Parametric solutions to the generalized Fermat equation

Jody Esmonde

Department of Mathematics and Statistics

McGill University, Montreal

April 1999

A thesis submitted to the Faculty of Graduate Studies and Research

in partial fulfilment of the requirement of the degree of Master of Science

Acknowledgments

I would like to take this opportunity to thank my supervisor Henri Darmon, for all the help and support he has given me during my time at McGill. He was very patient and encouraging, and always found the time to talk with me when I needed help. Several people helped me work out the details of some of the proofs contained in this paper: special thanks go to Ian Stewart, Ram Murty, Jordan Ellenberg, Eyal Goren and Tom Weston.

I would also like to thank the ISM and CICMA for the financial support they provided for the past two years.

Abstract

In this paper we examine parametric solutions to the generalized Fermat equation,

$$x^p + y^q = z^r.$$

Simple criteria are given for the existence of solutions over an algebraically closed field and all such solutions are described. Parametric solutions over non-algebraically closed fields are then considered, along with an investigation of the number of distinct classes of solutions, up to an appropriate notion of equivalence.

Résumé

Dans cette thèse nous examinons les solutions paramétriques de l'équation de Fermat généralisée.

$$x^p + y^q = z^r.$$

Nous donnons deux critères simples d'existence de solutions sur un corps algébriquement clos, ainsi qu'une description complète de l'ensemble de ces solutions. Nous considérons aussi le cas d'un corps non-algébriquement clos.

Contents

1 Introduction

In this paper we examine the generalized Fermat equation, $x^p + y^q = z^r$, for exponents $p, q, r \geq 2$.

Definition 1 *Let F be any field. A triple of polynomials $a(t), b(t), c(t)$ in $F[t]$ is said to be a* parametric solution *to the equation $x^p + y^q = z^r$ if:*

1. *$a(t)^p + b(t)^q = c(t)^r$;*

2. *$a(t), b(t)$ and $c(t)$ are pairwise relatively prime; and*

3. *the degree of each of $a(t), b(t)$ and $c(t)$ is at least 1.*

We will consider *parametric solutions* to this equation over different fields.

The *degree* of a parametric solution $(a(t), b(t), c(t))$ over F is defined to be $\max\{\deg(a(t)^p), \deg(b(t)^q), \deg(c(t)^r)\}$.

We define the *Euler characteristic* $\chi(p, q, r)$ of the equation associated to the triple (p, q, r) by

$$\chi(p, q, r) = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1.$$

The study of the generalized Fermat equation can be separated into three cases:

1. $\chi(p,q,r) < 0$, known as the *hyperbolic* case;

2. $\chi(p,q,r) = 0$, known as the *elliptic* case; and

3. $\chi(p,q,r) > 0$, known as the *spherical* case.

The main goals of this paper are to describe precisely when parametric solutions to the generalized Fermat equation exist, and to understand 'how many' such solutions there are. The answers to these questions depend strongly on the field of definition of the solutions and on the Euler characteristic of the equation.

Chapter 2 gives a necessary and sufficient condition for existence of parametric solutions over algebraically closed fields. Over most algebraically closed fields, parametric solutions exist only to those equations with strictly positive Euler characteristic (the spherical case). The exceptional fields are those with characteristic dividing the degree of a minimal parametric solution. There are only a finite number of triples (p,q,r) with positive Euler characteristic, and we are able to give explicit solutions in these cases. These solutions are obtained by associating a finite group, denoted $\Gamma_{p,q,r}$, to each equation, and exploiting the invariant theory of this group.

The main focus of Chapter 3 is to understand the smallest field in which parametric solutions to the equation $x^p + y^q = z^r$ exist. We examine the more general equation

$$\lambda_1 x^p + \lambda_2 y^q = z^r. \tag{1}$$

and conclude that if there exists some embedding of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(\overline{F})$ which is fixed globally by the Galois group $G_F := Gal(\overline{F}/F)$, then there is a parametric solution to an equation of type (1).

We then show that all parametric solutions over an algebraically closed field are, in some sense, equivalent. This result enables us to relate non-equivalent parametric solutions to Galois cohomology. More specifically, the non-equivalent parametric solutions over F to $x^p + y^q = z^r$ are in natural bijection with a subset of the non-abelian cohomology set $H^1(G_F, \mathrm{Aut}(\Gamma_{p,q,r}))$.

2 Solutions over algebraically closed fields

2.1 Introduction

The main theorem of this chapter is:

Theorem 1 *Let F be an algebraically closed field. Then*

1. *If $\chi(p,q,r) \leq 0$, then the equation $x^p + y^q = z^r$ has no non-trivial parametric solution over F of degree relatively prime to the characteristic of F.*

2. *If $\chi(p,q,r) > 0$, and $N = N(p,q,r) = 2/\chi(p,q,r)$ is relatively prime to $char(F)$, then the equation $x^p + y^q = z^r$ has a parametric solution $(a(t), b(t), c(t))$ of degree N. Any other parametric solution is of the form*

$$\left(a\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(a)}, b\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(b)}, c\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(c)}\right)$$

for some polynomials $g(t), h(t) \in F[t]$, of degree at least one.

The proof of the first part of the theorem is elementary, involving only basic properties of polynomials. The proof of the second part is based on properties of finite subgroups of $\mathbf{PGL_2}(F)$, and their invariant theory.

The Euler characteristic as defined above arises in a natural way in the classification of subgroups of $\mathbf{PGL_2}(F)$. More precisely, each triple of exponents satisfying $\chi(p,q,r) > 0$ (the 'spherical case'), corresponds to a finite

group $\Gamma_{p,q,r} \subseteq \mathbf{PGL_2}(F)$, as follows: $\Gamma_{2,2,r} \simeq D_r$, the dihedral group of order $2r$; $\Gamma_{2,3,3} \simeq A_4$; $\Gamma_{2,3,4} \simeq S_4$; and $\Gamma_{2,3,5} \simeq A_5$.

Given a particular embedding of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(F)$, one can construct a rational function f whose numerator is a pth power and whose denominator is an rth power.

$$f(t) = \frac{a(t)^p}{c(t)^r}.$$

and such that

$$f(t) - 1 = -\frac{b(t)^q}{c(t)^r}.$$

where $a(t)$, $b(t)$, $c(t)$ are relatively prime polynomials.

This, then, gives a parametric solution to the generalized Fermat equation over F. The final step is to show that all primitive parametric solutions of the generalized Fermat equation arise from solutions obtained as above; this proof relies on some basic algebraic geometry and results about coverings of the projective line over F.

2.2 The elliptic and hyperbolic cases

This section establishes part 1 of Theorem 1; namely, that with one small condition, there are no non-trivial primitive parametric solutions to the generalized Fermat equation $x^p + y^q = z^r$, in the elliptic and hyperbolic cases.

Theorem 2 *Let F be any field. If $\chi(p,q,r) \leq 0$, there do not exist non-trivial parametric solutions $(a(t), b(t), c(t))$ over F to the equation $x^p + y^q = z^r$ of degree relatively prime to $charF$.*

Proof: Suppose $(a(t), b(t), c(t))$ is a parametric solution to the equation $x^p + y^q = z^r$. Let N be the maximal degree of $a(t)^p$, $b(t)^q$ and $c(t)^r$, and suppose that N is relatively prime to the characteristic of F. Note that at least two of $a(t)^p$, $b(t)^q$ and $c(t)^r$ must have degree exactly N.

Differentiating the equation

$$a(t)^p + b(t)^q = c(t)^r \tag{2}$$

gives

$$pa(t)^{p-1}a'(t) + qb(t)^{q-1}b'(t) = rc(t)^{r-1}c'(t). \tag{3}$$

Claim: none of $a(t)$, $b(t)$, $c(t)$ have zero derivative.

Proof of Claim: Suppose at least one of $a(t)^p$, $b(t)^q$ and $c(t)^r$ becomes 0 upon differentiation. If $pa(t)^{p-1}a'(t) = 0$, equation (3) becomes

$$qb(t)^{q-1}b'(t) = rc(t)^{r-1}c'(t).$$

Since $b(t), c(t)$ are relatively prime, this implies that $b(t)^{q-1}$ divides $c'(t)$, and $c(t)^{r-1}$ divides $b'(t)$. The degree of each side of this equation is $N-1$, so $\deg(b(t)) = N/q$ and $\deg(c(t)) = N/r$.

If $b(t)^{q-1} \mid c'(t)$, then either $\deg(b(t)^{q-1}) \leq \deg(c'(t))$ or $c'(t) = 0$. In the latter case, $b'(t) = 0$, which implies that $charF$ divides N, contradicting the earlier assumption. So,

$$\deg(b(t)^{q-1}) = \frac{N}{q}(q-1) = N\left(1 - \frac{1}{q}\right) \leq \deg(c'(t)) = \frac{N}{r} - 1,$$

which becomes $N \leq N/q + N/r - 1$, and since $q, r \geq 2$, this is impossible. The same argument can be made to show that $qb(t)^{q-1}b'(t) \neq 0$ and $rc(t)^{r-1}c'(t) \neq 0$. This proves the claim.

Eliminating $a(t)^p$ in equations (2) and (3) gives

$$b(t)^{q-1}[pa'(t)b(t) - qa(t)b'(t)] = c(t)^{r-1}[pa'(t)c(t) - ra(t)c'(t)].$$

At least one of $b(t)^q$ and $c(t)^r$ has degree N; assume that $\deg(c(t)^r) = N$. Since $b(t)$ and $c(t)$ are relatively prime, $c(t)^{r-1}$ divides $pa'(t)b(t) - qa(t)b'(t)$. Hence either $pa'(t)b(t) - qa(t)b'(t) = 0$ or

$$\deg(c(t)^{r-1}) \leq \deg(pa'(t)b(t) - qa(t)b'(t)).$$

Since $a(t)$ and $b(t)$ are relatively prime, $pa'(t)b(t) - qa(t)b'(t) = 0$ implies that $a(t)$ divides $a'(t)$, which is impossible since the degree of $a(t)$ is at least

one. So

$$\begin{aligned}\deg(c(t)^{r-1}) &= \frac{N}{r}(r-1)\\ &\leq \deg(pa'(t)b(t) - qa(t)b'(t))\\ &\leq \frac{N}{p} + \frac{N}{q} - 1.\end{aligned}$$

Rearranging this equation gives

$$\frac{1}{N} \leq \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1,$$

so that $\lambda(p,q,r) > 0$.

If $\deg(c(t)^r) < N$ then $\deg(b(t)^q) = N$, and an analogous argument, beginning with the fact that $b(t)^{q-1}$ divides $pa'(t)c(t) - rc'(t)a(t)$, gives the same result.

Thus, if $\lambda(p,q,r) \leq 0$, the degree of every parametric solution over F to the equation $x^p + y^q = z^r$ is divisible by the characteristic of F. □

The condition on the characteristic of F is a necessary one; to see this, consider a field F of characteristic p. Let $a(t), b(t) \in F[t]$ be two non-constant relatively prime polynomials. Then

$$a(t)^p + b(t)^p = (a(t) + b(t))^p.$$

and the triple $(a(t), b(t), a(t)+b(t))$ is a parametric solution to the generalized Fermat equation $x^n + y^n = z^n$.

2.3 The spherical case

Parametric solutions to the generalized Fermat equation will be obtained by considering the invariant theory of finite subgroups of $\mathbf{PGL_2}(F)$. We begin by exploring some properties of $\mathbf{PGL_2}(F)$ and of its subgroups.

2.3.1 Some facts about $\mathbf{PGL_2}(F)$

Let F be a field. Denote by $\mathbf{GL_2}(F)$ the set of 2×2 invertible matrices with entries in F. Let $\mathbf{SL_2}(F)$ be the subgroup of $\mathbf{GL_2}(F)$ consisting of all matrices with determinant 1.

The group $\mathbf{GL_2}(F)$ acts on $F \cup \{\infty\}$ by the following rule:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot t := \frac{at+b}{ct+d}.$$

with the convention that

$$\frac{a\infty + b}{c\infty + d} = \frac{a}{b}, \quad \text{and} \quad \frac{x}{0} = \infty.$$

This action is not faithful, as the elements

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

give the same fractional linear transformation. To rectify the situation, we take the quotient of $\mathbf{GL_2}(F)$ by its center, which consists of all matrices of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

$\lambda \neq 0$, which we call *scalar* matrices. This new group is called $\mathbf{PGL_2}(F)$. Define also

$$\mathbf{PSL_2}(\overline{F}) = \mathbf{SL_2}(\overline{F})/\pm 1.$$

and

$$\mathbf{PSL_2}(F) = \mathbf{PSL_2}(\overline{F})^{G_F}.$$

the set of elements of $\mathbf{PSL_2}(\overline{F})$ fixed by the Galois group of $\overline{F}/F$.

The following lemmas explore the action of $\mathbf{PGL_2}(F)$ on $\mathbb{P}^1(F)$.

Lemma 1 *Let z_1, z_2 and z_3 be three distinct elements of $\mathbb{P}^1(F)$. For any triple w_1, w_2, w_3 of distinct elements of $\mathbb{P}^1(F)$, there is an element $\gamma \in$*

$\mathbf{PGL_2}(F)$ *such that* $\gamma(z_i) = w_i$.

Proof: Use the equation

$$\frac{(t - z_1)(z_2 - z_3)}{(t - z_3)(z_2 - z_1)} = \frac{(\gamma(t) - w_1)(w_2 - w_3)}{(\gamma(t) - w_3)(w_2 - w_1)}$$

and solve for $\gamma(t)$. □

Lemma 2 *Let F be an algebraically closed field. Let $\gamma \in \mathbf{GL_2}(F)$ be a matrix of finite order, and suppose that $charF$ does not divide the order of γ. Then γ is diagonalizable.*

Proof: Every matrix in $\mathbf{GL_2}(F)$ is similar to a matrix either of the form

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Since similar matrices have the same order, and since γ has finite order prime to the characteristic of F, the second case cannot occur. □

Lemma 2 shows that elements of finite order of $\mathbf{PGL_2}(F)$ can be diagonalized; for, if one representative of $\gamma \in \mathbf{PGL_2}(F)$ is diagonal, then all scalar multiples are also diagonal. Thus, if $\gamma \in \mathbf{PGL_2}(F)$ has finite order relatively prime to the characteristic of F, then γ is diagonalizable.

The following useful lemma gives a characterization of the order of an element of $\mathbf{PSL_2}(F)$ based on its trace.

Lemma 3 *Let* $T \in \mathbf{PSL_2}(F)$.

1. *Let* r *be an even integer. Then* T *has order* r *if and only if* $Trace(T) = \pm(\zeta + \zeta^{-1})$ *where* ζ *is a* $2r$*th root of unity.*

2. *Let* r *be an odd integer. Then* T *has order* r *if and only if* $Trace(T) = \pm(\zeta + \zeta^{-1})$ *where* ζ *is an* r*th or a* $2r$*th root of unity.*

Proof: Suppose $T \in \mathbf{PSL_2}(F)$ has order r, where $charF \nmid r$. Using the result of Lemma 2, assume that T is diagonal, since it is diagonalizable. Then

$$T = \pm \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

so that

$$T^r = \pm \begin{pmatrix} a^r & 0 \\ 0 & a^{-r} \end{pmatrix} = \pm I$$

which implies that $a^r = a^{-r}$, meaning a is either a primitive rth root of unity (and r is odd), or a primitive $2r$th root of unity.

Now, suppose $T \in \mathbf{PSL_2}(F)$ has trace $\zeta + \zeta^{-1}$, ζ a primitive rth root of unity. The product of the eigenvalues of T is 1 and their sum is $\zeta + \zeta^{-1}$, and thus the eigenvalues of T must be $\pm\zeta$ and $\pm\zeta^{-1}$, so (by extending scalars if necessary) one can diagonalize T, as long as $\zeta \neq \zeta^{-1}$.

