Aspects of $x + y - z = 1$ in positive characteristic

Inauguraldissertation
zur
Erlangung der Würde eines Doktors der Philosophie

vorgelegt der
Philosophisch-Naturwissenschaftlichen Fakultät
der Universität Basel

von

Dominik Leitner
aus
Basel, Schweiz

Basel, 2013

Genehmigt von der Philosophisch-Naturwissenschaftlichen Fakultät auf Antrag von Prof. Dr. David Masser und Prof. Dr. Felipe Voloch.

Basel, den 26. Februar 2013

Prof. Dr. Jörg Schibler
Dekan

Contents

1 Introduction

The basic problem in diophantine analysis is to solve polynomial equations in rational integers, but this is recognized as hopelessly difficult even in relatively simple situations. For example at present there is no known algorithm to determine if the equation

$$x^4 - 2y^4 + xy - x \ = \ 2013 \tag{1.1}$$

has a solution in integers x, y. Or whether the equation

$$x^3 + y^3 + z^3 \ = \ 3 \tag{1.2}$$

has any solutions with $x \neq -5, 1, 4$.

The problem changes if we restrict the unknowns, and for example it has been known for nearly 800 years that the line $x + y = 1$ (and now we are in diophantine geometry) has exactly two points with x a power of 2 and y a power of -3. And there are algorithms to determine if for example (1.1) has such a point. It is known that for general curves there are at most finitely many points except for trivial cases as for example the line $x = 1$.

The natural extension is to allow x and y to lie in multiplicative subgroups of $\mathbb{Q}^*$ which are finitely generated, and it is no loss of generality to take them as the same group G, which in the example above would be generated by 2 and -3. Such problems are associated with the names Mordell-Lang.

This sometimes allows the linearization of the problem; for example (1.1) leads to an equation

$$\frac{1}{2013}x_1 - \frac{2}{2013}x_2 + \frac{1}{2013}x_3 - \frac{1}{2013}x_4 \ = \ 1$$

with x_1, x_2, x_3, x_4 in the above group. We could even eliminate the coefficients to get

$$x_1 + x_2 + x_3 + x_4 \ = \ 1$$

with unknowns in the bigger group generated by $-3, 2, 2013$; but in practice this can be a wasteful trick.

Another fruitful way of restricting the unknowns is to roots of unity whose order is itself unknown. Such problems are associated with the names Manin-Mumford. For (1.1) it is clear at once that there are no points, and for the line $x + y = 1$ a moment's thought involving the intersection of two circles shows that there are exactly two points. And (1.2) is a borderline case, but also one sees quickly that there are exactly 27 points. Again for general curves there are at most finitely many points except for trivial cases like $x = 1$ above or also like $xy = 1$.

A way of combining these situations is to take the unknowns in the radical $\sqrt{G}$ of G, defined as the set of γ for which there exists a positive integer s with γ^s in G. So the radical of the trivial group in $\mathbb{C}$ is the set of all roots of unity ζ. And the radical of the group generated by 2 and -3 is the set of all $2^\alpha 3^\beta \zeta$ with α, β rational.

We now discuss in more detail a linearized equation in arbitrarily many unknowns over an arbitrary field.

Let K be a field and let G be a finitely generated subgroup of the multiplicative group K^*. As we have seen, equations of the form

$$a_1 x_1 + \cdots + a_n x_n \ = \ 1, \tag{1.3}$$

to be solved with unknowns $x_1, \ldots, x_n$ in G, play a central role in number theory and diophantine geometry. Here $a_1, \ldots, a_n$ are considered constants in K, and for convenience we take them in K^*. We can clearly suppose $n \geq 2$.

Much is known about (1.3). Here it is necessary to divide into two cases depending on the characteristic of K.

In zero characteristic a simple example is given by the field $K = \mathbb{Q}$ and the multiplicative subgroup G consisting of all elements $3^a 5^b 7^c$ with integers a, b, c together with the equation $x + y - z = 1$. Here we certainly see an infinite family

$$(1, y, y) \quad (y \in G) \tag{1.4}$$

and the similar $(x, 1, x)$ $(x \in G)$. But in addition we find for example 172 solutions over G with $|a|, |b|, |c| \leq 2$ coming from

