)$ corresponds to a subfield $K \subset L^H \subset L$
   (c) Every subfield $K \subset M \subset L$ corresponds to a subgroup $\Gamma(L:M) \subset \Gamma(L:K)$
2. The pairing between subfields and subgroups is *perfect:* every subfield corresponds to a different subgroup, every subgroup corresponds to a different subfield
   (a) Going back and forth gets you back where you started: This proves that the pairing is perfect.
      1. $H = \Gamma\left(L : L^H\right)$ for every subgroup $H \subset \Gamma(L:K)$
         1. Therefore $\#H = \left[L : L^H\right]$
      2. $M = L^{\Gamma(L,M)}$ for every field $K \subset M \subset L$
         1. Therefore $[L:M] = \#\Gamma(L:M)$
   (b) All this is pretty easy to prove. Let's work on (i). For any field extension we have $H \subset \Gamma\left(L : L^H\right)$. But since L/K is Galois, L/L^H is Galois and $\#\Gamma\left(L : L^H\right) = \left[L : L^H\right] = \#H$. The last equality follows from (3).
   To prove (ii), we know that $M \subset L^{\Gamma(L,M)}$. But $\left[L : L^{\Gamma(L,M)}\right] = \#\Gamma(L:M) = [L:M]$.
3. If $K \subset L \subset M$ and M/K is normal, we have an *exact sequence:*

$$1 \longrightarrow \Gamma(L:M) \longrightarrow \Gamma(L:K) \longrightarrow \Gamma(M:K) \longrightarrow 1$$

   (a) so $\Gamma(M:K) \cong \dfrac{\Gamma(L:K)}{\Gamma(L:M)}$.
   (b) **Proof:** All three extensions M/K, L/K, and L/M are normal, so $\hom_K(M, \bar{K}) = \Gamma(M:K)$, $\hom_K(L, \bar{K}) = \Gamma(L:K)$, and $\hom_M(L, \bar{K}) = \Gamma(L:M)$.. The maps

$$\hom_M\left(L, \bar{K}\right) \longrightarrow \hom_K\left(L, \bar{K}\right) \longrightarrow \hom_K(M, K)$$

   become:

$$\Gamma(L:M) \longrightarrow \Gamma(L:K) \longrightarrow \Gamma(M:K)$$

   where the first map is injective, the second surjective, and the kernal of the second is the image of the first.
   (c) **Corollary:** If M/K is normal then $\Gamma(L:M)$ is a normal subgroup of $\Gamma(L:K)$, because it is the kernal of a homomorphism.
4. Normal subgroups correspond to normal extensions M/K, (Since L/K is separable, every subextension $K \subset M \subset L$ is separable over K and so M/K will be normal if and only if M/K is Galois.)

(a) **Lemma:** Suppose $\tau \in \Gamma(L:K)$ and $K \subset M \subset L$. Then $\Gamma(L:\tau(M)) = \tau\Gamma(L:M)\tau^{-1}$.

1. **Proof:** If $\sigma \in \Gamma(L:M)$ and $m \in M$ then $\tau\sigma\tau^{-1}(\tau(m)) = \tau\sigma(m) = \tau(m)$ so $\tau\sigma\tau^{-1} \in \Gamma(L:\tau(M))$ and $\tau\Gamma(L:M)\tau^{-1} \subset \Gamma(L:\tau(M))$. The opposite inclusion follows immediately by replacing τ with τ^{-1}: $\tau^{-1}\Gamma(L:\tau(M))\tau \subset \Gamma\left(L:\tau^{-1}\tau(M)\right) = \Gamma(L:M)$.

(b) **Proof of 4:** Suppose H is a normal subgroup of $\Gamma(L:K)$. To show that L^H/K is normal, we will show that $\Gamma\left(L^H:K\right) = \hom_K\left(L^H,\bar{K}\right)$. We know that $\Gamma\left(L^H:K\right) \subset \hom_K\left(L^H,\bar{K}\right)$. If $\tau \in \hom_K\left(L^H,\bar{K}\right)$ then $\tau H\tau^{-1} = H$ and so $\Gamma\left(L:L^H\right) = \Gamma\left(L:\tau\left(L^H\right)\right)$ as subgroups of $\Gamma(L:K)$. Since subgroups of $\Gamma(L:K)$ are paired with subfields between K and L, we have $\tau\left(L^H\right) = L^H$ and $\tau \in \Gamma\left(L^H:K\right)$.
The converse is proven above.

Galois' Application of Galois Theory–Unsolvable Equations

I don't want to take the time necessary to do this carefully. You can read about it in Stewart. Here's the basic idea. Let's assume we are working over a field K of characteristic 0. Galois worked over $\mathbb{Q}$.

1. A polynomial $f \in K[t]$ can be *solved by radicals* if there are some elements $a_i \in K$ and integers n_i such that the splitting field M/K for f is a subfield of the splitting field L/K for $\prod_i (t-a_i)^{n_i}$. We call L a *radical extension .*

2. The Galois group for a normal, radical extension (like L) has the property that it is *solvable:*

   (a) there exists a sequence of subgroups $(1) \subset H_0 \subset H_1 \subset \cdots \subset H_n = \Gamma(L:K)$ where H_i is a normal subgroup of H_{i+1} and H_{i+1}/H_i is abelian (or, what comes to the same thing, cyclic).

   (b) The quotient of a solvable group is solvable, and $\Gamma(M:K)$ is a quotient of $\Gamma(L:K)$, so if a polynomial can be solved by radicals then its Galois group (the Galois group of its splitting field) is solvable.

3. Conversely, any Galois extension with a solvable Galois group can be imbedded in a radical extension, so if the Galois group of a polynomial is solvable, then the polynomial can be solved by radicals.