Then $T = \pm \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$. Let m be the order of T. This implies $\zeta^m = \zeta^{-m}$, i.e., $\zeta^{2m} = 1$.

If r is odd, $2m \equiv 0 \pmod{r} \Rightarrow m \equiv 0 \pmod{r}$, so the order of T is r.

If r is even, then $2m \equiv 0 \pmod{r}$, and the least such m is $r/2$. So the order of T is $r/2$. $\square$

2.3.2 Finite subgroups of $\mathbf{PGL_2}(F)$

This section establishes some properties of finite subgroups of $\mathbf{PGL_2}(F)$ which will enable us to give a characterization of all such subgroups.

Lemma 4 *Let F be a field. For $T \in \mathbf{GL_2}(F)$, define*

$$\Delta(T) := Tr(T)^2 - 4\det(T).$$

If $T \neq I$, then T has 0 fixed points if and only if $\Delta(T)$ is a non-square in $F^\times$, 1 fixed point if and only if $\Delta(T) = 0$, and 2 fixed points if and only if $\Delta(T)$ is a square in $F^\times$. In particular, every non-identity element of $\mathbf{PGL_2}(F)$ has at most two fixed points in $\mathbb{P}^1(F)$.

Proof: Let $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If z is a fixed point of T, then

$$\frac{az+b}{cz+d} = z.$$

so that z satisfies the quadratic equation $cz^2 + (d-a)z - b = 0$ $(*)$. There are three cases to consider: i) $c \neq 0$, ii) $c = 0$ and $d \neq a$, and iii) $c = 0$, $d = a \neq 0$.

First, assume that $c \neq 0$. Then the quadratic formula gives the roots of this equation:

$$z = \frac{a - d \pm \sqrt{\Delta(T)}}{2c}.$$

Thus, the equation has:

1. 1 root in F if $\Delta(T) = 0$.

2. 2 roots in F if $\Delta(T)$ is a non-zero square.

3. 0 roots in F if $\Delta(T)$ is not a square.

If $c \neq 0$ then ∞ is not fixed by T, so the roots listed above are all the fixed points of T in $\mathbb{P}^1(F)$.

If $c = 0$ but $d \neq a$, the equation $(*)$ has 1 root. But

$$\left(\frac{a\infty + b}{d}\right) = \infty,$$

so that ∞ is also a fixed point of T. Thus, in this case, $\Delta(T) = (a-d)^2$ and T has two fixed points.

If $c = 0$ and $d = a \neq 0$, the above equation gives $-b = 0$, which clearly has no solutions unless $b = 0$. However, if $b = 0$ then $T = \pm I$, contrary to

our assumption. Thus, $b \neq 0$, and

$$\frac{a\infty + b}{a} = \infty.$$

so ∞ is the only fixed point of T, and $\Delta(T) = (a - a)^2 - 0 = 0$.

T is a representative for an element of $\mathbf{PGL_2}(F)$. Suppose a different representative is chosen in $\mathbf{GL_2}(F)$. All such representatives are of the form λT for $\lambda \in F^*$. Then $\Delta(\lambda T) = \lambda^2 \Delta(T)$, and so $\Delta(T)$ is defined up to a non-zero square. Thus, the result is independent of the choice of representative.

This proves the result. □

Corollary 1 *Let F be a field. The action of $\mathbf{PGL_2}(F)$ on $\mathbb{P}^1(F)$ as defined above is faithful.*

Proof: By the preceding lemma, every non-identity element of $\mathbf{PGL_2}(F)$ has at most two fixed points. □

Corollary 2 *Given any two triples (z_1, z_2, z_3), (w_1, w_2, w_3) of distinct elements of $\mathbb{P}^1(F)$, there is a* unique *$\gamma \in \mathbf{PGL_2}(F)$ such that $\gamma(z_i) = w_i$.*

Proof: Existence was shown in Lemma 1, and uniqueness follows from the fact that $\mathbf{PGL_2}(F)$ acts faithfully on $\mathbb{P}^1(F)$. □

The following two lemmas give important properties of finite subgroups of $\mathbf{PGL_2}(F)$ which will be used extensively in the sequel.

Lemma 5 *Let G be a finite subgroup of $\mathbf{PGL_2}(F)$ such that $charF \nmid |G|$ and such that every element in G has a common fixed point in $\mathbb{P}^1(F)$. Then G is cyclic.*

Proof: By extending scalars if necessary to include all the square roots of determinants of elements of G, we can assume that G is contained in $\mathbf{PSL_2}(F)$. Indeed, if $g \in G$, let $\lambda = \det g$. Then multiplying g by the scalar matrix $\lambda^{-1/2} I$ gives a matrix equivalent to g whose determinant is 1.

By translating if necessary, assume that the common fixed point of all elements of G is ∞, so that if $f \in G$ then f is of the form

$$\pm \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}.$$

If $a = a^{-1} = \pm 1$ then f has either infinite order or order $charF$, which contradicts our earlier assumption. So we can assume that $a \neq a^{-1}$ and f is diagonalizable.

Fix one element $f \neq I$ and conjugate the group G if necessary so that

$$f = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Recall that if $g \in G$ then

$$g = \begin{pmatrix} b & c \\ 0 & b^{-1} \end{pmatrix}.$$

Then

$$fgf^{-1}g^{-1} = \begin{pmatrix} 1 & bc(a^2-1) \\ 0 & 1 \end{pmatrix}$$

and this matrix is in G. Any matrix of this form is either I or has order p or ∞. so $fgf^{-1}g^{-1} = I$ for all $g \in G$. Then $bc(a^2-1) = 0$. so $b = 0$ (impossible) or $a = \pm 1$ (impossible) or $c = 0$. Therefore all elements of G are diagonal matrices of the form

$$\pm \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}.$$

which implies that G is cyclic. □

Lemma 6 *Let F be a field, and Γ a finite subgroup of $\mathbf{PGL_2}(F)$, whose order is relatively prime to $charF$. There exists a set X endowed with a Γ-action such that every non-identity element of Γ has precisely two fixed points in X.*

Proof: Consider Γ, a finite subgroup of $\mathbf{PGL_2}(F)$, where F is a field whose characteristic does not divide $|\Gamma|$. Γ acts on $\mathbb{P}^1(F)$ and every non-identity

element of Γ has *at most* two fixed points.

Let $\overline{F}$ be the algebraic closure of F. Then

1. $\Gamma \subseteq \mathbf{PSL_2}(\overline{F})$: and

2. $T \in \Gamma \Rightarrow (Tr(T))^2 - 4$ is a square in $\overline{F}$.

Thus, all non-identity elements of Γ have either 1 or 2 fixed points in $\mathbb{P}^1(\overline{F})$.

Now, suppose $\gamma \in \Gamma$ has only 1 fixed point. Then

$$Tr(\gamma)^2 - 4 = (\zeta + \zeta^{-1})^2 - 4 = (\zeta - \zeta^{-1})^2 = 0$$

$$\Rightarrow \zeta = \zeta^{-1} \Rightarrow \zeta^2 = 1 \Rightarrow \zeta = \pm 1.$$

Putting γ in normal form gives

$$\gamma \sim \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which has infinite order if $char\overline{F} = 0$ and order p if $char\overline{F} = p$. Since Γ is a finite group and $charF \nmid |\Gamma|$, this cannot occur.

Thus, all elements of Γ have exactly two fixed points in $\mathbb{P}^1(\overline{F})$. $\square$

One can now make a definition which encapsulates the properties explored in the preceding lemmas:

Definition 2 *Let G be a group acting faithfully on a set X. The action of G on X is said to be of* $\mathbf{PGL_2}$-type *(respectively* $\mathbf{SO_3}$-type*) if every non-identity element has at most (resp. exactly) two fixed points and the stabilizer of every point in X is cyclic.*

Thus, Lemmas 5 and 6 say that if $\Gamma \subseteq \mathbf{PGL_2}(F)$ is a finite subgroup such that $|\Gamma|$ is relatively prime to the characteristic of F, then there is a set X on which Γ acts with an action of $\mathbf{SO_3}$-type.

Lemma 7 *Let G be a group with* $\mathbf{SO_3}$*-type action on a set X. Let H be a normal subgroup of G. If P is the set of points of X fixed by some non-trivial element of H, then P is fixed by the action of G.*

Proof: Suppose x belongs to P. Then x is fixed by an element of H, say h. Consider σx, for $\sigma \in G$.

$$\sigma x = \sigma h \sigma^{-1} \sigma x.$$

and $\sigma h \sigma^{-1}$ is an element of H, say h^*, so $\sigma x = h^*(\sigma x)$, proving that σx is also in P. □

We will now characterize all finite groups with an $\mathbf{SO_3}$-type action on some set, and in so doing, we will obtain a characterization for all possible finite subgroups of $\mathbf{PGL_2}(F)$ of order relatively prime to $charF$.

Suppose G is a finite group of order $N > 1$ endowed with an $\mathbf{SO_3}$-type action on a set X. Let P be the set of all points of X having a non-trivial

stabilizer. P is clearly a finite set, since G is a finite group, and each non-identity element has precisely two fixed points in X. Thus, the number of elements of P is at most $2X - 2$. Further, P is fixed as a set by the action of G. Indeed, let $x \in P$. Then x is fixed by some element of G, say by g. Let $f \neq g$ be an element of G. Then fx is fixed by fgf^{-1}, so fx belongs to P for all $f \in G$.

P can be written as a disjoint union $P = P_1 \cup \cdots \cup P_n$ of G-orbits. Let e_i be the order of the stabilizer of an element of P_i; this does not depend on the choice of element since if x_1, x_2 belong to P_i, then the stabilizer of x_1 is conjugate to the stabilizer of x_2, and thus both stabilizers have cardinality e_i. It follows that a normal subgroup of G which contains the stabilizer of some $x \in P_i$ must contain the stabilizers of all elements of P_i; this fact will be of use later.

Lemma 8 *With notation as above,*

$$2X - 2 = \sum_{i=1}^{n} \frac{X}{e_i}(e_i - 1).$$

Proof: First note that $e_i - 1$ is the number of non-identity elements of G which fix a given element of P_i. Therefore, $\#P_i(e_i - 1)$ is the number of elements of X which are fixed by some non-trivial element of the stabilizer of P_i, counting multiplicities. Summing over i, we get the total number of elements of P, counting multiplicities. Since there are $X - 1$ non-trivial elements of G, each having two fixed points, there is a total of $2X - 2$ fixed

points of G, counting multiplicities. Thus

$$2N - 2 = \sum_{i=1}^{n} \#P_i(e_i - 1).$$

From elementary group theory, $\#P_i = N/e_i$, proving the lemma. The identity can be rewritten as

$$2N - 2 = \sum_{i=1}^{n} N(1 - 1/e_i).$$

□

Dividing through by N in the above identity gives

$$2 - \frac{2}{N} = \sum_{i=1}^{n} \left(1 - \frac{1}{e_i}\right).$$

Since $N > 1$, it follows that $1 \leq 2 - 2/N < 2$, which implies that

$$1 \leq \sum_{i=1}^{n} \left(1 - \frac{1}{e_i}\right) < 2.$$

Since $e_i \geq 2\ \forall i$, $1/e_i \leq 1/2$ and $(1 - 1/e_i) \geq 1/2$. Thus,

$$\frac{n}{2} \leq \sum_{i=1}^{n} \left(1 - \frac{1}{e_i}\right).$$

and so $n = 2$ or 3.

One quickly dispenses with the case $n = 2$, since if $n = 2$ Lemma 8 says that

$$\frac{2}{N} = \frac{1}{e_1} + \frac{1}{e_2}$$

and since $e_i \leq N$, $e_i = N$. But then every element of G has a common fixed point, and Lemma 5 implies that G is cyclic.

If $n = 3$, set $(e_1, e_2, e_3) = (p, q, r)$. The only possibilities are that (p, q, r) is one of the following triples: $(2, 2, r)$ for $r \geq 2$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$.

CASE 1. $(p, q, r) = (2, 2, r)$. Then $|N| = 2r$, $|P_1| = |P_2| = r$, and $|P_3| = 2$.

Let $P_3 = \{x_1, x_2\}$. Let G_{x_1} be the stabilizer of x_1. It is cyclic of order r by Lemma 5, and has index 2 in G. It is therefore normal. Let $\sigma \in G_{x_1}$, and suppose that $\tau \in G$ does not fix x_1. Then $\tau x_1 = x_2$ and x_2 is fixed by $\tau\sigma\tau^{-1}$. But since G_{x_1} is normal, $\tau\sigma\tau^{-1} \in G_{x_1}$, and this holds for all $\tau \notin G_{x_1}$. Since there are r such elements, and r elements in the stabilizer of x_1, we conclude that $G_{x_1} = G_{x_2}$.

Note that any element in $G - G_{x_1}$ has order 2. Let $\sigma \in G_{x_1}$, $\tau \in G - G_{x_1}$. Note that $\tau\sigma x_1 = \tau x_1 = x_2$ since τ does not fix x_2. But then $\tau\sigma$ is not a member of G_{x_1}, and so $\tau\sigma$ has order 2, ie., $\tau\sigma\tau\sigma = 1$ or $\tau\sigma\tau^{-1} = \sigma^{-1}$. Thus, G is generated by an element τ of order 2 and an element σ of order r, satisfying the relation $\tau\sigma\tau^{-1} = \sigma^{-1}$. It follows that G is the dihedral group of order $2r$.

CASE 2. $(p, q, r) = (2, 3, 3)$. Then $N = 12$, $|P_1| = 6$, $|P_2| = 4$, and $|P_3| = 4$.

The action of G on P_2 yields a homomorphism $G \to S_4$. This action is injective, since every non-identity element has precisely two fixed points. Hence, G is isomorphic to a subgroup of S_4 of cardinality 12. The only such group is A_4.

CASE 3. $(p, q, r) = (2, 3, 4)$. Then $N = 24$, $|P_1| = 12$, $|P_2| = 8$, and $|P_3| = 6$.

Let $x \in P_2$. The stabilizer of x has order 3, so if x is fixed by an element $\sigma \in G$, then x is also fixed by σ^2, and $\sigma^3 = e$. Further, if σ fixes x, then any other point fixed by σ must be in P_2, since the other stabilizer groups have orders not divisible by 3. Thus, we can decompose P_2 into four pairs of elements (call them p_1, p_2, p_3, p_4), with the two elements in a given pair having the same stabilizer. If x, y have the same stabilizer, then $\tau x, \tau y$ also have the same stabilizer, for all $\tau \in G$, since if x, y are both fixed by $\sigma \in G$, then $\tau x, \tau y$ are both fixed by $\tau\sigma\tau^{-1}$. Thus, the action of G on the set $\{p_1, p_2, p_3, p_4\}$ gives a map $\varphi : G \to S_4$. Suppose σ_1 and σ_2 belong to $\mathrm{Ker}\varphi - \{1\}$. Then σ_1 and σ_2 must exchange the pair of elements of at least three of the p_i, since each element has at most two fixed points. We immediately see that $\sigma_1\sigma_2$ must act trivially on P_2, but then $\sigma_1\sigma_2$ has at least 8 fixed points; so $\sigma_1\sigma_2 = e$. Hence the kernel of φ has order at most two.

But G does not have a normal subgroup of order 2, since the fixed points of such a subgroup would be a G-orbit of order 2, and the smallest G-orbit

has order 6. Hence φ is injective and $G \simeq S_4$.

CASE 4. $(p, q, r) = (2, 3, 5)$. Then $N = 60$, $|P_1| = 30$, $|P_2| = 20$, and $|P_3| = 12$.

Let us examine the 2-Sylow subgroups of G. The Sylow theorems state that if $|G| = p^k m$ for some prime p, $p \nmid m$, then the number of subgroups of G of order p^k is $\equiv 1 \pmod{p}$ and divides m (see [Hun74], II 5.7, 5.9 and 5.10). Thus, the number of subgroups of order 4 divides 15 and is odd. Further, since there are 15 elements of order 2 in G, and each one is a member of at least one 2-Sylow subgroup, the number of such subgroups is at least 5. Therefore, the number of 2-Sylow subgroups is either 5 or 15.

