MATH 4820/5820-3: EXAMPLE PROJECT 5
DEFINING THE GENUS AND FORMING
THE GALOIS GROUP OF A HOMOGENEOUS POLYNOMIAL

PROF. MICHAEL D. FRIED, OFFICE MATH. DEPT. #223

A homogeneous polynomial p defines a curve in $\mathbb{CP}^2$. Each *point* has the form

$$\{t(x',y',z'),\ x',y',z' \text{ not all } 0, \text{ and } p(x',y',z')=0 \mid 0\neq t\in\mathbb{C}\}.$$

Refer to the collection of such points as C_p. This project describes one of the most famous results due to Riemann. The project won't attempt to prove it, just state it. A key tool for a proof – or solid understanding – is in §22.7, the *Fundamental group*. We won't do much directly on Chap. 22.

1. p defines a map $C_p \to \mathbb{CP}^1$

In class we discussed how $p(x,y,z)$, of degree n, gives a map:

$$C_p \to \mathbb{CP}^1 \text{ by } (x',y',z') \mapsto (x',z').$$

We need two things to make this work.

(1.1a) $p(x,y,z)$ actually involves y; and
(1.1b) $p(x,y,z)$ is irreducible ($p(x,y,1)=P(x,y)$ is irreducible) over $\mathbb{C}$.

Each $(x',z')\in\mathbb{CP}^1$, is represented by a point in $\{x',1\mid x'\in\mathbb{C}\}\cup\{(1,0)\}$. We just write x', using $x'=\infty$ for $\{(1,0)\}$. In class we discussed $p(x,y,z)=z^nP(y/z)-(x/z))$ with $P(y)$ a degree n polynomial in y.

2. The Puiseux series on C_p for x'

Puiseux expansions with fractional exponent $\frac{1}{m}$ are Lauren series in $(x-x')^{\frac{1}{m}}$:

$$\mathrm{Pu}_{x',m}=\mathbb{C}(((x-x')^{\frac{1}{m}})).\text{Replace } (x-x') \text{ by } 1/x \text{ if } z'=0.$$

Theorem 2.1 (Newton-Puiseux)**.** *There is a minimal integer $m(x')$ if $z'=1$ ($m(\infty)$ if $z'=0$) with this property.*

There are are n different $\{y_1(x),\dots,y_n(x)\}=\boldsymbol{y}$ in $\mathrm{Pu}_{x',m(x')}$, all zeros of $P(x,y)$.

That means $P(x,y(x)_k)\equiv 0$, identically the 0 series, $k=1,\dots,n$.

This project would start by discussing the following topics.

(2.1a) $\cup_{m=1}^{\infty}\mathrm{Pu}_{x',m}$ is an algebraically closed field, different from $\mathbb{C}$.
(2.1b) $\mathrm{Pu}_{x',m(x')}$ is a field containing all n zeros of $P(x,y)$ over $\mathbb{C}(x)$, therefore putting all those zeros in an algebraically closed field for each x'.
(2.1c) Substituting $x^{\frac{1}{m(x')}}\to e^{\frac{2\pi i}{m(x')}}x^{\frac{1}{m(x')}}$ gives a permutation

$$g_{x'} \text{ of } y_1(x),\dots,y_n(x) \text{ of order } m(x').$$

We may regard $g_{x'}$ as an element in S_n. §19.2 and §19.3 of the book discuss permutations as elements of S_n. Only if $m(x') > 1$ is the permutation $g_{x'}$ different from the identify, and there are only finitely many x' for which this holds.

These are x's where $P(x, y)$ and $\frac{\partial P}{\partial y}$ have a common zero (x', y'). This was a specific example of the topic of Bezout's Theorem. Such x' are called *branch points*.

Discuss why there are only finitely many branch points $\boldsymbol{z} \stackrel{\text{def}}{=} x_1, \dots, x_r$.

3. Between Galois and Riemann

Galois says that if you can put all zeros of an irreducible polynomial in one field extension, the smallest field containing them has as many automorphisms as its degree. Also, those automorphisms are determined by their effect on the zeros. Call the group of those automorphisms G_p.

If $h \in G_p$, then you get a new permutation of the $\boldsymbol{y}$, a *conjugate*, by restricting $h \circ g_{x'} \circ h^1$ to $\boldsymbol{y}$. For x_i a branch point, denote the set of conjugates of g_{x_i} by C_{x_i}.

This is a statement of a version of one of Riemann's most famous results that is an *inverse result*, producing curves in $\mathbb{CP}^2$.

Theorem 3.1. *Suppose you are given* $\boldsymbol{x} = \{x_1, \dots, x_r\}$ *and a group* G *and elements* $\boldsymbol{g} = \{g_1, \dots, g_r\}$ *in* G. *Then there is a* $p(x, y, z)$ *with a map* $C_p \to \mathbb{CP}^1$ *that produces such* $\boldsymbol{g}$ *if and only if the following conditions hold:*

(3.1a) $g_1 g_2 \cdots g_r$ *is the identify; and*
(3.1b) $g_1, \dots, g_r$ *generate* G.

4. Definition of the genus of p

For any $g \in S_n$ define its *index* as n minus the number of disjoint cycles in g. p. 408 has examples of elements of S_n and their disjoint cycles.

The genus of the curve $\{(x, y, z) \in \mathbb{CP}^2 \mid p(x, y, x) = 0\}$ is $\mathbf{g}$ where

$$2(n + \mathbf{g} - 1) = \sum_{i=1}^{r} \text{index of } g_i.$$

Suppose $g_1, \dots, g_4$ are conjugates of $(1\,2\,3)$ – called 3-cycles – in A_5, §19.8, the smallest simple group, discovered first by Abel. Denote its conjugacy class by C_3. This consists of all cycles of the form $(i\,j\,k)$ with i, j, k distinct.

Problem 4.1. Show that you can get a genus 0 curve from Riemann's Theorem by choosing $g_i \in \mathrm{C}_3$ to satisfy the conditions of (3.1) with $G = A_5$.[1]

Another Riemann Theorem says that this curve with its map to $\mathbb{CP}^1$ comes from the homogenous version given by a polynomial in two variables $P(y) - x$, as in our class discussion.

E-mail address: michael.fried@Colorado.edu
E-mail address: michaeldavidfried@gmail.com

[1]First you want to show that everything in A_5 can be written as a product of 3-cycles.