4. There are unsolvable groups, the smallest is A_5, the even elements of the permutation group S_5.

5. There are equations whose Galois groups is A_5, so there are equations that cannot be solved by radicals.

Chapter 7

Galois Theory over $\mathbb{C}(t)$

Much of the material in this chapter is taken from Völklein, *Groups as Galois Groups,* Cambridge University Press, Cambridge, England, 1996.

Laurent series and their algebraic closure

1. The ring of power series over $\mathbb{C}$, denoted $\mathbb{C}[[t]]$, consists of all sequences $(c_i)_{i\geq 0}$ of complex numbers.
   (a) We think of these series as including the variable t. A typical series in $\mathbb{C}[[t]]$ is $\sum_{i=0}^{\infty} c_i t^i$.
   (b) The series form an integral domain, a commutative ring with identity and no zero divisors.
      1. Series can be added term by term and multiplied in the obvious way by combining powers of t.
      2. If $c = \sum_{i=0}^{\infty} c_i t^i \in \mathbb{C}[[t]]$ then $ord_t(c) = \min\{i : c_i \neq 0\}$.
         1. $ord_t c = \infty$ if and only if $c = 0$
         2. If $ord_t c \neq ord_t c$ then $ord_t(c+d) = \min(ord_t c, ord_t d)$. In general, $ord_t(c+d) \geq \min(ord_t c, ord_t d)$.
         3. $ord_t(cd) = (ord_t c) + (ord_t d)$
      3. A series c is invertible if and only $ord_t c = 0$.
         1. The inverse of $\sum_{i=0}^{\infty} c_i t^i = c_0\left(1 + \sum_{i=1}^{\infty}\left(c_0^{-1}c_i\right)t^i\right)$ is $c_0^{-1}\left(\sum_{j=0}^{\infty}(-1)^j\left(\sum_{i=1}^{\infty}\left(c_0^{-1}c_i\right)t^i\right)^j\right)$.
      4. If $s > 0$ then the functions analytic in the disk $|z| < s$ form a subring $R_s \in \mathbb{C}[[t]]$.
         1. If $s_1 < s_2$ then $R_{s_1} \supset R_{s_2}$
         2. $R = \cup_{s>0} R_s$ is a subring of $\mathbb{C}[[t]]$, the subring of functions analytic is some neighborhood of 0. This is called the ring of *germs* of analytic functions at 0.
         3. $R \neq \mathbb{C}[[t]]$. There are power series that converge on no neighborhood of 0, e.g. $\sum_{n=0}^{\infty} n! t^n$.
2. The ring of Laurent series over $\mathbb{C}$, denoted $\Lambda = \mathbb{C}((t))$, consists of all sequences $(c_i)_{i\geq n}$ for some $n \in \mathbb{Z}$. We write $c = \sum_{i=n}^{\infty} c_i t^i$.
   (a) Negative indices are allowed, but each Laurent series has at most a finite number of negatively indexed terms.
   (b) Laurent series form a field containing $\mathbb{C}$.
      1. Laurent series are the quotient field of the integral domain $\mathbb{C}[[t]]$.
   (c) The *ord* function extends to $\mathbb{C}((t))$ with the same properties.
      1. If $c \in \mathbb{C}((t))$, $c \neq 0$, then $ord_t\left(c^{-1}\right) = -ord_t c$.

3. So we have

$$\begin{array}{ccccccc} & & & & \mathbb{C}(t) & & \\ & & & \nearrow & & \searrow & \\ \mathbb{C} & \longrightarrow & \mathbb{C}[t] & & & & \mathbb{C}((t)) \\ & & & \searrow & & \nearrow & \\ & & & & \mathbb{C}[[t]] & & \end{array}$$

4. There is are homomorphisms, obtained by setting $t = 0$

$$\begin{array}{ccccc} \mathbb{C}[t] & & \longrightarrow & & \mathbb{C}[[t]] \\ & \searrow & & \swarrow & \\ & & \mathbb{C} & & \end{array}$$

   These are left inverses to the inclusions $\mathbb{C} \subset \mathbb{C}[t]$ and $\mathbb{C} \subset \mathbb{C}[[t]]$.

   (a) In both cases the kernal is the ideal generated by t.

5. If $a = a_0 + a_1 t + \cdots \in \mathbb{C}[[t]]$ and $a_0 \neq 0$ then $a^{1/e}$ has e possible values in $\mathbb{C}[[t]]$

   (a) Let $a^{1/e} = b_0 + b_1 t + b_2 t^2 + \cdots$. Then

$$\begin{aligned} a &= \left(b_0 + b_1 t + b_2 t^2 + \cdots\right)^e \\ &= b_0^e + e b_0^{e-1} b_1 t + \left(\binom{e}{2} b_0^{e-2} b_1^2 + e b_0^{e-1} b_2\right) t^2 + \cdots \end{aligned}$$

   There are e possible values for b_0, and for each choice of b_0 the other values $b_1, b_2, \ldots$ follow.

6. Want more. Here's another field:. Let e be a positive integer. $\Delta_e = \mathbb{C}\left(\left(t^{1/e}\right)\right)$ is the collection of power series $\sum_{i=n}^{\infty} c_i t^{i/e}$. There are called the *fractional Laurent series* .