A direct calculation shows that the class equation for G is

$$60 = 1 + 15 + 20 + 12 + 12.$$

In particular, G has 15 elements of order 2 which are conjugate to each other, each having a centralizer of order 4.

Suppose there are 15 2-Sylow subgroups. Counting with multiplicity, there are 45 elements of order 2 in these subgroups, and so there is an element $\tau \in G$ such that τ is a member of at least 3 of the 2-Sylow subgroups. But then the order of the centralizer of τ is at least 8, a contradiction. Hence, G has 5 distinct 2-Sylow subgroups.

The action of G by conjugation on its set of 2-Sylow subgroups gives a map $\varphi : G \to S_5$. Let K be the kernel of this map. K is a normal subgroup

of G, and K is equipped with an action of $\mathbf{SO_3}$-type, so K is either cyclic, dihedral, A_4 or S_4. If K is cyclic, it has order either 2, 3 or 5. But the non-trivial conjugacy classes of elements in G all have size larger than 5, and we remarked that any normal subgroup of G which contains the stabilizer of some $x \in P_i$ must contain the stabilizers of all elements of P_i, a contradiction. So K is not cyclic. Then K is either dihedral, A_4 or S_4. In particular, K contains elements of order 2. The number of points fixed by such elements is r (with $r \leq 5$), 6 or 12. Lemma 7 implies that G has an orbit of the same size, which is a contradiction.

Thus, K is trivial, and φ is an injection. Hence G is isomorphic to a subgroup of S_5 of order 60: the only such subgroup is A_5.

Let $\Gamma_{p,q,r}$ denote the group associated to the triple (p, q, r) as above. The following lemma provides a nice characterization of these groups using generators and relations.

Lemma 9 *The group $\Gamma_{p,q,r}$ is described by generators and relations by*

$$\Gamma_{p,q,r} = \langle \alpha, \beta, \gamma \rangle / \langle \alpha^p = \beta^q = \gamma^r = \alpha\beta\gamma = 1 \rangle.$$

Proof: This is clear for $\Gamma_{2,2,r}$ since the description above is simply the definition of a dihedral group. Indeed, let σ and τ be generators of D_r, with $\sigma^2 = 1$, $\tau^r = 1$ and $\sigma\tau\sigma = \tau^{-1}$. Let $\alpha = \sigma\tau$, $\beta = \sigma$ and $\gamma = \tau$. Then the above conditions on σ and τ are equivalent to the conditions $\alpha^2 = \beta^2 = \gamma^r = \alpha\beta\gamma = 1$.

Now consider $\Gamma_{2,3,3}$. Let $\sigma = (123)$, $\tau = (234) \in A_4$. These generate A_4, since they generate all 3-cycles and A_4 is generated by its 3-cycles (see [Hun74], I 6.1). The map $\Gamma_{2,3,3} \to A_4$ which sends β to σ, γ to τ and α to $\sigma\tau = \tau^2\sigma^2$ is well-defined because σ, τ and $\sigma\tau$ satisfy the defining relations for β, γ and α respectively. It is onto because σ and τ generate A_4.

The Todd-Coxeter algorithm (see [Art91], 6.9) reveals that $\Gamma_{2,3,3}$ has order 12. Since every onto homomorphism between two finite groups of the same cardinality is an isomorphism, $\Gamma_{2,3,3} \simeq A_4$.

The result for $\Gamma_{2,3,4}$ and $\Gamma_{2,3,5}$ can be demonstrated in the same fashion: first find generators of S_4 and A_5 which satisfy the proper relations, thus providing an onto map from $\Gamma_{p,q,r}$. The Todd-Coxeter algorithm shows that the order of $\Gamma_{2,3,4}$ is 24 and the order of $\Gamma_{2,3,5}$ is 60. □

All of the results of this section can be combined into the following theorem:

Theorem 3 *If Γ is a finite subgroup of $\mathbf{PGL_2}(F)$ whose order is prime to the characteristic of F, then Γ is either cyclic or is isomorphic to $\Gamma_{p,q,r}$ with $1/p + 1/q + 1/r > 1$.*

2.3.3 Parametric solutions

This section exploits the invariant theory of the finite subgroups of $\mathbf{PGL_2}(F)$ to produce parametric solutions to the generalized Fermat equation $x^p + y^q =$

z^r. The groups $\Gamma_{p,q,r}$ of the previous section satisfy the equation

$$\chi(p,q,r) = \frac{2}{|\Gamma_{p,q,r}|}.$$

Thus, if we consider only the Fermat equations with $\chi(p,q,r) > 0$, we can associate the group $\Gamma_{p,q,r}$ to the Fermat equation with the same exponents, over any algebraically closed field F such that $|\Gamma_{p,q,r}|$ is relatively prime to $char F$.

Throughout the rest of section 2.3, we assume that the field F is algebraically closed, and work over the field $F(t)$, the field of fractions of the polynomial ring $F[t]$. Elements of $\mathbf{PGL_2}(F)$ act on rational functions in the following way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} f(t) := f\left(\frac{at+b}{ct+d}\right).$$

Given a group $\Gamma \subseteq \mathbf{PGL_2}(F)$, a function f is said to be Γ-invariant if $\gamma f = f$ for all $\gamma \in \Gamma$.

There is a notion of degree for rational functions: given a rational function $f(t) = g(t)/h(t)$ with g, h relatively prime polynomials, define the degree of $f(t)$ to be $\max\{\deg(g(t)), \deg(h(t))\}$. If $(a(t), b(t), c(t))$ is a solution to the equation $x^p + y^q = z^r$ then the *degree* of the solution, as defined in the introduction, corresponds to the *degree* of the rational function $a(t)^p/c(t)^r$.

Theorem 4 *Suppose $\chi(p,q,r) > 0$. Fix an embedding of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(F)$*

and let Γ *denote its image. There is a unique rational function* $f \in F(t)$ *of degree* $N = |\Gamma_{p,q,r}|$ *which is* Γ*-invariant and which satisfies*

$$f(z_1) = 0, f(z_2) = 1, f(z_3) = \infty,$$

for $z_1 \in P_1$, $z_2 \in P_2$, $z_3 \in P_3$.

Proof: Let $\gamma_1, \ldots, \gamma_N$ be the elements of Γ. Define the rational function

$$f(t) = k \prod_{i=1}^{N} \frac{(\gamma_i(t) - \alpha)}{(\gamma_i(t) - \beta)}$$

where k is a constant chosen so that $f(z_2) = 1$ and α, β are any finite elements of the orbits of z_1 and z_3, respectively.

We first prove that f is Γ-invariant. Let $\gamma \in \Gamma$. Then

$$\begin{aligned} \gamma^{-1} f(t) = f(\gamma(t)) &= k \prod_{i=1}^{N} \frac{(\gamma_i \gamma(t) - \alpha)}{(\gamma_i \gamma(t) - \beta)} \\ &= k \prod_{i=1}^{N} \frac{(\gamma_i(t) - \alpha)}{(\gamma_i(t) - \beta)} \\ &= f(t). \end{aligned}$$

as desired.

Setting

$$\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

rewrite f as

$$\begin{aligned} f(t) &= k\prod_{i=1}^{N}\frac{(\gamma_i(t)-\alpha)}{(\gamma_i(t)-\beta)} \\ &= k\frac{\prod_{i=1}^{N}\left(\frac{a_it+b_i}{c_it+d_i}-\alpha\right)}{\prod_{i=1}^{N}\left(\frac{a_it+b_i}{c_it+d_i}-\beta\right)} \\ &= k\frac{\prod_{i=1}^{N}(a_it+b_i-\alpha(c_it+d_i))}{\prod_{i=1}^{N}(a_it+b_i-\beta(c_it+d_i))}. \end{aligned}$$

The above expression implies that the degree of f is *at most* N. In fact, $\deg\left(\prod_i(a_it+b_i-\alpha(c_it+d_i))\right)$ is N if and only if $\infty \notin P_1$ and is $N-p$ otherwise. Similarly, the degree of the numerator of f is either N or $N-r$, depending on whether $\infty \in P_3$. Since P_1 and P_3 are disjoint orbits, there is no cancellation from among the zeros and poles of f, and we conclude that the degree of f is N. This proves the existence of a function f satisfying the desired conditions.

The proof of uniqueness requires

Theorem 5 (Lüroth's Theorem) *Let F be a field and $F(t)$ an extension of F of transcendence degree 1. Suppose E is a field extension of F such that*

$$F \subsetneq E \subseteq F(t).$$

Then E is purely transcendental of degree 1 over F, i.e., $E = F(s)$ for some $s \in F(t)$.

For a proof of Lüroth's theorem, see [Che51], VI. 2.

Consider $F(t)$, the field of rational functions in t. This is an extension of degree N over $F(t)^\Gamma$, the set of rational functions fixed by the action of Γ. By Lüroth's theorem, since $F \subsetneq F(t)^\Gamma \subseteq F(t)$, $F(t)^\Gamma$ is a transcendental extension of F of transcendence degree 1, so $F(t)^\Gamma \simeq F(s)$ for some s transcendental over F. Since f is a rational function of degree N which is fixed by the action of Γ, then $F(f(t)) \subseteq F(s)$ and $F(t)$ is an extension of degree N over $F(f(t))$. So $F(f(t)) = F(s)$. Then suppose, without loss of generality, that $f(t) = s$.

Suppose there exists a rational function $g \in F(t)$ satisfying the same conditions as f. Then $g \in F(s)$ so

$$g = \frac{as + b}{cs + d}$$

and $g(z_1) = 0$, $g(z_2) = 1$, $g(z_3) = \infty$. Thus,

$$\frac{as(z_1) + b}{cs(z_1) + d} = \frac{b}{d} = 0$$

and so $b = 0$. Also,

$$\frac{as(z_2)}{cs(z_2) + d} = \frac{a}{c + d} = 1$$

implying $a = c + d$. And lastly,

$$\frac{as(z_3)}{cs(z_3) + d} = \frac{a}{c} = \infty$$

and so $c = 0$. Therefore $a = d$, and we deduce that $g = f$. Thus, f is the unique rational function of degree N satisfying the conditions stated above.

□

Let $z \in F$ and $f \in F(t)$. Define the *order* of z at f, denoted $\mathrm{ord}_z(f)$, to be the integer m such that

$$(t - z)^{-m} f(t)$$

is holomorphic and non-zero in a neighborhood of z. Define

$$\mathrm{ord}_\infty(f) = -\mathrm{ord}_0\left(f\left(\frac{1}{t}\right)\right).$$

For all but a finite number of $z \in \mathbb{P}^1(F)$, $\mathrm{ord}_z f = 0$. The *divisor* of $f(t)$ is defined as the formal sum

$$\mathrm{div}(f) = \sum_{z \in \mathbb{P}^1(F)} \mathrm{ord}_z(f) \cdot [z].$$

The divisor of a rational function f gives a list of its zeros and its poles and their orders; hence, a divisor completely determines a function up to a constant.

Proposition 1 *Let f be the function described in Theorem 4. Then there exist polynomials $a(t), b(t), c(t) \in F[t]$ such that*

$$f(t) = \frac{a(t)^p}{c(t)^r}. \qquad f(t) - 1 = \frac{-b(t)^q}{c(t)^r}.$$

so $(a(t), b(t), c(t))$ is a solution to the equation $x^p + y^q = z^r$.

Proof: The proof of Theorem 4 gives all the information required to determine the divisor of the function f. Indeed, f has N/p zeros with multiplicity p, which are precisely the elements of P_1. Similarly, the poles of f all have multiplicity r and are the N/r elements of P_3. Hence, the divisor of f is

$$p \sum_{z \in P_1} [z] - r \sum_{z \in P_3} [z].$$

Thus, the function f is completely determined up to a constant factor, which is computed using the fact that $f(z_2) = 1$. If ∞ is not in P_1 or P_3, $f(t)$ can be written as

$$k \frac{\prod_{z \in P_1} (t - z)^p}{\prod_{z \in P_3} (t - z)^r}.$$

where k is a constant chosen (different from the constant used in Theorem 4) so that $f(z_2) = 1$. However, if ∞ is in P_1 or P_3, it is necessary to adopt the convention that $t - \infty = 1$. It is easily checked that with this convention, ∞ will be a zero or pole of f of the appropriate order. In any case, we may

write

$$f(t) = \frac{a(t)^p}{c(t)^r}.$$

with $a(t)$, $c(t)$ relatively prime polynomials.

The divisor of $f(t) - 1$ may also be computed. Since $f(t) - 1$ has a zero at each of the elements of P_2 with multiplicity q, and the same poles as $f(t)$. Thus

$$\mathrm{div}(f(t) - 1) = q \sum_{z \in P_2} [z] - r \sum_{z \in P_3} [z].$$

This allows us to deduce that

$$\begin{aligned} f(t) - 1 &= k \frac{\prod_{z \in P_2, z \neq \infty} (t - z)^q}{\prod_{z \in P_3, z \neq \infty} (t - z)^r} \\ &= -\frac{b(t)^q}{c(t)^r}. \end{aligned}$$

where $a(t)$, $b(t)$, $c(t)$ are relatively prime polynomials.

Now, since $f - (f - 1) = 1$, we have

$$\frac{a(t)^p}{c(t)^r} + \frac{b(t)^q}{c(t)^r} = 1.$$

or

$$a(t)^p + b(t)^q = c(t)^r.$$

and $(a(t), b(t), c(t))$ is a parametric solution over F to the generalized Fermat equation $x^p + y^q = z^r$. □

Two embeddings of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(\overline{F})$ are said to be *equivalent* if they have the same image in $\mathbf{PGL_2}(\overline{F})$. Equivalent embeddings produce the same parametric solution, so we need only concern ourselves with equivalence classes of embeddings.

Theorem 6 *Let F be an algebraically closed field. Let p, q, r be such that $\chi(p, q, r) > 0$ and let $N = N(p, q, r) = 2/\chi(p, q, r)$. Suppose that $charF$ does not divide N. There is a bijection between the set of equivalence classes of embeddings of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(F)$ and the set of parametric solutions of degree N to the generalized Fermat equation $x^p + y^q = z^r$.*

Proof: The Γ-invariant function f obtained from an equivalence class of embeddings of $\Gamma_{p,q,r}$ gives a parametric solution to the generalized Fermat equation, of the proper degree. It remains only to prove the converse.

Let $a(t), b(t), c(t) \in F[t]$ be such that $a(t)^p + b(t)^q = c(t)^r$. This relation implies that at least two of $a(t)^p$, $b(t)^q$ and $c(t)^r$ have degree N - say, $a(t)^p$ and $c(t)^r$. Let

$$f(t) = \frac{a(t)^p}{c(t)^r}.$$

Let Γ be the set of all $\gamma \in \mathbf{PGL_2}(F)$ such that $\gamma f = f$. This set is, in fact,

a group. Indeed, if $\gamma_1, \gamma_2 \in \Gamma$, then

$$\gamma_1\gamma_2 f = \gamma_1 f = f,$$

so $\gamma_1\gamma_2 \in \Gamma$. Further, if $\gamma \in \Gamma$, then

$$f = \gamma^{-1}\gamma f = \gamma^{-1} f,$$

so $\gamma^{-1} \in \Gamma$.

Any element of Γ permutes the roots of $a(t)$, $b(t)$, and $c(t)$. Indeed, suppose z_1 is a root of $a(t)$. Then $f(z_1) = 0 = f(\gamma(z_1))$ (since f is Γ-invariant), so $\gamma(z_1)$ is also a root of $a(t)$. Since $\mathbf{PGL_2}(F)$ is triply transitive, any $\gamma \in \Gamma$ is uniquely determined by its action on the roots of $a(t), b(t)$, and $c(t)$. Hence Γ is a finite group.

In general, an element of $\mathbb{P}^1(F)$ has an orbit of order N, since for all but finitely many $\alpha \in \mathbb{P}^1(F)$, the equation $f(t) = f(\alpha)$ has N distinct roots. Thus, $|\Gamma| \geq N$. Since each of the roots of $a(t)$, $b(t)$ and $c(t)$ has an orbit of less than N elements, they must have a non-trivial stabilizer. Then Γ has precisely three orbits of fixed points, of orders N/p, N/q and N/r respectively. Thus, $\Gamma \simeq \Gamma_{p,q,r}$, and each set of parametric solutions to $x^p + y^q = z^r$ gives rise to an embedding of $\Gamma_{p,q,r}$.

The class of embeddings of $\Gamma_{p,q,r}$ obtained from a given parametric solution $(a(t), b(t), c(t))$ is precisely the class of embeddings which gives rise to

$(a(t), b(t), c(t))$, and so the map defined above is in fact a bijection. ∎

2.3.4 Some algebraic geometry

As the final step in the proof of Theorem 1, it remains only to prove that every parametric solution of the generalized Fermat equation with $\chi(p, q, r) > 0$ can be obtained from one of the solutions described in the preceding section. In preparation for the proof, we begin with some facts about function fields and coverings of $\mathbb{P}^1$.

A *covering* of a topological space Y is a pair (X, π), with X a topological space and $\pi : X \to Y$ a map between them, such that for any $y \in Y$, there exists a neighborhood N of y such that the inverse image $\pi^{-1}(N)$ consists of disjoint open sets, U_i, such that U_i is homeomorphic to N for all i. We are concerned primarily with algebraic covering maps, in which the inverse image of any point is a finite set.

Now suppose that X, Y are varieties over some algebraically closed field F. To each variety V over F is associated a field of functions, denoted $F(V)$. Let f be any rational function $f : X \to Y$. The map f induces an inclusion of function fields, so $F(Y) \subseteq F(X)$. Let $P \in X$. Then the field $F(X)_P$ ($F(X)$ localized at P) is an extension of the field $F(Y)_{f(P)}$. Let π be a generator of the ideal corresponding to $f(P)$. Define a valuation $v_\pi : F(Y)_{f(P)} \to \mathbb{Z}$ by $v_\pi(\tau) = n$ if and only if $\tau = \pi^n \tau'$ where π does not divide τ'. The *value group* of this valuation is the image of v_π; in this case, the value group is $\mathbb{Z}$.

Now, choose a generator $\bar{\pi}$ of the ideal associated to P in $F(X)$: Define

a valuation $v_{\bar{\pi}} : F(X)_P \to \mathbb{Q}$ such that $v_{\bar{\pi}}$ restricted to $F(Y)_{f(P)}$ is v_π. The image of $v_{\bar{\pi}}$ in $\mathbb{Q}$ is $\frac{1}{e}\mathbb{Z}$ for some $e \in \mathbb{N}$. This number e depends on P: it is called the *ramification index* of P. A point $Q \in Y$ is said to be *ramified* if there is some $P \in f^{-1}(Q)$ with ramification index greater than 1.

A *nonsingular complete curve* X/F is a pair $(X, F(X)/F)$ consisting in a field $F(X)/F$ of transcendence degree 1 over F and a set X identified with the variety $V(F(X)/F)$ through a given bijection between X and $V(F(X)/F)$. We will want to apply this theorem to coverings of $\mathbb{P}^1$, which are nonsingular complete curves by this definition, associated to the field of functions $F(t)/F$.

The last definition we will need is that of the genus of a curve. If X is a curve defined by a homogeneous equation of degree d, then the *genus* of X is the integer

$$\frac{(d-1)(d-2)}{2}.$$

These ideas are all combined in the following theorem.

Theorem 7 (Riemann-Hurwitz Formula) *Suppose that F is an algebraically closed field and let $f : X \to Y$ be a morphism of nonsingular complete curves over F. Assume that the degree N of f is prime to the characteristic of F. Then*

$$2g(X) - 2 = N(2g(Y) - 2) + \sum_{P \in X} (e_P - 1).$$

where $g(X)$ is the genus of the curve X and e_P is the ramification index of P.

A proof can be found in [Har77], IV 2.4.

2.3.5 Solutions of higher degree

The final step in the proof of the main theorem for this chapter will be accomplished in two parts. First, we use the Riemann-Hurwitz Formula to prove the following lemma, which will be vital to the proof of the main theorem.

Lemma 10 *There are no non-trivial unramified coverings of $\mathbb{P}^1$.*

Proof: Let (X, f) be a covering of $\mathbb{P}^1(F)$ of degree $d \geq 1$. The Riemann-Hurwitz formula in this case says that

$$2g(X) - 2 = -2d + \sum_{p \in X} (e_P - 1).$$

If (X, f) is unramified, we have $2g(X) - 2 = -2d$. The left-hand side is at least -2, and the right-hand side is at most -2, so we must have $2g(X) - 2 = -2d = -2$, and so $d = 1$, which implies that f is an isomorphism. □

This lemma provides the strategy for the second part of the proof. The idea is to take two parametric solutions, one of degree N and one of arbitrary degree, and look at the corresponding function fields. If we can prove

that a certain covering of $\mathbb{P}^1(F)$ is trivial, this will provide a map from one parametric solution to the other.

Theorem 8 *Let F be an algebraically closed field, and let $\chi(p,q,r) > 0$. Every primitive parametric solution to the equation $x^p + y^q = z^r$ is of the form*

$$\left(a\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(a)}, b\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(b)}, c\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(c)}\right),$$

where the degree of $a(t)^p/c(t)^r$ is $N(p,q,r) = 2/\chi(p,q,r)$, and $g(t), h(t) \in F[t]$.

Proof:

Suppose $(x(t), y(t), z(t))$ is a primitive parametric solution to the generalized Fermat equation, and let $(a(t), b(t), c(t))$ be a parametric solution of degree $N(p,q,r)$.

Let $A, X \simeq \mathbb{P}^1(F)$. Let $\alpha : A \to \mathbb{P}^1(F)$ be defined as $\alpha(u) = a(u)^p/c(u)^r$, and let $\xi : X \to \mathbb{P}^1(F)$ be the map $\xi(s) = x(s)^p/z(s)^r$. Finally, let W be the variety corresponding to the compositum of the function fields of A and X. Then the commutative diagram

$$\begin{array}{ccc} W & \longrightarrow & A \\ \downarrow & & \downarrow{\scriptstyle \alpha(u)=\frac{a(u)^p}{c(u)^r}} \\ X & \xrightarrow[\xi(s)=\frac{x(s)^p}{z(s)^r}]{} & \mathbb{P}^1(F) \end{array}$$

gives rise to the following diagram of function fields:

$$\begin{array}{ccc} & F(u,s) & \\ \swarrow & & \searrow \\ F(X) = F(s) & & F(A) = F(u) \\ \searrow & & \swarrow \\ & F(t) & \end{array}$$

where $t = \frac{r(s)^p}{z(s)^r}$ and $t = \frac{a(u)^p}{c(u)^r}$.

The strategy is to prove that W is an unramified covering of X: Lemma 10 then implies that $W \simeq X$, so that ξ factors through α. Let $w \in W$. If w is ramified over X, then the image of w in A must be ramified over $\mathbb{P}^1(F)$. Since the only ramified points of A over $\mathbb{P}^1(F)$ lie above 0, 1 and ∞, it is necessary only to examine these points.

The ramified points of $a(u)^p/c(u)^r$ are precisely those points of $\mathbb{P}^1(F)$ which have a non-trivial stabilizer in the group $\Gamma \subseteq \mathbf{PGL_2}(F)$ that fixes $a(u)^p/c(u)^r$. The points corresponding to 0 are the points in the orbit P_1, the points corresponding to 1 the points of P_2, and the points corresponding to ∞ are the points of P_3. The ramification indices of these points are p, q and r, respectively.

Consider the points of X lying over 0, 1 and ∞. If the ramification indices of these points are multiples of p, q, and r respectively, then W will be an unramified covering of X.

Since $t = x(s)^p/z(s)^r$, the ideals lying over t are those corresponding to linear factors of $x(s)$. Let $(s - \beta)$ be one such factor, with exponent e. Then $(s - \beta)^{ep}$ divides t, so the ramification index of $(s - \beta)$ is ep, for some integer $e \geq 1$. Thus, if w is any point in W whose image in X lies above 0, then w is unramified over X. An analogous proof, considering points lying above 1 and ∞, shows that all points of W lying over 1 and ∞ in $\mathbb{P}^1(F)$ are unramified over X. Thus, W is an unramified covering of X, and so $W \simeq X$. Hence $F(A)$ is contained in $F(X)$. The inclusion provides a map from X to A, thus proving the result. □

In particular, we have the following corollary.

Corollary 3 *Let $\chi(p, q, r) > 0$ and suppose F is an algebraically closed field. Let $(a(t), b(t), c(t))$ be a parametric solution over F of degree $N = N(p, q, r)$ to the equation $x^p + y^q = z^r$. Then all other parametric solutions of degree N can be obtained by taking $(a(\gamma t), b(\gamma t), c(\gamma t))$ and clearing denominators, for $\gamma \in \mathbf{PGL_2}(F)$.*

Combining Theorem 2 with Proposition 1 and Theorem 8 gives a complete proof of Theorem 1.

2.4 Examples

Lemmas 3 and 9 suggest a method for writing down explicit embeddings of the groups $\Gamma_{p,q,r}$ as subgroups of $\mathbf{PGL_2}(\overline{\mathbb{Q}})$, noting that if F is algebraically

closed, then $\mathbf{PGL_2}(F) = \mathbf{PSL_2}(F)$. We will demonstrate this method for the group $\Gamma_{2,2,r}$.

The strategy is to begin with

$$\gamma = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$$

where r is the least positive integer such that $\omega^r = \omega^{-r}$, so that γ has order r. Then let

$$\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and try to find a, b, c, d such that $Tr\beta = 0$ (since we want β to have order 2), $\det \beta = 1$ and $Tr\beta\gamma = 0$ to ensure that $\alpha = \beta\gamma$ has order 2.

The trace condition on β allows us to deduce that $d = -a$. Then

$$\beta\gamma = \begin{pmatrix} a\omega & b\omega^{-1} \\ c\omega & -a\omega^{-1}. \end{pmatrix}$$

and the trace condition on $\beta\gamma$ implies that $a\omega - a\omega^{-1} = 0$, and hence $a = 0$ since $\omega \neq \omega^{-1}$. Substituting back into β gives

$$\beta = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}.$$

Now choose b, c so that $\det \beta = 1$. For simplicity, we choose $b = 1$, $c = -1$, but we can choose any $b \in \overline{\mathbb{Q}}^*$, choosing $c = -1/b$. Thus, the matrices

$$\gamma = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix},$$

$$\beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

give one embedding of $\Gamma_{2,2,r}$ into $\mathbf{PGL_2}(\overline{\mathbb{Q}})$.

It is worth emphasizing that this is just one choice of embedding, and that any other choice for b would give a different one.

To find an embedding of $\Gamma_{2,3,3}$ let

$$\gamma = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$$

where ω is a primitive cube root of unity. We must find β such that $Tr\beta = -1 = \omega + \omega^2$, $\det \beta = 1$ and $Tr\beta\gamma = 0$. One choice for β is

$$\beta = \frac{1}{1-\omega} \begin{pmatrix} \omega & 2 \\ \omega & -1 \end{pmatrix}.$$

This embedding enables us to write down a parametric solution to the equa-

tion $x^2 + y^3 = z^3$ over $\overline{\mathbb{Q}}$, using the rational function f of Theorem 4. The fixed points of this particular embedding of $\Gamma_{2,3,3}$ fall into the three orbits $P_1 = \{1 \pm \sqrt{3}, \omega(1 \pm \sqrt{3}), \omega^2(1 \pm \sqrt{3})\}$, $P_2 = \{1, \omega, \omega^2, \infty\}$, and $P_3 = \{0, 2, 2\omega, 2\omega^2\}$.

This gives the polynomials

$$\begin{aligned} a(t) &= k_1 \prod_{z \in P_1} (t - z) \\ &= k_1(t^6 - 20t^3 - 8), \\ b(t) &= k_2 \prod_{z \in P_2, z \neq \infty} (t - z) \\ &= k_2(t^3 - 1), \\ c(t) &= k_3 \prod_{z \in P_3} (t - z) \\ &= k_3(t^4 + 8t), \end{aligned}$$

where k_1, k_2 and k_3 are chosen so that

$$a(t)^2 + b(t)^3 = c(t)^3.$$

Since

$$\begin{aligned} a(t)^2 &= k_1^2(t^{12} - 40t^9 + 384t^6 + 320t^3 + 64), \\ b(t)^3 &= k_2^3(t^9 - 3t^6 + 3t^3 - 1), \\ c(t)^3 &= k_3^3(t^{12} + 24t^9 + 192t^6 + 512t^3), \end{aligned}$$

we choose $k_1 = 1$, $k_2 = 4$ and $k_3 = 1$.

Thus, for exponents $(2, 3, 3)$, $(t^6 - 20t^3 - 8, 4t^3 - 4, t^4 + 8t)$ gives a parametric solution to the generalized Fermat equation. These polynomials have integer coefficients; we could have predicted this by looking at the orbits P_1, P_2, and P_3. Each of the orbits is closed under the action of $G_{\mathbb{Q}}$, implying that the coefficients of a, b and c are in $\mathbb{Q}$; since all the finite points in P_1, P_2 and P_3 are algebraic integers, the coefficents must in fact be rational integers.

For $\Gamma_{2,3,4}$ let

$$\gamma = \begin{pmatrix} \omega & 0 \\ 0 & -\omega^3 \end{pmatrix}$$

where ω is a primitive eighth root of unity. Then find a matrix β such that $\det \beta = 1$, $Tr\beta = -1$ and $Tr\beta\gamma = 0$. One possible choice is

$$\beta = \frac{1}{2} \begin{pmatrix} -1 - \omega^2 & -1 \\ 2 & \omega^2 - 1 \end{pmatrix}.$$

Using Maple, we can compute the fixed points of Γ and calculate their

orbits to find the polynomials a, b and c. We find

$$\begin{aligned} a(t) &= k_1\left(t^{12}+\frac{33}{4}t^8-\frac{33}{16}t^4-\frac{1}{64}\right), \\ b(t) &= k_2\left(t^8-\frac{7}{2}t^4+\frac{1}{16}\right), \\ c(t) &= k_3\left(t^5+\frac{1}{2}t\right). \end{aligned}$$

Expanding, we can choose $k_1 = 1$, $k_2 = -1$ and $k_3 = 27^{1/4}$.

Finally, for $\Gamma_{2,3,5}$, we let

$$\gamma = \begin{pmatrix} \omega & 0 \\ 0 & \omega^4 \end{pmatrix}$$

where ω is a primitive fifth root of unity. We then try to find β such that $\det\beta = 1$, $Tr\beta = -1$ and $Tr\beta\gamma = 0$. We obtain

$$\beta = \frac{1}{1-\omega^3}\begin{pmatrix} \omega^3 & 1+\omega^3+\omega^2 \\ -\omega^3+2+2\omega & -1 \end{pmatrix}.$$

Again using Maple, we compute the fixed points of Γ and calculate their

orbits. Let $\zeta = \frac{-1}{2} - \frac{1}{2}\sqrt{5}$. We find that

$$\begin{aligned} a(t) &= k_1(t^{30} + (-46458 - 28710\zeta)t^{25} + (-109514730 - 67683825\zeta)t^{20} \\ &\quad -(1656629310705 - 1023853220775\zeta)t^{10} \\ &\quad +(10630535780628 + 6570032431050\zeta)t^5 \\ &\quad +25047307819\dot{6}1 + 15480087559\dot{2}0\zeta). \end{aligned}$$

$$\begin{aligned} b(t) &= k_2(t^{20} + (20292 + 12540\zeta)t^{15} + (5402324 + 3341910\zeta)t^5 \\ &\quad -165580141 + 102334155\zeta). \end{aligned}$$

and

$$c(t) = k_3(t^{11} + (-979 - 605\zeta)t^6 + (-10946 - 6765\zeta)t).$$

We can choose $k_1 = 1$, $k_2 = -1$, $k_3 = (153792 + 95040\zeta)^{1/5}$.