   (a) Abstractly $\Delta_e = \mathbb{C}\left(\left(t^{1/e}\right)\right) \cong \mathbb{C}((t)) = \Lambda$, but we prefer to think $\mathbb{C}((t)) \subset \mathbb{C}\left(\left(t^{1/e}\right)\right)$

   (b) If $e \,|\, f$ then $\mathbb{C}\left(\left(t^{1/e}\right)\right) \subset \mathbb{C}\left(\left(t^{1/f}\right)\right)$, $\Delta_e \subset \Delta_f$, and conversely since $\Delta_e \subset \Delta_f$ implies $t^{1/e} = \left(t^{1/f}\right)^m$ or $f = em/$

      1. So $\Delta_3 \subset \Delta_6$ but $\Delta_3 \nsubseteq \Delta_7$
      2. However, for any positive integers e and f , $\Delta_e \subset \Delta_{ef} \supset \Delta_f$.
         1. The "union" of all the fields Δ_e is $\mathbb{C}\left(\left(t^{1/\infty}\right)\right) = \Delta_\infty$
         2. Our goal is to show that $\Delta_\infty = \bar{\Lambda}$, the algebraic closure of $\Lambda = \mathbb{C}((t))$. This result is originally due to Newton.

   (c) $[\Delta_e : \Lambda] = e$ and is a Galois extension since it is the splitting field of $y^e - t$, whose roots are $\zeta_e^i t^{1/e}$, $i = 0 \cdots e-1$. Clearly $t^{1/e} \in \Delta_e$ and $\zeta_e \in \mathbb{C}$.

      1. $\Gamma(\Delta_e : \Lambda) = \dfrac{\mathbb{Z}}{(e)}$ a cyclic extension. The subgroups of these group correspond to the positive divisors f of e, which in turn correspond to the intermediate fields $\Lambda \subset \Delta_f \subset \Delta_e$. Do lattice for Δ_{12}.

7. The following are all different: $\mathbb{C}[x,t] = \mathbb{C}[x][t]$, $\mathbb{C}[[x,t]] = \mathbb{C}[[x]][[t]]$, $\mathbb{C}[[t]][x]$ and $\mathbb{C}[x][[t]]$.

   (a) We care going to consider $\mathbb{C}[[t]][x]$

      1. For example $\cos t + (\sin t)\, x - e^t x^2$
      2. We might ask for a solution to $x^2 - \sin t = 0$, which might or might not exist in $\mathbb{C}[[t]]$ or $\mathbb{C}((t))$.
         1. Actually no solution x can exist, because $ord_t\left(x^2\right) = 2$ $ord_t x = 1$

2. There might be some hope for solving $x^2 - \cos t = 0$

$$\begin{aligned} x &= c_0 + c_1 t + c_t t^2 + \cdots \\ x^2 &= c_0^2 + (2c_0 c_1)\, t + \left(2c_0 c_2 + c_1^2\right) t^2 + \cdots \\ \cos t &= 1 - \frac{1}{2}t^2 + \frac{1}{24}t^4 + \cdots \\ c_0 &= 1 \\ c_1 &= 0 \\ c_2 &= -\frac{1}{4} \\ & \text{etc.} \end{aligned}$$

(b) Actually, there might be some hope to solving $x^2 = \sin t$. Consider $y^2 = \sin\left(t^2\right) = t^2 - \frac{t^6}{3!} + \frac{t^{10}}{5!} - \cdots$

1. $y = t + a_2 t^2 + a_3 t^3 + \cdots$
2. $y^2 = t^2 + 2a_2 t^3 + \left(2a_3 + a_2^2\right) t^4 + \cdots$ so

$$\begin{aligned} 2a_2 &= 0 \\ 2a_3 + a_2^2 &= 0 \\ & \textit{etc.} \end{aligned}$$

We can solve for a_i, and then $\sqrt{\sin t} = t^{1/2} + a_2 t + a_3 t^{3/2} + \cdots \in \Delta_2$.

3. Another approach is to note that $\frac{\sin t}{t} = 1 - \frac{t^2}{3!} + \frac{t^4}{5!} = \cdots$ has a square root power series, and $\sqrt{\sin t} = \sqrt{t}\sqrt{\frac{\sin t}{t}}$

8. If $F \in \mathbb{C}[[t]][x]$, $\deg_x F = n$, then $F = F_0 + F_1 t + F_2 t^2 + \cdots$ with $F_i \in \mathbb{C}[x]$ and $\deg F_i \leq n$.

(a) If F is monic of degree n then

1. F_0 is monic of degree n
2. $\deg F_i < n$ for $i > 0$

(b) We have a homomorphism $\mathbb{C}[[t]][x] \longrightarrow \mathbb{C}[x]$ given by $F \longrightarrow F_0$.

9. **Lemma; Let** $F \in \mathbb{C}[[t]][x]$ be monic in x and suppose $F_0 = gh$ for $g, h \in \mathbb{C}[x]$ *with no common factors*. There there exist monic polynomials $G, H \in \mathbb{C}[[t]][x]$ such that $GH = F$ and $G_0 = g$ and $H_0 = h$. That is, the factorization $F_0 = gh$ can be lifted to a factorization $F = GH$.

(a) Proof is in Völklein, pp 28-29

(b) Example $F = x(x-1) + tx + t^2(x-1) + t^3 x + t^4(x-1) + \cdots$

1. $F_0 = x(x-1)$. $g = x$, $h = x - 1$.
2. $G = x + G_1 t + G_2 t^2 + \cdots$, $H = (x-1) + H_1 t + H_2 t^2 + \cdots$
3. The problem is to find $G_i, H_i \in \mathbb{C}[x]$ of bounded degree such that $GH = F$
   1. $(x-1)G_1 + xH_1 = x$ so take $H_1 = 1$, $G_1 = 0$
   2. $(x-1)G_2 + G_1 H_1 + xH_2 = (x-1)$ so take $G_2 = 1$, $H_2 = 0$
   3. etc.