3 Solutions over general fields

3.1 Introduction

This chapter addresses two basic questions: given a field F which is not necessarily algebraically closed, do there exist parametric solutions to the generalized Fermat equation over F? And, supposing at least one parametric solution exists, how many distinct classes of solutions are there over F, up to a suitable notion of equivalence?

Theorem 1 gives conditions for precisely when parametric solutions to the generalized Fermat equation exist over an algebraically closed field. In practice, we will often be working over fields which are not algebraically closed, and so we need a refinement of this theorem. The first step will be to look at the solutions described in Theorem 6 to determine the smallest field containing their coefficients. We discover that parametric solutions over F to the generalized Fermat equation come from *F-rational* embeddings of $\Gamma_{p,q,r}$: that is, embeddings that are fixed globally by the Galois group G_F.

We then turn to the second question. Two parametric solutions over F are said to be *F-equivalent* if one can be obtained from the other by replacing the parameter t by a fractional linear transformation of t, with coefficients in F. We prove that over an algebraically closed field, all parametric solutions of degree $N(p,q,r)$ to the equation $x^p + y^q = z^r$ are equivalent.

The situation over non-algebraically closed fields is more complex. An investigation of the number of F-equivalence classes of parametric solutions

leads us to consider the set of F-equivalence classes of F-rational embeddings of $\Gamma_{p,q,r}$. We define a map between this set and the first cohomology set of G_F in $\mathrm{Aut}(\Gamma_{p,q,r})$ and prove that it is injective; it is not, in general, surjective. To obtain a surjective map we must enlarge the set of embeddings we consider to include embeddings of $\Gamma_{p,q,r}$ into the $\overline{\mathbb{Q}}$-automorphism groups of conics defined over $\mathbb{Q}$. We prove that the map between this new set and $H^1(G_F, \mathrm{Aut}(\Gamma_{p,q,r}))$ is indeed surjective when $(p,q,r) = (2,3,3)$ or $(2,3,4)$. We prove a similar theorem for $\Gamma_{2,3,5}$, and give criteria for which elements of $H^1(G_{\mathbb{Q}}, \mathrm{Aut}(\Gamma_{2,3,5}))$ correspond to parametric solutions over $\mathbb{Q}$.

3.2 The equation $Ax^p + By^q = z^r$

The Galois group G_F acts on $\mathbf{PGL_2}(\overline{F})$ by its action on $\overline{F}$, and this extends to an action on the set of embeddings of $\Gamma_{p,q,r}$ in a natural way. Let $A_{p,q,r}$ denote the automorphism group of $\Gamma_{p,q,r}$.

Definition 3 *An embedding $\rho : \Gamma_{p,q,r} \to \mathbf{PGL_2}(\overline{F})$ is said to be* F-rational *if for each $\sigma \in G_F$ there exists $\alpha_\sigma \in A_{p,q,r}$ such that ${}^\sigma\rho = \rho \cdot \alpha_\sigma$. That is, the image of ρ is preserved by the action of G_F.*

Proposition 2 *Let $\chi(p,q,r) > 0$, and suppose that $N = N(p,q,r)$ is relatively prime to the characteristic of F. Let Γ be the image of an F-rational embedding of the group $\Gamma_{p,q,r}$, and let f be the function associated to Γ as in Theorem 4. Then there are constants $\lambda_1, \lambda_2 \in F$ and relatively prime*

polynomials $a(t), b(t), c(t) \in F[t]$ *such that*

$$f(t) = \lambda_1 \frac{a(t)^p}{c(t)^r}, \quad f(t) - 1 = -\lambda_2 \frac{b(t)^q}{c(t)^r},$$

so that $(a(t), b(t), c(t))$ *is a parametric solution of degree* N *to the generalized Fermat equation*

$$\lambda_1 x^p + \lambda_2 y^q = z^r. \tag{4}$$

Proof:

Let

$$\begin{aligned} a(t) &= \prod_{z \in P_1} (t - z), \\ b(t) &= \prod_{z \in P_2} (t - z), \\ c(t) &= \prod_{z \in P_3} (t - z), \end{aligned}$$

with the convention that $(t - \infty) = 1$.

Since Γ is F-rational, the set of fixed points of Γ is preserved under the action of G_F, as are P_1, P_2 and P_3. Thus, if $\sigma \in G_F$, then

$$\sigma(a(t)) = \prod_{z \in P_1} (t - \sigma(z)) = \prod_{z \in P_1} (t - z) = a(t).$$

so the coefficients of $a(t)$ are fixed under the action of G_F. Hence, $a(t)$ is a polynomial with coefficients in F. Similarly, $b(t), c(t)$ belong to $F[t]$.

Let

$$\begin{aligned}\lambda_1 &= \frac{\prod_{z\in P_3}(z_2 - z)^r}{\prod_{z\in P_1}(z_2 - z)^p} = \frac{c(z_2)^r}{a(z_2)^p}.\\ \lambda_2 &= -\frac{\prod_{z\in P_3}(z_1 - z)^r}{\prod_{z\in P_2}(z_1 - z)^q} = \frac{-c(z_1)^r}{b(z_1)^q}.\end{aligned}$$

Then

$$\begin{aligned}\sigma(\lambda_1) &= \frac{\prod_{z\in P_3}(\sigma(z_2) - \sigma(z))^r}{\prod_{z\in P_1}(\sigma(z_2) - \sigma(z))^p}\\ &= \frac{\prod_{z\in P_3}(\sigma(z_2) - z)^r}{\prod_{z\in P_1}(\sigma(z_2) - z)^p}\\ &= \frac{c(\sigma z_2)^r}{a(\sigma z_2)^p}.\end{aligned}$$

but $\sigma(z_2) \in P_2$ since Γ is an F-rational embedding, so $\sigma(\lambda_1) = \lambda_1$ for every $\sigma \in G_F$. Thus, $\lambda_1 \in F$, and similarly, $\lambda_2 \in F$. □

Note that if λ_1 is a pth power and λ_2 is a qth power in F, they can be absorbed into the polynomials $a(t)$ and $b(t)$ respectively, giving a solution to the equation

$$x^p + y^q = z^r.$$

Unfortunately, this isn't always the case, as the examples of Section 1.4 demonstrate. However, for exponents (2,3,5), multiplying equation (4) by $\lambda_1^{15}\lambda_2^{20}$ gives the equation

$$(\lambda_1^8\lambda_2^{10}a(t))^2 + (\lambda_1^7\lambda_2^7b(t))^3 = (\lambda_1^3\lambda_2^4c(t))^5,$$

providing a parametric solution to the equation $x^2 + y^3 = z^5$. A similar method for exponents (2,3,3) will only work if λ_2 is a cube, and for (2,3,4) if λ_1 is a square.

3.3 F-equivalent solutions

Definition 4 *Two parametric solutions* $(a(t), b(t), c(t))$ *and* $(\tilde{a}(t), \tilde{b}(t), \tilde{c}(t))$ *are said to be* F-equivalent *if there exists some* $\gamma \in \mathbf{PGL_2}(F)$ *such that* $\tilde{a}(t) = a(\gamma t)$, $\tilde{b}(t) = b(\gamma t)$ *and* $\tilde{c}(t) = c(\gamma t)$.

These solutions are equivalent in the sense that the set of solutions in F^3 to the generalized Fermat equation obtained by specializing t to values in F are the same for both parametric solutions.

Definition 5 *Let* ρ_1 *and* ρ_2 *be two embeddings of* $\Gamma_{p,q,r}$ *into* $\mathbf{PGL_2}(\overline{F})$. *They are said to be* F-equivalent, *denoted* $\rho_1 \sim \rho_2$, *if there exists an element* $M \in \mathbf{PGL_2}(F)$ *and* $\alpha \in A_{p,q,r}$ *such that* $\rho_1 = M(\rho_2 \cdot \alpha)M^{-1}$.

Lemma 11 *Let* ρ_1, ρ_2 *be* F*-equivalent embeddings of* $\Gamma_{p,q,r}$ *into* $\mathbf{PGL_2}(\overline{F})$. *The parametric solutions corresponding to* ρ_1 *and to* ρ_2 *are* F*-equivalent.*

Proof: Let Γ be the image of ρ_1 in $\mathbf{PGL_2}(\overline{F})$. Suppose that the image of ρ_2 is $M\Gamma M^{-1}$, where

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PGL_2}(F).$$

The orbits of the fixed points of this new group are MP_1, MP_2 and MP_3 where P_1, P_2, and P_3 are the fixed points of the original embedding Γ. The function f obtained from $M\Gamma M^{-1}$ is

$$\begin{aligned} f(t) &= \frac{\prod_{z\in P_1}(t-\frac{az+b}{cz+d})^p \prod_{z\in P_3}(\frac{az_2+b}{cz_2+d}-\frac{az+b}{cz+d})^r}{\prod_{z\in P_3}(t-\frac{az+b}{cz+d})^r \prod_{z\in P_1}(\frac{az_2+b}{cz_2+d}-\frac{az+b}{cz+d})^p} \\ &= \frac{\prod_{z\in P_1}((cz+d)t-(az+b))^p}{\prod_{z\in P_3}((cz+d)t-(az+b))^r} \frac{\prod_{z\in P_3}(ad-bc)^r(z_2-z)^r}{\prod_{z\in P_1}(ad-bc)^p(z_2-z)^p} \\ &= \frac{\prod_{z\in P_1}((dt-b)-z(a-ct))^p}{\prod_{z\in P_3}((dt-b)-z(a-ct))^r} \frac{\prod_{z\in P_3}(ad-bc)^r(z_2-z)^r}{\prod_{z\in P_1}(ad-bc)^p(z_2-z)^p} \\ &= \frac{\prod_{z\in P_1}\left(\frac{dt-b}{-ct+a}-z\right)^p}{\prod_{z\in P_3}\left(\frac{dt-b}{-ct+a}-z\right)^r} \frac{\prod_{z\in P_3}(z_2-z)^r}{\prod_{z\in P_1}(z_2-z)^p}. \end{aligned}$$

and hence the parametric solution corresponding to $M\Gamma M^{-1}$ is obtained from the solution corresponding to Γ by a fractional linear transformation. □

Theorem 6 directly implies the following theorem.

Theorem 9 *Let $\chi(p,q,r) > 0$, and let F be a field whose characteristic does not divide $N = N(p,q,r)$. The assignment $\rho \mapsto (a(t), b(t), c(t))$ described in Proposition 2 induces a bijection between the set of F-equivalence classes of F-rational embeddings of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(\overline{F})$, and the set of F-equivalence*

classes of parametric solutions of degree N to the generalized Fermat equations $\lambda_1 x^p + \lambda_2 y^q = z^r$, where λ_1 and λ_2 vary.

3.4 How many parametric solutions are there?

In this section we use Theorem 9 to investigate the number of F-equivalent parametric solutions over any field F. In some cases, this number can be explicitly calculated.

3.4.1 Algebraically closed fields

We have already proved the following result:

Proposition 3 *Over an algebraically closed field F, all parametric solutions of degree N are F-equivalent.*

Proof: Combine Theorem 9 with Corollary 3. □

In [Beu98], it is proved that all solutions of the generalized Fermat equation can be obtained from parametric solutions by specializing the parameters to values in F. This result, together with Proposition 3, implies that all solutions in F^* to the equation $x^p + y^q = z^r$ can be obtained by taking values of a single parametric solution to the equation.

3.4.2 Non-abelian cohomology

Our investigation into the number of F-equivalence classes of parametric solutions will lead us to consider non-abelian cohomology, so we begin with

some basic definitions and results. Throughout this section, let G be a *profinite group*, that is, a topological group which is the projective limit of finite groups, each given the discrete topology.

Let A be a group, endowed with the discrete topology, on which G acts continuously. For $g \in G$ and $a \in A$, we denote the action of g on a by ${}^g a$. We call such groups *G-groups* if the structure of A is invariant under the action of G, i.e., ${}^g(ab) = ({}^g a)({}^g b)$ for all a, b in A. Commutative G-groups are also called G-modules.

Let A be a G-group. A *cocycle of G in A* is a continuous map $g \to a_g$ from G to A which satisfies the cocycle relation

$$a_{gh} = a_g \cdot {}^g a_h$$

for all $g, h \in G$. The set of such cocycles is denoted $Z^1(G, A)$.

Two cocycles a and a' are said to be *cohomologous* if there exists $b \in A$ such that

$$a'_g = b^{-1} a_g \, {}^g b$$

for all $g \in G$. One writes $a \sim a'$ if a and a' are cohomologous.

Proposition 4 *The binary relation $\sim$ is an equivalence relation on $Z^1(G, A)$.*

Proof: We first prove reflexivity: that is, $a \sim a$ for all $a \in A$. Taking $b = 1$, the identity of A, a is cohomologous to itself.

The relation $\sim$ is symmetric: that is, if $a \sim a'$ then $a' \sim a$. Suppose $a \sim a'$. Then there is some $b \in A$ such that $a'_g = b^{-1} a_g {}^g b$. Thus, $b a'_g ({}^g b)^{-1} = b a'_g {}^g (b^{-1}) = a_g$, and so $a' \sim a$.

The relation $\sim$ is transitive: that is, if $a \sim a'$ and $a' \sim a''$ then $a \sim a''$. Suppose $a \sim a'$ and $a' \sim a''$. Then there exist $b, c \in A$ such that $a'_g = b^{-1} a_g {}^g b$ and $a''_g = c^{-1} a'_g {}^g c$. But then $a''_g = c^{-1} b^{-1} a_g {}^g b {}^g c = (bc)^{-1} a_g {}^g (bc)$, and so $a \sim a'$.

This completes the proof. □

Definition 6 *The quotient of $Z^1(G, A)$ by the equivalence relation $\sim$ is denoted $H^1(G, A)$, and is called* the first cohomology set of G in A.

Note that in general, $H^1(G, A)$ is not a group, but a pointed set, i.e., a set with a distinguished element, corresponding to the class of the trivial cocycle.

We will use two basic results of non-abelian cohomology, both proved in [Ser97].

Proposition 5 *Let $1 \to A \to B \to C \to 1$ be an exact sequence of G-groups. Then there exists a map δ such that the sequence*

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

is exact (in the category of pointed sets).

For a proof, see [Ser97], I, 5.5.

Theorem 10 (Hilbert's Theorem 90) *For every Galois extension $K/\mathbb{Q}$, $H^1(Gal(K/\mathbb{Q}), K^\times) = 0$.*

See [Ser97], II, 1.2.

Proposition 6 $\mathbf{GL_2}(F)/F^\times \simeq \mathbf{PGL_2}(\overline{F})^{G_F}$.

Proof: The sequence

$$1 \to \overline{F}^\times \to \mathbf{GL_2}(\overline{F}) \to \mathbf{PGL_2}(\overline{F}) \to 1$$

is exact. Hence the sequence

$$1 \to F^\times \to \mathbf{GL_2}(F) \to \mathbf{PGL_2}(\overline{F})^{G_F} \to H^1(G_F, \overline{F}^\times)$$

is exact. But by Hilbert's Theorem 90, $H^1(G_F, \overline{F}^\times)$ is trivial, and so

$$\mathbf{GL_2}(F)/F^\times \simeq \mathbf{PGL_2}(\overline{F})^{G_F}.$$

□

3.4.3 Arbitrary fields

In this section we relate the distinct classes of parametric solutions over an arbitrary field F to non-abelian cohomology. The group G_F acts on $\Gamma_{p,q,r}$ with a trivial action. In this case, $H^1(G_F, A_{p,q,r})$ is simply the set $Hom(G_F, A_{p,q,r})$, modulo conjugation by $A_{p,q,r}$.