10. **Corollary:** let $F \in \mathbb{C}((t))[x]$ and suppose

(a) F is monic and $\deg_x F = n > 1$

(b) $F_0 = a_0 + a_1 x + \cdots + a_{n-2} x^{n-2} + x^n \in \mathbb{C}[x]$

(c) $F_0 \neq x^n$

Then F is reducible.

Proof: $F_0 = \prod_{i=1}^{n}(x - r_i)$. Since $F_0 \neq x^n$ at least one $r_i \neq 0$, and since $a_{n-1} = -\sum_{i=1}^{n} r_i = 0$ not all the r_i are equal. Thus we can split the product into two parts with no common factor:

$$\begin{aligned} F_0 &= gh \\ g &= \prod_{i \in I}(x - r_i) \\ h &= \prod_{i \in \{1 \ldots n\} \tilde{} I}(x - r_i) \end{aligned}$$

Thus $F = GH$ where $G_0 = g$ and $F_0 = f$.

11. **Theorem (**well-known and not proven here). Let $[L : K]$ be a finite separable field extension. Then $L = K(a)$ for some $a \in L$. That is, L is a simple extension of K.

12. **Theorem :** Let $[L : \mathbb{C}((t))] < \infty$. Then $L \cong \Delta_e$ for $e = [L : \mathbb{C}((t))]$

    (a) The proof needs a lemma.

13. **Lemma (Newton):** if $F \in \mathbb{C}[[t]][x]$ then F has a root in Δ_e for some e.

(a) Example:

$$\begin{aligned} F &= x^2 - 2(\cos t)\, x + e^t \\ x &= \frac{2\cos t + \sqrt{4\cos^2 t - 4e^t}}{2} \\ &= \cos t + \sqrt{\cos^2 t - e^t} \end{aligned}$$

The power series are:

$$\begin{aligned} \cos t &= 1 - \frac{t^2}{2} + \frac{t^4}{4!} - \cdots \\ \cos^2 t &= 1 - t^2 + \left(\frac{2}{4!} + \frac{1}{4}\right) t^4 + \cdots \\ e^t &= 1 + t + \frac{t^2}{2} + \cdots \\ \cos^2 t - e^t &= -t - \frac{3t^2}{2} + \cdots \\ &= t\left(-1 - \frac{3t}{2} + \cdots\right) \\ \sqrt{\cos^2 t - e^t} &= \sqrt{t}\,(\pm i + ?t + \cdots) \end{aligned}$$

so the solutions are in Δ_2.

(b) Show that (13) suffices to prove (**??**). By (11), $L = \mathbb{C}((t))(\theta)$ for some $\theta \in L$. Let f be the minimal polynomial of L. Write

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

where $f_i \in \mathbb{C}((t))$. Thus

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = 0$$

Multiplying by a high power of t, we have

$$\begin{aligned} 0 &= t^{mn}\theta^n + (t^{mn}a_{n-1})\,\theta^{n-1} + \cdots + (t^{mn}a_0) \\ &= (t^m\theta)^n + t^m a_{n-1}(t^m\theta)^{n-1} + t^{2m}a_{n-2}(t^m\theta)^{n-2} + \cdots + (t^{mn}a_0) \end{aligned}$$

Choosing m sufficiently large, we can assume that $t^{im}a_{n-i} \in \mathbb{C}[[t]]$ for $1 \le i \le n$. Since $L = \mathbb{C}((t))(\theta) = \mathbb{C}((t))(t^m\theta)$, the minimal polynomial for $t^m\theta$ has the same degree as the minimal polynomial for θ. Thus

$$F = x^n + (t^m a_{n-1})\,x^{n-1} + \cdots + (t^{mn}a_0) \in \mathbb{C}[[t]][x]$$

is the minimal polynomial for $t^m\theta$. That is, any finite extension L of $\mathbb{C}((t))$ is a generating element θ whose minimal polynomial F is in $\mathbb{C}[[t]][x]$.

By (13), one of the roots of F (possibly but not necessarily θ) is in Δ_{e_1} for some e_1. Call this root φ. Then $\mathbb{C}((t))[\varphi] \subset \Delta_{e_1}$ so $\mathbb{C}((t))[\varphi] = \Delta_{e_2}$ for some $e_2 \mid e_1$. Moreover, $L \cong \Delta_{e_2}$ because both fields are simple extensions with the same minimal polynomial.

(c) Now to prove (13). Among all the polynomials failing to satisfy (13), choose F of minimal degree. It will be convenient to change our convention and write

$$F = x^n + a_1(t)\,x^{n-1} + \cdots + a_{n-1}(t)\,x + a_n(t)$$

where $a_i(t) \in \mathbb{C}[[t]]$.

Then $\deg F > 1$, and F is irreducible. Replacing F by $F\left(x - \frac{a_1(t)}{n}\right)$ we can assume that $a_1(t) = 0$. Since F is irreducible, $F_0 = x^n$. That is, $ord_t a_i > 0$ for $2 \leq i \leq n$. At least one $a_i \neq 0$ or $F = x^n$ and is reducible.

For $a_i \neq 0$, define $\mu_i = ord_t a_i$. Then $\mu_i > 0$. Let $\mu = \min\left\{\frac{\mu_i}{i}\right\}$. The points $\left(i, \frac{\mu_i}{i}\right)$ form the *Newton polygon,* and the line from the origin with slope μ lies below the polygon and touches at least one vertex We have $\mu \in \mathbb{Q}$, $\mu > 0$. Write $\mu = \frac{d}{e}$ for positive integers d and e with no common factors.

Let $\tau = t^{1/e}$ and consider the polynomial:

$$\begin{aligned} F^*(x) &= \tau^{-dn} F\left(\tau^d x\right) \\ &= x^n + a_2\tau^{-2d}x^{n-2} + a_3\tau^{-3d}x^{n-3} + \cdots + a_n\tau^{-nd} \\ &\in \Delta_e[x] \end{aligned}$$

The non-zero coefficients satisfy $ord_t(a_i\tau^{-id}) = \mu_i - \frac{i}{e}d \geq i\frac{d}{e} - i\frac{d}{e} = 0$, and for at least one i, $ord_t\left(a_i\tau^{-id}\right) = 0$. Thus $F^*(x) \in \mathbb{C}[[\tau]][x]$. is a monic polynomial of degree n such that F_0^* has degree n, the coefficient of x^{n-1} is zero, and $F_0^* \neq y^n$. Therefore, by (10), F^* is reducible. Note that $\Delta_e = \mathbb{C}((\tau))$. By the minimality of the degree of F, one of the factors of F^* (and therefore F^* itself) has a root in $\Delta_e\left(\tau^{1/f}\right) = \Delta_{ef}$. Thus F has a root in Δ_{ef}.

How Fractional Power Series are Computed and Used

Throughout this section, upper-case letters represent variables and lower-case letters represent values. I want to show you how fractional power series are used to analyze the singularities on an algebraic curve.

An old but thorough reference for this topic is Walker, *Algebraic Curves,* Dover.

1. Suppose we have a polynomial in two variables with complex coefficients:

$$\begin{aligned} f(T,X) &\in \mathbb{C}[T,X] \\ f(T,X) &= \sum \alpha_{ij} T^i X^j \\ &= \sum_{i=0}^{n} a_i(T) X^i \end{aligned}$$

   (a) Dividing by a_n we have

$$F(X) = \sum_{i=0}^{n} b_i(T) X^i \in \mathbb{C}(T)[X] \subset \mathbb{C}((T))[X]$$

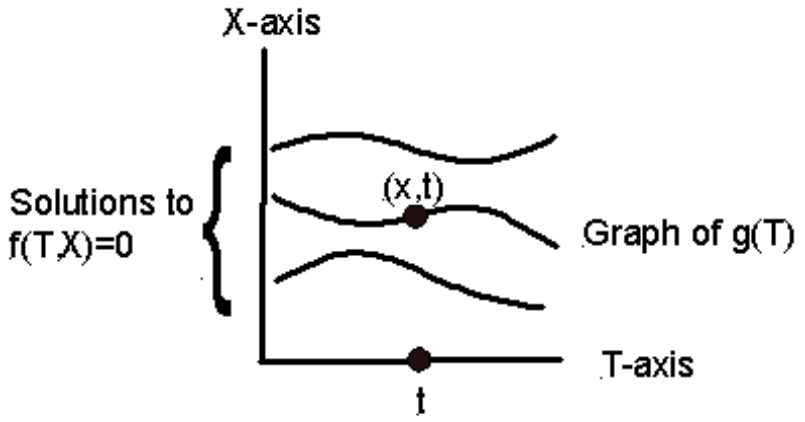
2. Sometimes we think of X as a *multi-valued function* of T.

   (a) Most simply, when T is given a value $t \in \mathbb{C}$, then X has n possible values.

      1. Possibly not all the values are distinct
      2. Possibly there are fewer possible values if $a_n(t) = \cdots = a_i(t) = 0$

   (b) **The Implicit Function Theorem:** if $x, t \in \mathbb{C}$ are such that $f(x,t) = 0$ and if $\frac{\partial f}{\partial X}(x,t) \neq 0$ then there exists a neighborhood U of t, $U \subset \mathbb{C}$, and an analytic function $g(T)$ defined on U such that $g(t) = x$ and such that $f(g(s), s) = 0$ for all $s \in U$.

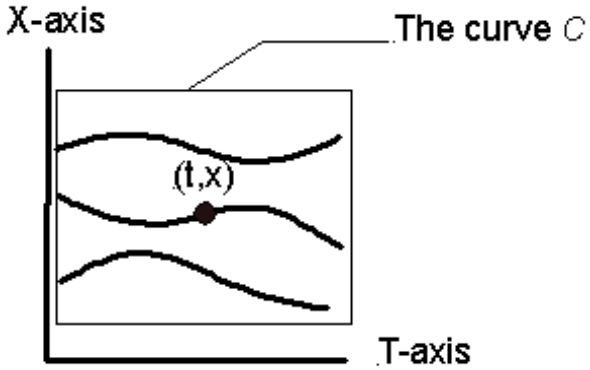
      1. The idea is that $X = g(T)$ is a solution to $f(X,T) = 0$
      2. The graphis of the solutions x to $F(X,T) = 0$ form n sheets above the T-plane. The graph of $g(T)$ coincides with one of those sheets.



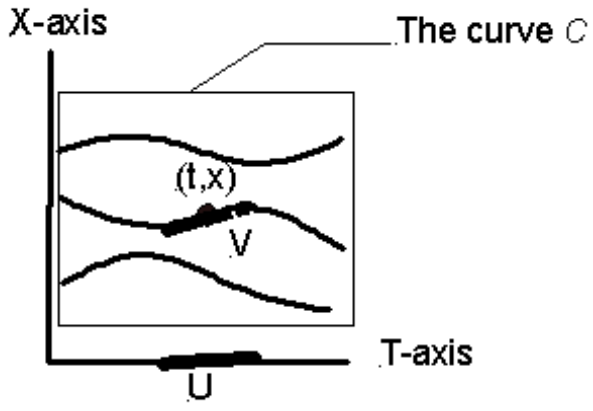
3. In modern mathematics, "multi-valued function" is an oxymoron

   (a) However, we can consider the set of point $f(t,x)=0$ in $\mathbb{C}^2$. This is an *algebraic curve*.$C \subset \mathbb{C}^2$

   (b) There are obvious functions $T : C \longrightarrow \mathbb{C}$ and $X : C \longrightarrow \mathbb{C}$ (the vertical and horizontal projections in the picture)



   (c) Another way to think of the implicit function theorem is to say that, if $\dfrac{\partial f}{\partial X}(t,x) \neq 0$ then there is a neighborhood V of (t,x) on C that maps homeomorphically (by T) to a neighborhood U on the T-axis. The function $g : U \longrightarrow X$-axis in the implicit function theorem is just $X \circ T^{-1}$ where $T^{-1} : U \longrightarrow V$.