Let $\rho : \Gamma_{p,q,r} \to \mathbf{PGL_2}(\overline{F})$ be an F-rational embedding. Then for every

$\sigma \in G_F$, there exists a unique $c(\sigma) \in A_{p,q,r}$ such that ${}^{\sigma}\rho = \rho \cdot c(\sigma)$. In fact,

$$\begin{aligned} {}^{\sigma\tau}\rho = {}^{\sigma}({}^{\tau}\rho) &= {}^{\sigma}(\rho \cdot c(\tau)) \\ &= \rho \cdot c(\sigma)c(\tau). \end{aligned}$$

so the assignment $\rho \mapsto c$ gives a map from the set of F-rational embeddings to $Z^1(G_F, A_{p,q,r})$.

Let ρ_1 and ρ_2 be two F-rational embeddings of $\Gamma_{p,q,r}$. Suppose they are F-equivalent. Then $\rho_2 = M(\rho_1 \cdot b)M^{-1}$ for some $M \in \mathbf{PGL_2}(F)$ and $b \in A_{p,q,r}$. Let ${}^{M}\rho_1$ denote the conjugation of ρ_1 by M.

Then

$$\begin{aligned} {}^{\sigma}\rho_2 = {}^{\sigma}({}^{M}\rho_1 \cdot b) &= {}^{M}({}^{\sigma}(\rho_1 \cdot b)) \qquad \text{since } M \in \mathbf{PGL_2}(F) \\ &= {}^{M}(\rho_1 \cdot c_1(\sigma) \cdot b) \\ &= {}^{M}(\rho_1 \cdot b(b^{-1}c_1(\sigma)b)) \\ &= \rho_2 \cdot b^{-1}c_1(\sigma)b. \end{aligned}$$

So, conjugate embeddings map to the same cohomology class, and so the function which maps ρ_1 to the class of c_1 is a function from F-equivalence classes of embeddings of $\Gamma_{p,q,r}$ to $H^1(G_F, A_{p,q,r})$.

Hence, φ induces a map from F-equivalence classes of F-rational embeddings of $\Gamma_{p,q,r}$ to the cohomology set $H^1(G_F, A_{p,q,r})$.

Theorem 11 *The map φ is injective.*

Proof: Let ρ_1 and ρ_2 be two F-rational embeddings. From Proposition 3, there exists $M \in \mathbf{PGL_2}(\overline{F})$ such that $\rho_1 = {}^M\rho_2$. Suppose that ρ_1 and ρ_2 map to the same cohomology class. By replacing ρ_2 by $\rho_2 \cdot b$ for some $b \in A_{p,q,r}$, assume that ρ_1 and ρ_2 give rise to the same cocycle. Then

$$\begin{aligned} {}^\sigma\rho_1 &= \rho_1 \cdot c_1(\sigma) \\ &= {}^\sigma({}^M\rho_2) = {}^{\sigma M}({}^\sigma\rho_2) \\ &= {}^{\sigma M}(\rho_2 \cdot c_1(\sigma)) \end{aligned}$$

and so $\rho_1 = {}^{\sigma M}\rho_2 = {}^M\rho_2$. Hence the matrix $M^{-1}({}^\sigma M)$ commutes with all elements of the image of Γ, so that $M^{-1}({}^\sigma M) = 1$. Therefore $M = {}^\sigma M$ for all $\sigma \in G_F$, but $\mathbf{PGL_2}(\overline{F})^{G_F} = \mathbf{PGL_2}(F)$ by Hilbert's Theorem 90. Hence, M belongs to $\mathbf{PGL_2}(F)$, and ρ_1 and ρ_2 are F-equivalent. Thus, φ is one-to-one. □

The map φ is not, in general, surjective. To see this, consider the trivial cocycle in $H^1(G_F, A_{p,q,r})$. If there exists some $\rho : \Gamma \hookrightarrow \mathbf{PGL_2}(\overline{F})$ such that ${}^\sigma\rho = \rho \cdot c(\sigma) = \rho$, then ρ is an embedding of $\Gamma_{p,q,r}$ into $\mathbf{PGL_2}(F)$. Such an embedding need not exist; for example, consider $\Gamma_{2,3,5}$. The elements in $\Gamma_{2,3,5}$ of order 5 have traces in $\mathbb{Q}(\sqrt{5})$, and so there is no embedding of $\Gamma_{2,3,5}$ into $\mathbf{PGL_2}(\mathbb{Q})$. In fact, we will see that for $(p,q,r) = (2,3,3)$, $(2,3,4)$ and $(2,3,5)$, the group $\Gamma_{p,q,r}$ does not embed in $\mathbf{PGL_2}(\mathbb{Q})$. Thus, over $\mathbb{Q}$, the trivial cocycle is never the image of an embedding of $\Gamma_{p,q,r}$ in $\mathbf{PGL_2}(\overline{\mathbb{Q}})$.

3.5 Forms and cohomology

Theorem 11 provides information on the number of equivalence classes of embeddings of Γ. But it does not address the question: when can $\Gamma_{p,q,r}$ be embedded into the group $\mathbf{PGL_2}(F)$? This is closely related to the failure of surjectivity of φ. This failure of surjectivity is accounted for by the existence of non-trivial forms of $\mathbf{PGL_2}(F)$ over $\mathbb{Q}$. Forms of $\mathbf{PGL_2}(F)$ are isomorphic to B^*/F^*, where B^* is the multiplicative group of a quaternion algebra over F, or equivalently, to $\mathrm{Aut}_F(X)$, where X is a conic over F. Note that $\mathbf{PGL_2}(F)$ is in fact $\mathrm{Aut}_F(\mathbb{P}^1)$, and every conic with at least one F-rational point is isomorphic to $\mathbb{P}^1(F)$. Thus, it is natural to replace $\mathbf{PGL_2}(F)$ by $\mathrm{Aut}_F(X)$ and ask: when does there exist a conic X such that $\Gamma_{p,q,r}$ can be embedded in $\mathrm{Aut}_F(X)$? It turns out that this point of view leads to more satisfying answers.

3.5.1 Conics and quaternion algebras

A *conic* X defined over a field F (of characteristic not 2) is the set of points in F^2 satisfying a degree 2 polynomial equation $f(x, y) = 0$, with the condition that X is non-singular. Sometimes it is preferable to homogenize the defining equation for X and to consider it as a projective curve. That is, X can be thought of as the set of points $[x : y : z]$ in $\mathbb{P}_2(F)$ satisfying the equation $F(X, Y, Z) = f(\frac{X}{Z}, \frac{Y}{Z})Z^2 = 0$. The nonsingularity condition is equivalent to asking that the first partial derivatives of F never vanish simultaneously for

some point in $\mathbb{P}_2(F)$. Otherwise, the curve X is said to be *degenerate*.

Proposition 7 *Every projective conic is equivalent to some diagonal form*

$$ax^2 + by^2 + cz^2 = 0.$$

For a proof, see [Lam73], I 2.4. In fact, every conic is equivalent to a quadratic form $ax^2 + by^2 + cz^2 = 0$ with $abc \neq 0$, since the quadratic forms $x^2 = 0$ and $ax^2 + by^2 = 0$ are both degenerate.

Conics and quaternion algebras are intimately related: we now provide some basic definitions and results about quaternion algebras, and explain the connection between the two.

Definition 7 *Let F be a field, $charF \neq 2$, and let $a, b \in F^*$. Define the quaternion algebra $B = (\frac{a,b}{F})$ to be the F-algebra generated by i, j with the relations $i^2 = a$, $j^2 = b$, $ij = -ji$.*

Let $k = ij$: then $k^2 = (ij)(ij) = -ij^2i = -i^2j^2 = -ab$. B is a four-dimensional algebra over F with basis $1, i, j, k$. The following proposition gives some basic results about quaternion algebras which will be useful in what follows.

Proposition 8 *1. $(\frac{-1,1}{F}) \simeq M_2(F)$, the ring of 2×2 matrices over F.*

2. $(\frac{a,b}{F}) \simeq (\frac{ax^2,by^2}{F})$, where $a, b, x, y \in F^\times$.

3. The center of $(\frac{a,b}{F})$ is F.

Proof: (1.) Let $i_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $j_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $i_0^2 = -I$, $j_0^2 = I$, and $i_0 j_0 = -j_0 i_0$. Further, I, i_0, j_0 and $i_0 j_0$ are linearly independent and span $M_2(F)$: they form a basis for $M_2(F)$ as a vector space over F. This proves the result.

(2.) Let $B_1 = (\frac{a,b}{F})$ and $B_2 = (\frac{ax^2,by^2}{F})$. The linear map from B_1 to B_2 which sends $f \in F$ to itself, $i \mapsto xi$ and $j \mapsto yj$ is an isomorphism.

(3.) If $h = \lambda + xi + yj + zk$ is in the center of $(\frac{a,b}{F})$ then in particular, it must commute with i. But

$$(\lambda + xi + yj + zk)i = \lambda i + xa - yk + zj.$$

and

$$i(\lambda + xi + yj + zk) = \lambda i + xa + yk - zj.$$

so $y = 0$ and $z = 0$. Since h is in the center, it must also commute with j, but

$$(\lambda + xi)j = \lambda j + xk.$$

and

$$j(\lambda + xi) = \lambda j - xk.$$

so $x = 0$. Thus, $h \in F$.

□

Let $B = (\frac{a,b}{F})$. For $h = \lambda + xi + yj + zk \in B$, define the *conjugate* of h to be $\overline{h} = \lambda - xi - yj - zk$. This allows us to define the *trace function*, $T(h) = h + \overline{h} = 2\lambda \in F$, and the *norm function*, $N(h) = h \cdot \overline{h} = \lambda - ax^2 - by^2 + abz^2 \in F$. A direct calculation shows that the norm is multiplicative: that is, if $g, h \in B$, then $N(gh) = N(g)N(h)$.

It is the norm function which provides a connection between quaternion algebras and conics. If $T(h) = 0$, then $N(h) = -ax^2 - by^2 + abz^2$ is the defining equation for a conic. Conversely, given any non-degenerate conic, it is possible to construct a corresponding quaternion algebra.

Let X be a non-degenerate conic over the field F. Assume that X is defined by an equation of the form $X : x^2 + ay^2 + bz^2 = 0$. Let B_X be the quaternion algebra $(\frac{-b/a,-b}{F})$.

Suppose $h \in B_X$ and $T(h) = N(h) = 0$. Then $\lambda = 0$ and

$$N(h) = -\frac{b}{a}x^2 - by^2 - \frac{b^2}{a}z^2 = 0.$$

which implies that $x^2 + ay^2 + bz^2 = 0$. That is, $[x : y : z] \in X$. Using projective coordinates for X, h and fh ($f \in F^\times$) map to the same point on X, so X can be identified with the curve

$$\{h \in B_X \mid T(h) = N(h) = 0\}/F^\times.$$

In order to explore the connection between $H^1(G_F, \mathrm{Aut}(\Gamma))$ and embeddings of Γ into $\mathrm{Aut}_{\overline{F}}(X)$, it is necessary to understand the group $\mathrm{Aut}_F(X)$.

Lemma 12 *Let $h \in B = (\frac{a,b}{F})$. Then h is a unit if and only if $N(h) \neq 0$.*

Proof: Suppose that h is a unit. Then h^{-1} exists, and $N(h)N(h^{-1}) = N(hh^{-1}) = N(1) = 1$, so $N(h) \neq 0$.

Now, suppose that $N(h) \neq 0$. Then the equation $h\overline{h} = N(h)$ shows that the inverse of h is $\overline{h}/N(h)$.

Thus, the set of units in B is $B^\times = \{h \in B | N(h) \neq 0\}$. □

Proposition 9 *Let $B = (\frac{a,b}{F})$ be the quaternion algebra associated to the conic X defined over the field F. Then the action of $B^\times$ on X by conjugation yields an injection $B^\times/F^\times \hookrightarrow \mathrm{Aut}_F(X)$.*

Proof: We first prove that $B^\times$ acts on X by conjugation. Since the norm is multiplicative, conjugation preserves the norm.

Let $h_1 = \lambda_1 + x_1 i + y_1 j + z_1 k$ and $h_2 = \lambda_2 + x_2 i + y_2 j + z_2 k$ be two elements of B. Then

$$\begin{aligned} Tr(h_1 h_2) &= 2(\lambda_1\lambda_2 + x_1 x_2 a + y_1 y_2 b - z_1 z_2 ab) \\ &= Tr(h_2 h_1), \end{aligned}$$

which implies that $Tr(hgh^{-1}) = Tr(g)$. Thus, $B^\times$ acts by conjugation on X.

This action is not faithful, since conjugation by any element of $F^\times$ acts as the identity. Elements of $F^\times$ are the only elements of $B^\times$ which commute

with every element of X, and so the action of $B^\times/F^\times$ on X is faithful. This provides a one-to-one map from $B^\times/F^\times$ to $\mathrm{Aut}_F(X)$. □

3.5.2 Forms

In this section we make use of some formal properties of cohomology to prove some very useful results.

Let V, V' be algebraic varieties, defined over a field F. The variety V' is said to be an *F-form* of V if V and V' are isomorphic over $\overline{F}$. Two F-forms of V are said to be *equivalent* if they are isomorphic over F.

Let $E(V)$ be the set of equivalence classes of F-forms of V. Let V' be an F-form of V, and $\varphi : V \to V'$ an isomorphism between them. The group G_F acts on φ by ${}^\sigma\varphi = \sigma\varphi\sigma^{-1}$. Define a map $\tilde{\theta} : E(V) \to Z^1(G_F, \mathrm{Aut}V)$ by the rule $V' \mapsto c_{V'}$, where $c_{V'}(\sigma) = \varphi^{-1} \cdot {}^\sigma\varphi$. The map $c_{V'}$ is a cocycle, since

$$\begin{aligned} c_{V'}(\sigma\tau) &= \varphi^{-1}\sigma\tau\,\varphi\,\tau^{-1}\sigma^{-1} \\ &= (\varphi^{-1}\sigma\,\varphi\,\sigma^{-1})\sigma(\varphi^{-1}\tau\,\varphi\,\tau^{-1})\sigma^{-1} \\ &= c(\sigma)\,{}^\sigma c(\tau). \end{aligned}$$

The map $\tilde{\theta}$ depends on the choice of isomorphism φ.

Let θ be the map from $E(V)$ to $H^1(G_F, \mathrm{Aut}V)$ induced by $\tilde{\theta}$.

Lemma 13 *The map $\theta : E(V) \to H^1(G_F, \mathrm{Aut}V)$ is independent of the choice of isomorphism $\varphi : V \to V'$.*

Proof: Let ψ be an F-automorphism of V''. Then $\psi\varphi : V' \to V''$ is an isomorphism over $\overline{F}$, and

$$\begin{aligned} c_{\psi V''}(\sigma) &= (\psi\varphi)^{-1}\sigma(\psi\varphi)\sigma^{-1} \\ &= \varphi^{-1}\psi^{-1}\sigma\psi\varphi\sigma^{-1} \\ &= (\varphi^{-1}\psi^{-1}\varphi)(\varphi^{-1}\sigma\varphi\sigma^{-1})(\sigma\varphi^{-1}\psi\varphi\sigma^{-1}) \end{aligned}$$

where $\varphi^{-1}\psi\varphi \in \mathrm{Aut}(V')$. So $c_{\psi V''}$ is cohomologous to $c_{V''}$. Thus, the map $V'' \mapsto c_{V''}$ is a well-defined function from equivalence classes of F-forms of V' to $H^1(G_F, \mathrm{Aut}(V'))$. □

Theorem 12 *The map $\theta : E(V') \to H^1(G_F, \mathrm{Aut}V')$ is an isomorphism of pointed sets.*

Proof: The map $V'' \mapsto c_{V''}$ is injective. Indeed, let V'' and V''' be two F-forms of V', and $\psi : V'' \to V'''$ be an isomorphism defined over $\overline{F}$. Suppose $c_{V''}$ is cohomologous to $c_{V'''}$. By modifying V''' by some automorphism, assume that $c_{V''} = c_{V'''}$. Then

$$\begin{aligned} \varphi^{-1}\sigma\varphi\sigma^{-1} &= \varphi^{-1}\psi^{-1}\sigma\psi\varphi\sigma^{-1} \qquad \forall\sigma \in G_F \\ \Rightarrow \qquad {}^{\sigma}\psi &= \psi \qquad \forall\sigma \in G_F \end{aligned}$$

and thus ψ is an isomorphism defined over F.