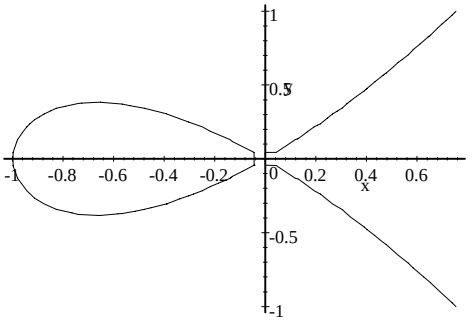


4. Let's suppose we have shifted coordinates so that $t = 0$

(a) The inverse function theorem says, if $\frac{\partial f}{\partial X}(0,x) \neq 0$, that $g(T)$ is an analytic function on a neighborhood of 0

(b) Newton's theorem says, without any hypotheses, that the function $g(T)$ is a fractional power series.defining a function whose graph coincides with the algebraic curve C in a neighborhood of $(0,x)$.

5. For an algebraic curve C defined by an equation $F(T,X)=0$, the important question is this: given a point $(t,x) \in C$, is there a neighborhood of the point homeomorphic to a neighborhood of $0 \in \mathbb{C}$.



$$t^3 - x^2 + t^2 = 0$$

6. At any point *except* $(0,0)$ the curve is locally homeomorphic to $\mathbb{C}$

(a) The picture shows only the real part, so the curve in the picture is locally homeomorphic to $\mathbb{R}$ everywhere except $(0,0)$

(b) But at $(0,0)$ the curve is not locally homeomorphic to $\mathbb{C}$ because it crosses itself.

7. If the point has a neighborhood homeomorphic to $\mathbb{C}$, we say that it is a *non-singular* point (or *smooth* point) on the curve. Otherwise it is a *singular* point on the curve.

(a) By the implicit function theorem, if $\frac{\partial f}{\partial X}(t,x) \neq 0$ then the projection T maps a neighborhood of (t,x) homeomorphically to a neighborhood of t in $\mathbb{C}$, so if $\frac{\partial f}{\partial X}(t,x) \neq 0$ then the point (t,x) is non-singular.

1. Switching variables, if $\frac{\partial f}{\partial T}(t,x) \neq 0$, then the point (t,x) is non-singular.

(b) So if the point (t,x) is singular then $\frac{\partial f}{\partial X}(t,x) = \frac{\partial f}{\partial T}(t,x) = 0$. This condition is also sufficient, and sometimes serves as a defnition of "singular".

1. Then it applies to any curve $F(T,X)=0$ where $F \in K[T,X]$ for any field K.

(c) In the example:a singular point would have to satisfy three equation, the equation for the curve and the two partial derivatives:

$$\begin{aligned} f(T,X) &= T^3 - X^2 + T^2 = 0 \\ \frac{\partial f}{\partial T}(T,X) &= 3T^2 + 2T = 0 \\ \frac{\partial f}{\partial X}(T,X) &= 2X = 0 \end{aligned}$$

The only solution is $(0,0)$.

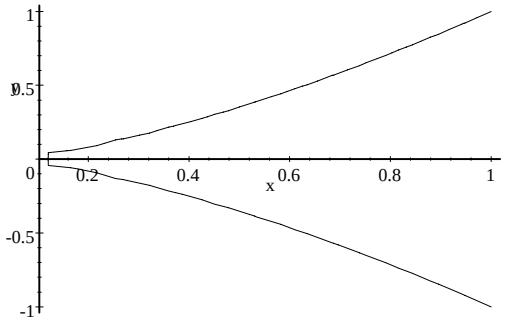
8. Let's assume that the point $(0,0)$ is on our curve.

(a) If $(0,0)$ is non-singular, then at least one of the variables can be written as a power series in terms of the other on the curve

1. That is, if $\dfrac{\partial f}{\partial X}(0,0) \neq 0$ then we can formally solve the equation $f(T,X)=0$ with a power series $X = a_1T + a_2T^2 + \cdots$.
2. If (t,x) is a point on the curve near $(0,0)$ then $x = a_1t + a_2t^2 + \cdots$ as a convergent sum of complex numbers
3. Sometimes we say we have *parametrized* the curve, because each point (t,x)—at least in a neighborhood of 0—is a function of the parameter t.

(b) If $(0,0)$ is singular, then each variable is a fractional power series of the other.

1. Example



$$x^2 - t^3 = 0$$

In this example, the only singular point is $(0,0)$, and there $x = t^{3/2}$

1. This is only a formal solution, not a parametrization of the curve in a neighborhood of $(0,0)$ because the function $t \longrightarrow t^{3/2}$ does not map a neighborhood of 0 to a neighborhood of 0. The function is not analytic at 0.

2. In our first example $x = \pm t\sqrt{1+t} = \pm\left(t + \dfrac{1}{2}t^2 + \cdots\right)$,

1. Here the two solutions define two curves in a neighborhood of 0. The singularity has two *branches*, each of which is the graph of an analytic (but not a polynomial) function.
2. Each branch is smooth.

9. In general, given an algebraic curve one may want to find its singularities and then analyze each one.

(a) To analyze a singularity, we divide it into branches and analyze each branch

(b) The knottiest singularities are those that cannot be separated into branches.

Problems due December 6

1. Let $a \in \mathbb{C}[[t]]$ have a non-zero constant term. Verify carefully that a is invertible.

   (a) Extend this result to show that every non-zero Laurent series $\alpha \in \mathbb{C}((t))$ is invertible

2. Find a simple description of $\mathbb{C}(t) \cap \mathbb{C}[[t]]$

3. Show, using power series, that $\left(e^{x/2}\right)^2 = e^x$.

4. Find a fractional power series for $\sqrt{\tan x}$, or at least find the first few terms.

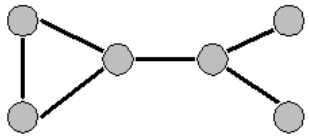
5. Prove that every non-trivial ideal in $\mathbb{C}[[t]]$ is generated by a power of t.

Chapter 8

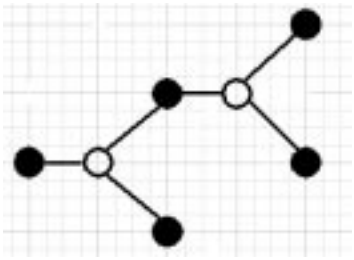
Final Exam

You may ask questions during the exam.

1. Can the graph below be a dessin? Why or why not.

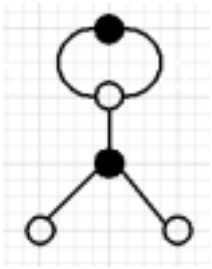


2. In the following dessin, filled vertices are above 0 and open vertices are above 1.



   (a) Is this the dessin for a polynomial or a rational function? How do you know?
   (b) If it is the dessin of a polynomial, what is the degree of the polynomial?

3. In the following dessin, filled vertices are above 0 and open vertices are above 1.



   Suppose the function for the dessin is $\frac{f}{g}$ where $f, g \in \mathbb{C}[x]$ and f, g have no common factors.

   (a) What are the degrees of f and g
   (b) Is this a clean dessin? Why or why not?
   (c) Find the generators σ_0 and σ_1 for the monodromy group of this dessin.
   (d) What is the genus of this dessin.

4. Here is a clean dessin, showing only the vertices above 0.

   (a) If you added the vertices above 1, where would they go?
   (b) What is degree of the mapping for this dessin?
   (c) Can you find the function for this dessin?

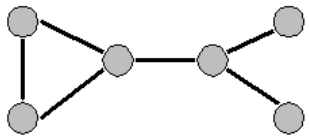
5. Give an example of a Riemann surface other than $\mathbb{P}^1_{\mathbb{C}}$.
6. Give an example of a dessin with genus greater than 0.
7. Consider $f \in \mathbb{Q}[x]$, $f = x^5 - 9x^4 + 12x^3 - 3x^2 - 9x + 3$
   (a) Show that f is irreducible.
   (b) If θ is a root of f and $L = \mathbb{Q}[\theta]$, what is $[L : \mathbb{Q}]$?
   (c) How many fields M can you find with $\mathbb{Q} \subsetneqq M \subsetneqq L$?
8. Give examples of two field extensions of $\mathbb{Q}$, both of degree 4, one that is Galois and one that is not.
   (a) What is the Galois group of your Galois extension.
9. Find the degree of the splitting field L of $x^3 - 2$ over $\mathbb{Q}$.
   (a) Show that the Galois group of this splitting field is not abelian.
10. Let $f \in \mathbb{C}((t))[x]$, $f = x^3 - tx^2 + t^2\, x - 1$. Is f irreducible over $\mathbb{C}((t))$? How do you know?
11. Let $f \in \mathbb{C}((t))[x]$, $f = x^2 - t\, x - 1$. Use the quadratic formula to find the roots of f in $\mathbb{C}((t))$.
12. What is the Galois group of $\Delta_e = \mathbb{C}\left(\left(t^{1/e}\right)\right)$ over $\mathbb{C}((t))$?
13. True or false: every finite extension of $\mathbb{C}((t))$ is Galois..

Chapter 9

Final Exam Answers

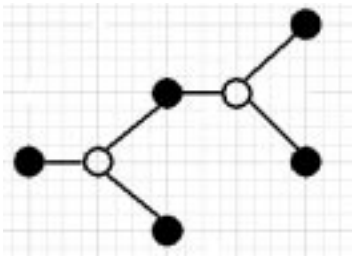
You may ask questions during the exam.

1. Can the graph below be a dessin? Why or why not.



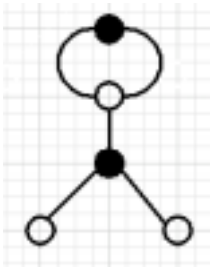
   The graph cannot be a dessin, becaue the triangle at the left end cannot be bi-colored.

2. In the following dessin, filled vertices are above 0 and open vertices are above 1.



   (a) Is this the dessin for a polynomial or a rational function? How do you know?
   This is the dessin of a polynomial because it is a tree.
   (b) If it is the dessin of a polynomial, what is the degree of the polynomial?
   The degree of the polynomial six, the number of edges in the dessin.

3. In the following dessin, filled vertices are above 0 and open vertices are above 1.



   Suppose the function for the dessin is $\frac{f}{g}$ where $f, g \in \mathbb{C}[x]$ and f, g have no common factors.

   (a) What are the degrees of f and g
   The denominator g has degree 1 because there is one poly of multiplicity 1 in the cycle at the top of the dessin. The function as a whole has degree 5, because there are five edges, so the numerator f has degree 5.