Further, the distinguished element V' of $E(V')$ is mapped to the distinguished element of $H^1(G_F, \mathrm{Aut}(V'))$, the trivial cocycle. The map defined

above is thus a monomorphism of pointed sets.

To prove surjectivity, we define an injective map $H^1(G_F, \mathrm{Aut}(V)) \to E(V)$ and show that it is the inverse of the map defined in the statement of the theorem.

Given a cocycle $c \in Z^1(G_F, \mathrm{Aut}(V))$, let V_c be the variety defined by the rule

$$V_c(L) = V(\overline{F})^{Gal(\overline{F}/L)},$$

where the group action of $Gal(\overline{F}/L)$ is defined by $\sigma * P = c(\sigma)\,{}^{\sigma}P$.

Suppose c, c' are cohomologous. Then $c(\sigma) = b\,c'(\sigma)\,{}^{\sigma}b^{-1}$ for $b \in \mathrm{Aut}(V)$. Then

$$\begin{aligned} V_c(L) &= \{P \in V(\overline{\mathbb{Q}}) \mid c(\sigma)\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= \{P \in V(\overline{\mathbb{Q}}) \mid bc'(\sigma)\,{}^{\sigma}b^{-1}\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= \{P \in V(\overline{\mathbb{Q}}) \mid bc'(\sigma)\sigma b^{-1}\sigma^{-1}\sigma P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\}. \end{aligned}$$

and

$$V_{c'}(L) = \{P \in V(\overline{\mathbb{Q}}) \mid c'(\sigma)\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\}.$$

The map $P \mapsto b^{-1}P$ is an isomorphism between $V_{c'}$ and V_c. Thus, cocycles in the same class map to a well-defined class of F-forms of V. This provides a map $H^1(G_F, \mathrm{Aut}(V)) \to E(V)$.

Now, suppose that c and c' map to the same class of F-forms. By altering c' by an automorphism, we can assume that they map to the same variety, V_c. Then

$$\begin{aligned} V_c(L) &= \{P \in V(\overline{\mathbb{Q}}) \mid c(\sigma)\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= \{P \in V(\overline{\mathbb{Q}}) \mid c'(\sigma)\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= V_{c'}(L). \end{aligned}$$

for all Galois extensions $L/\overline{\mathbb{Q}}$. Then for all $P \in V_c(L)$, $c(\sigma)^{\sigma}P = c'(\sigma)^{\sigma}P$, and so $c(\sigma) = c'(\sigma)$ on $V_c(L)$. Since every P is in $V_c(L)$ for some field extension L, the action of c and the action of c' is the same on every $P \in V$. Thus, $c(\sigma) = c'(\sigma)$ and this map is one-to-one.

Finally, we prove that composing the two maps gives the identity. Given V'', an F-form of V, and $\varphi : V \to V''$.

$$\begin{aligned} V_{c_{V''}} &= \{P \in V(\overline{\mathbb{Q}}) \mid c_{V''}(\sigma)\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= \{P \in V(\overline{\mathbb{Q}}) \mid \varphi^{-1}\sigma\varphi\sigma^{-1}\,{}^{\sigma}P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= \{P \in V(\overline{\mathbb{Q}}) \mid \sigma\varphi P = \varphi P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \end{aligned}$$

and

$$\begin{aligned} V''(L) &= \{P \in V''(\overline{\mathbb{Q}}) \mid \sigma P = P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \\ &= \{P \in V(\overline{\mathbb{Q}}) \mid \sigma\varphi P = \varphi P \quad \forall \sigma \in Gal(\overline{\mathbb{Q}}/L)\} \end{aligned}$$

so $V_{\varphi''}(L) = V''(L)$ for all Galois extensions $L/\overline{\mathbb{Q}}$. so $V_{\varphi''} = V''$. □

This very useful theorem is the key ingredient in the proof of the following proposition.

Proposition 10 *Let X be a conic defined over F, and let B be the quaternion algebra associated to it. Then the inclusion of Proposition 9 $B^\times/F^\times \hookrightarrow \mathrm{Aut}_F(X)$ is an isomorphism.*

Proof: All conics defined over F are forms of $\mathbb{P}^1(F)$, since every conic with at least one rational point is isomorphic to $\mathbb{P}^1(F)$. Therefore $\mathrm{Aut}_F(X)$ is a form of $\mathrm{Aut}_F(\mathbb{P}^1) \simeq \mathbf{PGL_2}(F) = M_2(F)^\times/F^\times$. The F-forms of $M_2(F)$ are the quaternion algebras (see [Ser97], III 1.4), and so the F-forms of $\mathbf{PGL_2}(F)$ are the unit groups of the quaternion algebras, modulo scalars. Thus, $\mathrm{Aut}_F(X) \simeq B_X^\times/F^\times$. □

3.6 Examples

The examples given in Section 2.4 can be reinterpreted as embeddings of $\Gamma_{p,q,r}$ into the automorphism group of $\mathbb{P}^1(\overline{\mathbb{Q}})$. We would like to consider embeddings of $\Gamma_{p,q,r}$ into the automorphism groups of conics defined over $\mathbb{Q}$.

Consider first A_4 and S_4. The usual quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ corresponds to the conic $X : x^2 + y^2 + z^2 = 0$. The group S_4 acts on this conic in a natural way. The automorphism γ defined by

$$[x : y : z] \mapsto [y : z : x]$$

has order 3, and the automorphism β defined by

$$[x : y : z] \mapsto [x : -z : y]$$

has order 4. The composition $\beta\gamma$ is of the form

$$[x : y : z] \mapsto [y : x : -z].$$

which has order 2. The group generated by β and γ is isomorphic to $\Gamma_{2,3,4}$. This gives an embedding of S_4 (and therefore also A_4) into $\mathrm{Aut}_{\mathbb{Q}}(X)$.

It is more difficult to come up with an embedding of A_5 into the automorphism group of some conic. We follow [Ser80] in the following example.

Consider the quadric surface Y in $\mathbb{P}^4$ defined by the two equations

$$X_1 + X_2 + X_3 + X_4 + X_5 = 0 \tag{5}$$

and

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0. \tag{6}$$

Permutation of the coordinates gives a natural action of S_5 on this surface, and this action is defined over $\mathbb{Q}$. Let ζ be a primitive fifth root of unity, and let

$$\begin{aligned}
U_1 &= X_1 + X_2 + X_3 + X_4 + X_5, \\
U_2 &= X_1 + \zeta X_2 + \zeta^2 X_3 + \zeta^3 X_4 + \zeta^4 X_5, \\
U_3 &= X_1 + \zeta^2 X_2 + \zeta^4 X_3 + \zeta X_4 + \zeta^3 X_5, \\
U_4 &= X_1 + \zeta^3 X_2 + \zeta X_3 + \zeta^4 X_4 + \zeta^2 X_5, \\
U_5 &= X_1 + \zeta^4 X_2 + \zeta^3 X_3 + \zeta^2 X_4 + \zeta X_5.
\end{aligned}$$

In this new system of coordinates, equations (5) and (6) are equivalent to the two equations $U_1 = 0$ and $U_2U_5 = -U_3U_4$.

The lines on Y are divided naturally into two sets. The equations $U_2 = \lambda U_3$, $\lambda U_5 = -U_4$, describe the line $a(\lambda U_2 + U_3) + b(\lambda U_4 + U_5)$. Let $\mathcal{X}_1$ be the set of lines of this form. If $U_2 = \lambda U_4$, and $\lambda U_5 = -U_3$, we have the line $a(\lambda U_2 + U_4) + b(\lambda U_3 - U_5)$. Let $\mathcal{X}_2$ be the set of lines of this form. Since both $\mathcal{X}_1$ and $\mathcal{X}_2$ are parametrized by λ, each is isomorphic over $\overline{\mathbb{Q}}$ to $\mathbb{P}^1$. Let $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$.

Every automorphism of Y acts on $\mathcal{X}$, so the action of S_5 on Y induces

an action of S_5 on X; this action is defined over $\mathbb{Q}$. Elements of A_5 send X_1 to X_1 and X_2 to X_2, while elements of $S_5 \setminus A_5$ interchange them. The Galois group $Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ acts on X by interchanging X_1 and X_2.

More abstractly, let F be the fraction field of $\mathbb{Q}(\sqrt{5})[x, y]/(x^2 + y^2 = -1)$. It has transcendence degree 1 over $\mathbb{Q}$, and so corresponds to a curve over $\mathbb{Q}$. It can be described by the equations $x^2 + y^2 = 1$, $u^2 = 5$.

Lemma 14 *Let X be an irreducible variety over k with function field $k(X)$. Let k' be the maximal separable algebraic extension of k in $k(X)$. Let k'' be the Galois closure of k'. Suppose that k' is finite over k. Then over k'', X splits into $[k' : k]$ irreducible components.*

This is Corollary 4.5.10 of [GD65].

In this case Lemma 14 says that as an extension of $\mathbb{Q}(\sqrt{5})$, F is purely transcendental of transcendence degree 1 over $\mathbb{Q}(\sqrt{5})$. The action of the Galois group $Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$, interchanges the two irreducible components V_1 and V_2 of V over $\mathbb{Q}(\sqrt{5})$.

S_5 can be embedded into $\mathrm{Aut}_{\mathbb{Q}}(V)$. Consider the set

$$I = \left\{ \frac{1}{2}(\pm 2, 0, 0, 0)^A, \frac{1}{2}(\pm 1, \pm 1, \pm 1, \pm 1), \frac{1}{2}(0, \pm 1, \pm(1 - \sqrt{5}), \pm(1 + \sqrt{5}))^A \right\}$$

where (a, b, c, d) represents $a + bi + cj + dk \in B = (\frac{-1,-1}{\mathbb{Q}(\sqrt{5})})$, and where the superscript A means that all even permutations are included in I. This is a group of order 120 in B: it maps to a group of order 60 in $B^\times/\mathbb{Q}(\sqrt{5})^\times$. In fact, $I/\{\pm 1\}$ is isomorphic to A_5. For a discussion, see [CS88], 8.2. Consider

I as a group over $\mathbb{Q}$; that is, consider I as a subgroup of the eight-dimensional algebra with basis $1, i, j, k, \sqrt{5}, i\sqrt{5}, j\sqrt{5}, k\sqrt{5}$. It is fixed by the Galois group $G_{\mathbb{Q}}$. Let $\tilde{I}$ be the set obtained by taking all the odd permutations of the elements of I. Consider the set $S = I \cup \tilde{I}\tau$, where τ is an element of order two that permutes V_1 and V_2. Define a multiplication on S by $x\tau^i \cdot y\tau^j = x\bar{y}\tau^{i+j}$, where $\bar{y}$ denotes the action of $Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ on the coordinates of y. The set S with multiplication as defined above is a group, and is isomorphic to S_5.

3.7 Solutions over $\mathbb{Q}$

3.7.1 Embeddings of $\Gamma_{2,3,3}$ and $\Gamma_{2,3,4}$

Let $\chi(p,q,r) > 0$ and let $\Gamma = \Gamma_{p,q,r}$, with $(p,q,r) = (2,3,3)$ or $(2,3,4)$. In either case, $\mathrm{Aut}(\Gamma) = S_4$. Fix a field F. Consider the set of pairs (ι, X), where X is conic and ι is an F-rational embedding $\iota : \Gamma \hookrightarrow \mathrm{Aut}_{\overline{F}}(X)$. Two such pairs, (ι, X) and (ι', X') are said to be F-isomorphic if there exists an isomorphism $\varphi : X \to X'$ defined over F such that the diagram

$$\begin{array}{ccc} \Gamma & \xrightarrow{\iota} & \mathrm{Aut}_{\overline{F}}(X) \\ & \searrow^{\iota'} & \downarrow \tilde{\varphi} \\ & & \mathrm{Aut}_{\overline{F}}(X') \end{array}$$

commutes. Here $\tilde{\varphi}(\alpha) = \varphi \cdot \alpha \cdot \varphi^{-1}$.

Let Ω_F be the set of pairs (ι, X) modulo F-isomorphism. Note that a

pair (i, X) with $X \simeq \mathbb{P}^1(F)$ gives a parametric solution to the generalized Fermat equation over F.

Define a map θ from $\Omega_{\mathbb{Q}}$ to $H^1(G_{\mathbb{Q}}, A_{p,q,r})$ such that $(i, X) \mapsto c$, where ${}^{\sigma}i = i \cdot c(\sigma)$.

Theorem 13 *Let $\Gamma \simeq A_4$ or S_4. The map θ is an isomorphism.*

Proof: Let $(i, X) \in \Omega_{\mathbb{Q}}$. Since i is a $\mathbb{Q}$-rational embedding, ${}^{\sigma}i = i \cdot c(\sigma)$ for $c(\sigma) \in A_{p,q,r}$. The map $i \mapsto c$ provides a map from $\Omega_{\mathbb{Q}}$ to $H^1(G_{\mathbb{Q}}, A_{p,q,r})$.

Let X be a fixed conic. The proof of Theorem 11, only slightly modified, shows that $i \mapsto c$ is a one-to-one map from the set $\{(i, X)\}$ modulo $\mathbb{Q}$-equivalence to $H^1(G_{\mathbb{Q}}, A_{p,q,r})$.

To complete the proof that the map $\Omega_{\mathbb{Q}} \to H^1(G_{\mathbb{Q}}, A_{p,q,r})$ is one-to-one, it is necessary to prove that if (i, X) and (i', X') map to the same cohomology class c, then $X \simeq X'$ over $\mathbb{Q}$.

There exists an isomorphism $\varphi : X \to X'$ defined over $\overline{\mathbb{Q}}$ such that the following diagram commutes:

$$\begin{array}{ccc} \Gamma & \xrightarrow{i} & \mathrm{Aut}_{\overline{\mathbb{Q}}}(X) \\ & \searrow_{i'} & \downarrow \tilde{\varphi} \\ & & \mathrm{Aut}_{\overline{\mathbb{Q}}}(X') \end{array}$$

where for $\gamma \in \mathrm{Aut}_{\overline{\mathbb{Q}}}(X)$, $\tilde{\varphi}(\gamma) = \varphi\gamma\varphi^{-1}$. Since (i, X) and (i', X') both map

to the same $c \in H^1(G_{\mathbb{Q}}, A_{p,q,r})$, then ${}^{\sigma}i = i \cdot c(\sigma)$ and ${}^{\sigma}i' = i' \cdot c(\sigma)$. Thus,

$${}^{\sigma}i' = {}^{\sigma}(\tilde{\varphi} i) = {}^{\sigma}\tilde{\varphi}\,{}^{\sigma}i = {}^{\sigma}\tilde{\varphi}\, i' \cdot c(\sigma).$$

But ${}^{\sigma}i' = i' \cdot c(\sigma) = \tilde{\varphi} i \cdot c(\sigma)$. Hence, ${}^{\sigma}\tilde{\varphi} = \tilde{\varphi}$, and so φ is defined over $\mathbb{Q}$.

For $\Gamma = A_4$ and $\Gamma = S_4$, $\mathrm{Aut}(\Gamma) = S_4$. Section 3.6 provides an explicit embedding of S_4 into $\mathrm{Aut}_{\mathbb{Q}}(X_1)$, where X_1 is the conic corresponding to the usual quaternion algebra. Let e denote this embedding. The pair (e, X_1) (where for $\Gamma = A_4$, e is meant as the restriction of e to A_4) maps to the trivial cocycle c_1 in $H^1(G_{\mathbb{Q}}, S_4)$. The embedding e also provides a map to $H^1(G_{\mathbb{Q}}, \mathrm{Aut}_{\overline{\mathbb{Q}}}(X_1))$, and, as proved in Theorem 12, elements of this cohomology set correspond to the $\mathbb{Q}$-forms of X_1. Thus, given a cocycle $c \in H^1(G_{\mathbb{Q}}, S_4)$, there is a corresponding cocycle $c_X \in H^1(G_{\mathbb{Q}}, \mathrm{Aut}(X_1))$, which in turn corresponds to a conic X_c.

To prove that the map described above is surjective, we will find an embedding $\iota_c : \Gamma \to \mathrm{Aut}_{\overline{\mathbb{Q}}}(X_c)$ such that ${}^{\sigma}\iota_c = \iota_c \cdot c(\sigma)$.

An isomorphism between X_1 and X_c is equivalent to an isomorphism between the function fields $\mathbb{Q}(X_1)$ and $\mathbb{Q}(X_c)$. Construct an isomorphism $\varphi : \mathbb{Q}(X_1) \to \mathbb{Q}(X_c)$ such that $c_X(\sigma)\,{}^{\sigma}\varphi^{-1} = \varphi^{-1}$. Note that ${}^{\sigma}(\varphi^{-1}) = c_X(\sigma)^{-1}\varphi^{-1}$ and ${}^{\sigma}\varphi = \varphi c_X(\sigma)$.

The map φ provides an isomorphism, also denoted by φ, from X_1 to X_c.

Then $\iota_c := \varphi \cdot c \cdot \varphi^{-1}$ provides an embedding of Γ into $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_c)$. Now,

$$\begin{aligned} {}^{\sigma}\iota_c &= {}^{\sigma}(\varphi \cdot c \cdot \varphi^{-1}) \\ &= {}^{\sigma}\varphi\, {}^{\sigma}c\, {}^{\sigma}\varphi^{-1} \\ &= \varphi c_X(\sigma) c \cdot c_1(\sigma) \cdot c_X(\sigma)^{-1} \varphi^{-1} \\ &= \varphi c \cdot c(\sigma)\, \varphi^{-1}. \end{aligned}$$

since c_1 is the trivial cocycle and since conjugation by $c_X(\sigma)$ is the automorphism of X induced by $c(\sigma)$. Hence, ${}^{\sigma}\iota_c = \iota_c \cdot c(\sigma)$, which proves that the map defined above is surjective. □

To clarify some of the ideas in this proof, we examine a simple example. Instead of a conic, consider the cubic equation $X : x^3 + y^3 = 1$. Let Γ be the group $\mathbb{Z}/3\mathbb{Z}$.

Let $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$, a cube root of one. Γ acts on X by the following rule: $\gamma(x) = \zeta_3 x$, $\gamma(y) = \zeta_3^{-1} y$. Then $\{1, \gamma, \gamma^{-1}\}$ provides a $\mathbb{Q}$-rational embedding of Γ into $\mathrm{Aut}(X)$. This embedding corresponds to the cocycle

$$c_1(\sigma) = \begin{cases} 1 & \text{if } \sigma(\sqrt{-3}) = \sqrt{-3}, \\ -1 & \text{if } \sigma(\sqrt{-3}) = -\sqrt{-3}. \end{cases}$$

$\mathrm{Aut}(\Gamma)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This can also be embedded into $\mathrm{Aut}(X)$: the non-identity element of $\mathrm{Aut}(\Gamma)$ acts by interchanging x and y.

Given a cocycle $c \in H^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}))$, we will demonstrate how to find the

pair $(i_c, X_c) \in \Omega_{\mathbb{Q}}$ which corresponds to it. First, note that $H^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z})) \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Each cocycle corresponds to $\sqrt{d}$ for some squarefree $d \in \mathbb{Q}$. If c corresponds to d, then

$$c(\sigma) = \begin{cases} 1 & \text{if } \sigma(\sqrt{d}) = \sqrt{d}, \\ -1 & \text{if } \sigma(\sqrt{d}) = -\sqrt{d}. \end{cases}$$

The embedding $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{Aut}(X)$ provides a map

$$H^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) \to H^1(G_{\mathbb{Q}}, \mathrm{Aut}(X)),$$

where each cocycle c_X on the right corresponds to some $\mathbb{Q}$-form of X.

Fix a cocycle c corresponding to $\sqrt{d}$. The function field of X is the fraction field of the ring $\mathbb{Q}[x, y]/(x^3 + y^3 = 1)$. Let X_c be a form of X; then the function field of X_c is the fraction field of $\mathbb{Q}[u, v]/I$ for some ideal I. To find an isomorphism from X_c to X we will first find a pair of elements in X which are invariant under $c_X(\sigma)^\sigma$. Two such elements are $x + y$ and $\sqrt{d}(x - y)$, for

$$c_X(\sigma)^{\,\sigma}(x + y) = c_X(\sigma)(x + y) = x + y.$$

and

$$\begin{aligned} c_\chi(\sigma)^\sigma(\sqrt{d}(x-y)) &= \begin{cases} \sqrt{d}(x-y) & \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ -\sqrt{d}(x-y) & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \end{cases} \\ &= \begin{cases} \sqrt{d}(x-y) & \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ -\sqrt{d}(y-x) & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \end{cases} \\ &= \sqrt{d}(x-y). \end{aligned}$$

This provides an isomorphism from $\mathbb{Q}(X_c)$ to $\mathbb{Q}(X)$. Let $u = x + y$, $v = \sqrt{d}(x-y)$. Then $x = \frac{u}{2} + \frac{v}{2\sqrt{d}}$ and $y = \frac{u}{2} - \frac{v}{2\sqrt{d}}$. Rewriting the equation $x^3 + y^3 = 1$ in terms of u and v gives the equation $du^3 + 3uv^2 = 4d$. Thus, $\mathbb{Q}(X_c)$ is the fraction field of the ring $\mathbb{Q}[u,v]/(du^3 + 3uv^2 = 4d)$.

The action of Γ on X_c can be written explicitly using the isomorphism described above. We find that $\Gamma = \{1, \tilde{\gamma}, \tilde{\gamma}^{-1}\}$, where

$$\begin{aligned} \tilde{\gamma}(u) &= \frac{-u}{2} + \frac{\sqrt{-3}}{2\sqrt{d}}v, \\ \tilde{\gamma}(v) &= \frac{\sqrt{-3}\sqrt{d}}{2}u - \frac{v}{2}. \end{aligned}$$

and

$$\begin{aligned} \tilde{\gamma}^{-1}(u) &= \frac{-u}{2} - \frac{\sqrt{-3}}{2\sqrt{d}}v, \\ \tilde{\gamma}^{-1}(v) &= -\frac{\sqrt{-3}\sqrt{d}}{2}u - \frac{v}{2}. \end{aligned}$$

Call this embedding i. A quick calculation reveals that

$$^{\sigma}i = i \cdot c_1(\sigma)c(\sigma),$$

and so (i, X_i) is the pair corresponding to the cocycle c.

3.7.2 Embeddings of $\Gamma_{2,3,5}$

All that is needed in the proof of Theorem 13 is an embedding of $\Gamma_{p,q,r}$ into $\mathrm{Aut}_{\mathbb{Q}}(X)$ for some conic X. Since $\Gamma_{2,3,5}$ has elements of order 5, with traces in $\mathbb{Q}(\sqrt{5})$, such an embedding does not exist. It is possible, however, to embed $\Gamma_{2,3,5}$ into $\mathrm{Aut}_{\mathbb{Q}(\sqrt{5})}(X)$. Hence we can prove that

Theorem 14 $\Omega_{\mathbb{Q}(\sqrt{5})} \simeq H^1(G_{\mathbb{Q}(\sqrt{5})}, A_{p,q,r})$.

The proof is omitted, as it is virtually identical to the proof of Theorem 13.

Let V be the variety described at the end of Section 3.6. Although it is irreducible over $\mathbb{Q}$, over $\overline{\mathbb{Q}}$ it is isomorphic to the union of two curves of genus 0. Consider the set of all pairs (i, X) where X is a form of V (that is, $X(\overline{\mathbb{Q}})$ is isomorphic to two copies of $\mathbb{P}^1$) and $i : S_5 \hookrightarrow \mathrm{Aut}_{\mathbb{Q}}(X)$ a $\mathbb{Q}$-rational embedding. Let $\Omega_{\mathbb{Q}}$ consist of the set of all such pairs, modulo $\mathbb{Q}$-isomorphism.

Theorem 15 *Let $\Omega_{\mathbb{Q}}$ be defined as above. Then $\Omega_{\mathbb{Q}} \simeq H^1(G_{\mathbb{Q}}, S_5)$.*

Proof: The example at the end of Section 3.6 provides an element of $\Omega_{\mathbb{Q}}$ which corresponds to the trivial cocycle in $H^1(G_{\mathbb{Q}}, S_5)$. The proof is virtually

identical to the proof of Theorem 13. □

The question remains: which of the pairs (i_c, X_c) correspond to parametric solutions over $\mathbb{Q}$ to the generalized Fermat equation $x^2 + y^3 = z^5$? Theorem 9 says that there is a one-to-one correspondence between $\mathbb{Q}$-equivalent parametric solutions to this equation (not necessarily defined over $\mathbb{Q}$) and $\mathbb{Q}$-rational embeddings of A_5 into $\mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{P}^1)$. A pair $(i, X) \in \Omega_{\mathbb{Q}}$ gives an embedding of A_5 into $\mathrm{Aut}_{\mathbb{Q}}(X)$: if this embedding produces a parametric solution over $\mathbb{Q}$ to the generalized Fermat equation then X must be isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1(\mathbb{Q}) \cup \mathbb{P}^1(\mathbb{Q})$.

Thus, we are interested in varieties X_c which have rational points: these varieties must be reducible to two conics defined over $\mathbb{Q}$, at least one of which is isomorphic to $\mathbb{P}^1(\mathbb{Q})$. Let X_c be a form of V, with corresponding function field L_c. Let $L_c' = L_c \cap \overline{\mathbb{Q}}$. The Galois group of L_c' over $\mathbb{Q}$ acts on the two components of X_c by interchanging them. Hence, L_c' is at most a quadratic extension of $\mathbb{Q}$, and X_c is reducible over $\mathbb{Q}$ if and only if $L_c' = \mathbb{Q}$.

Proposition 11 *If $c \in H^1(G_{\mathbb{Q}}, S_5)$ then c corresponds to a variety X_c which is reducible to two components over $\mathbb{Q}$ if and only if the map $G_{\mathbb{Q}} \xrightarrow{\varsigma} S_5 \to \{\pm 1\}$ corresponds to the action of $G_{\mathbb{Q}}$ on $\mathbb{Q}(\sqrt{5})$.*

Proof: The variety X_c reduces to two components over $\mathbb{Q}$ if and only if the action of $G_{\mathbb{Q}}$ on X_c fixes globally each of its components. Recall that there is an automorphism of V corresponding to c, denoted c_V, given by $c \cdot c = \varphi^{-1}\sigma\varphi\sigma^{-1}$. Consider this map.

Let $\sigma \in G_{\mathbb{Q}}$. If $\sigma(\sqrt{5}) = \sqrt{5}$, then σ fixes globally the two components of V. Thus, $c_V(\sigma) = \varphi^{-1}\sigma\varphi\sigma^{-1}$ fixes the two components of V, and so $c(\sigma) \in A_5$.

If $\sigma(\sqrt{5}) = -\sqrt{5}$, then σ permutes the two components of V. Thus, $c_V(\sigma) = \varphi^{-1}\sigma\varphi\sigma^{-1}$ permutes the two components of V, and so $c(\sigma) \in S_5 \setminus A_5$.

□

4 Conclusion

The main theorem of Chapter 1 is

Theorem 16 *Let F be an algebraically closed field. Then*

1. *If $\chi(p,q,r) \leq 0$, then the equation $x^p + y^q = z^r$ has no non-trivial parametric solution over F of degree relatively prime to the characteristic of F.*

2. *If $\chi(p,q,r) > 0$, and $N = N(p,q,r) = 2/\chi(p,q,r)$ is relatively prime to $char(F)$, then the equation $x^p + y^q = z^r$ has a parametric solution $(a(t), b(t), c(t))$ such that the degree of the rational function $a(t)^p/c(t)^r$ is equal to N. Any other parametric solution is of the form*

$$\left(a\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(a)}, b\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(b)}, c\left(\frac{g(t)}{h(t)}\right)h(t)^{\deg(c)}\right)$$

for some polynomials $g(t), h(t) \in F[t]$.

The remainder of the paper focuses on the equations with exponents $(2,3,3)$, $(2,3,4)$ and $(2,3,5)$. Explicit parametric solutions to these equations are given, using the relationship between parametric solutions and finite groups of $\mathbf{SO_3}$-type. This relationship was constantly exploited and virtually every statement in this paper about parametric solutions has an analog as a statement about embeddings of groups.

Thus, most results of the paper describe properties of embeddings of A_4, S_4 and A_5 into automorphism groups of conics. We prove that non-equivalent

embeddings of the above groups into $\mathbf{PGL}_2(F)$ correspond bijectively to elements in a certain cohomology set. We go on to prove that a bijection exists between the set

$$\{(\iota, X) \mid X \text{ a conic}, \ \iota : \Gamma \hookrightarrow \mathrm{Aut}(X) \text{ a } \mathbb{Q}\text{-rational embedding}\}$$

and $H^1(G_{\mathbb{Q}}, \mathrm{Aut}(\Gamma))$, when $\Gamma = A_4$ or S_4. A similar result holds for A_5: consider the set of pairs (ι, X) where $X(\mathbb{Q})$ is isomorphic to the union of two conics, and ι is a $\mathbb{Q}$-rational embedding of S_5 into $\mathrm{Aut}(X)$. There is a bijection between this set and $H^1(G_{\mathbb{Q}}, S_5)$, and we give an explicit description of those cocycles which correspond to embeddings giving a parametric solution over $\mathbb{Q}$.

References

[Art91] M. Artin. *Algebra.* Prentice-Hall. Inc., Englewood Cliffs. New Jersey. 1991.

[Beu98] F. Beukers. The diophantine equation $ax^p + by^q = cz^r$. *Duke Math. J.*, 91(1):61–88. 1998.

[Che51] C. Chevalley. *Introduction to the Theory of Algebraic Functions of one Variable.* Waverley Press. Inc., 1951.

[CS88] J.H. Conway and N.J.A. Sloane. *Sphere Packings. Lattices and Groups.* Springer-Verlag. New York. 1988.

[GD65] A. Grothendieck and J.A. Dieudonné. Eléments de géometrie algébrique iv: Etude locale des schémas et des morphismes de schémas (seconde partie). *Publ. Math. IHES.* 24. 1965.

[Har77] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag. New York. 1977.

[Hun74] T. Hungerford. *Algebra.* Springer-Verlag, New York. 1974.

[Lam73] T. Y. Lam. *The Algebraic Theory of Quadratic Forms.* W.A. Benjamin. Inc., Reading. Massachussetts. 1973.

[Lor96] D. Lorenzini. *An Invitation to Arithmetic Geometry.* American Mathematical Society, Providence. Rhode Island. 1996.

[Ser80] J.P. Serre. Extensions icosaédriques. In *Séminaire de Théorie des Nombres de Bordeaux*. 1980.

[Ser97] J. P. Serre. *Galois Cohomology*. Springer-Verlag, Berlin Heidelberg, 1997.