(b) Is this a clean dessin? Why or why not?
The dessin is not clean because the white vertices are not all of valence 2.

(c) Find the generators σ_0 and σ_1 for the monodromy group of this dessin.
I've numbered the edges. In terms of these numbers, $\sigma_0 = (1,2)(3,4,5)$ and $\sigma_1 = (1,2,3)$

(d) What is the genus of this dessin.
Since the dessin can be drawn on the plane, it's genus is 0. Also,

$$\begin{aligned} g &= 1 - \frac{k_0 + k_1 + k_\infty - N}{2} \\ &= 1 - \frac{3+2+2-5}{2} \\ &= 0 \end{aligned}$$

4. Here is a clean dessin, showing only the vertices above 0.

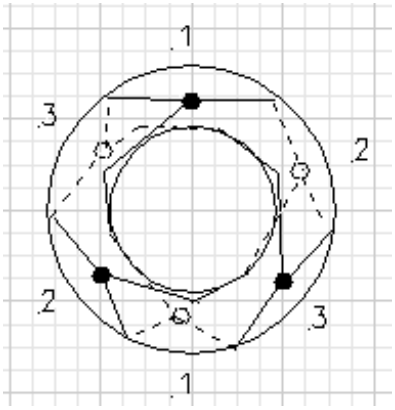
(a) If you added the vertices above 1, where would they go?
In the middle of each edge

(b) What is degree of the mapping for this dessin?
The degree is 4, the number of edges after the vertices above 1 are added.

(c) Can you find the function for this dessin?
The function is $4x^2\left(1-x^2\right)$ from class notes.

5. Give an example of a Riemann surface other than $\mathbb{P}^1_{\mathbb{C}}$.
The algebraic curve $x^3 + y^3 = 1$ has genus 1

6. Give an example of a dessin with genus greater than 0.
Here's the dessin of the function x^3 on the curve above:



7. Consider $f \in \mathbb{Q}[x]$, $f = x^5 - 9x^4 + 12x^3 - 3x^2 - 9x + 3$

(a) Show that f is irreducible.

The polynomial is irreducible by Eisenstein's criterion with $p = 3$.

(a) If θ is a root of f and $L = \mathbb{Q}[\theta]$, what is $[L : \mathbb{Q}]$?
$[L : \mathbb{Q}] = 5$, the degree of the polynomial

(b) How many fields M can you find with $\mathbb{Q} \subsetneqq M \subsetneqq L$?
There are no fields M as required, because the degree of the extension $M/\mathbb{Q}$ would have to be greater than 1 and a proper divisor of 5.

8. Give examples of two field extensions of $\mathbb{Q}$, both of degree 4, one that is Galois and one that is not.

   A non-Galois extension is the simple extension $\mathbb{Q}[\theta]$ where θ is a root of the irreducible polynomial x^4-2. A Galois extension is $\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right] = \mathbb{Q}\left[\sqrt{2}+\sqrt{3}\right]$. We know that the second extension is Galois because all conjugates of its generators, namely $\pm\sqrt{2}$ and $\pm\sqrt{3}$, are in the extension.

   (a) What is the Galois group of your Galois extension.

   The Galois group is isomorphic to $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}$, The Galois group action on the field extension is exchanging $\pm\sqrt{2}$ and $\pm\sqrt{3}$.

9. Find the degree of the splitting field L of x^3-2 over $\mathbb{Q}$.

   The degree is 6, since $L = \mathbb{Q}\left[\sqrt[3]{2}, .\zeta_3\right]$ and $\left[\mathbb{Q}\left[\sqrt[3]{2}\right] : \mathbb{Q}\right] = 3$ and $\left[L : Q\left[\sqrt[3]{2}\right]\right] = 2$.

   (a) Show that the Galois group of this splitting field is not abelian.

   One way to think of L is as $L = \mathbb{Q}[\omega_1, \omega_2, \omega_3]$ where ω_i are the roots of $t^3-2=0$. There are six elements in the Galois group, and each element permutes these roots. Moreover, it two elements of the Galois group permute the roots in the same way, then the elements are equal. Thus the Galois group must correspond to the full permutation group of these three roots, or S_3, which is a non-abelian group.

10. Let $f \in \mathbb{C}((t))[x]$, $f = x^3 - tx^2 + t^2\,x - 1$. Is f irreducible over $\mathbb{C}((t))$? How do you know?

    f is not irreducible. $f_0 = x^3-1$ factors into distinct factors over $\mathbb{C}$, so f factors over $\mathbb{C}((t))$ by Hensill's lemma.

11. Let $f \in \mathbb{C}((t))[x]$, $f = x^2 - t\,x - 1$. Use the quadratic formula to find the roots of f in $\mathbb{C}((t))$

    The roots are

$$\begin{aligned} x &= \frac{t \pm \sqrt{t^2+4}}{2} \\ &= \frac{t}{2} \pm \sqrt{1+\left(\frac{t}{2}\right)^2} \\ &= \pm \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{t^{2i}}{4^i} + \frac{t}{2} \end{aligned}$$

    We know from homework that $.\sqrt{1+\left(\frac{t}{2}\right)^2}$ can be expanded into a power series.

12. What is the Galois group of $\Delta_e = \mathbb{C}\left(\left(t^{1/e}\right)\right)$ over $\mathbb{C}((t))$?

    The Galois group is the cyclic group $\frac{\mathbb{Z}}{(e)}$ The generator of the group can be taken to be the galois map that sends $t^{1/e} \longrightarrow \zeta_e t^{1/e}$

13. True or false: every finite extension of $\mathbb{C}((t))$ is Galois.

    True, because every finite extension is (isomorphic to) Δ_e, which is a cyclic Galois extension of $\mathbb{C}((t))$.