$$\begin{array}{rcccccccc}
6 & = & 1 & + & 5^1 & = & 3^1 & + & 3^1 \\
8 & = & 1 & + & 7^1 & = & 3^1 & + & 5^1 \\
10 & = & 1 & + & 3^2 & = & 5^1 & + & 5^1 \\
10 & = & 1 & + & 3^2 & = & 3^1 & + & 7^1 \\
10 & = & 5^1 & + & 5^1 & = & 3^1 & + & 7^1 \\
12 & = & 5^1 & + & 7^1 & = & 3^1 & + & 3^2 \\
14 & = & 7^1 & + & 7^1 & = & 3^2 & + & 5^1 \\
16 & = & 1 & + & 3^1 5^1 & = & 3^2 & + & 7^1 \\
22 & = & 1 & + & 3^1 7^1 & = & 3^1 5^1 & + & 7^1 \\
26 & = & 1 & + & 5^2 & = & 5^1 & + & 3^1 7^1 \\
28 & = & 7^1 & + & 3^1 7^1 & = & 3^1 & + & 5^2 \\
30 & = & 5^1 & + & 5^2 & = & 3^2 & + & 3^1 7^1 \\
36 & = & 1 & + & 5^1 7^1 & = & 3^1 5^1 & + & 3^1 7^1 \\
46 & = & 1 & + & 3^2 5^1 & = & 5^2 & + & 3^1 7^1 \\
50 & = & 1 & + & 7^2 & = & 5^1 & + & 3^2 5^1 \\
50 & = & 1 & + & 7^2 & = & 5^2 & + & 5^2 \\
50 & = & 1 & + & 7^2 & = & 3^1 5^1 & + & 5^1 7^1 \\
52 & = & 3^1 & + & 7^2 & = & 3^2 5^1 & + & 7^1 \\
54 & = & 5^1 & + & 7^2 & = & 3^2 & + & 3^2 5^1 \\
64 & = & 1 & + & 3^2 7^1 & = & 3^1 5^1 & + & 7^2 \\
70 & = & 7^1 & + & 3^2 7^1 & = & 3^2 5^1 & + & 5^2 \\
70 & = & 21 & + & 7^2 & = & 3^2 5^1 & + & 5^2 \\
84 & = & 5^1 7^1 & + & 7^2 & = & 3^2 & + & 3^1 5^2 \\
246 & = & 1 & + & 5^1 7^2 & = & 3^2 5^2 & + & 3^1 7^1
\end{array}$$

The huge number here may of course be due to the small exponents a, b, c, but also when restricting to exponents having absolute value at most 10 for example we find 892 additional solutions anyhow.

Let us return to the general case (1.3) in zero characteristic. It was proved independently by Evertse [E] in 1984 and van der Poorten and Schlickewei [PS] in 1991 that there are at most finitely many solutions of (1.3) which satisfy the subsum restriction $\sum_{i \in I} a_i x_i \neq 0$ for every non-empty subset I of $\{1, \ldots, n\}$. This is a minor restriction because if it fails, then we may use induction to reduce the number of variables. In particular for three-term equations it shows that there are at most finitely many solutions, and for more terms it leads easily to a complete structure.

For our example above it shows there are at most finitely many solutions in addition to the two infinite families from (1.4). Thus for example, there are at most finitely many solutions to the equation

$$3^a + 5^b - 7^c = 1 \tag{1.5}$$

in non-negative integers a, b, c and indeed we will prove in Appendix D (which we published as [Le1]) that the only solutions of (1.5) are $a = b = c = 0$ and $a = b = c = 1$.

However, as far as we know no-one has yet succeeded in giving the full set of solutions for the above example with $x + y - z = 1$ and G the subgroup generated by 3,5 and 7 in $\mathbb{Q}$.

A compensation may be that the number of solutions when finite can be explicitly estimated from above. But the work [ESS] of Evertse, Schlickewei and Schmidt provides only the upper bound $\exp(4.18^9) \approx 10^{344585380964}$, which is little use in actually finding the solutions. The same can be said even for the great improvement $24^{1944} \approx 10^{2683}$ by Amoroso and Viada [AmVi].

Now suppose that K has positive characteristic p. The result of Evertse, van der Poorten and Schlickewei then becomes false. The simplest counterexample comes from the equation

$$x + y \ = \ 1 \tag{1.6}$$

over the function field $K = \mathbb{F}_p(t)$ with $G = \langle t, 1-t \rangle$ generated by t and $1 - t$. Namely if $q = 1, p, p^2, \ldots$ then

$$x \ = \ t^q, \qquad y \ = \ (1-t)^q \ = \ 1 - t^q \tag{1.7}$$

clearly supply infinitely many solutions unrestricted by subsums.

A less simple counterexample was observed in 2004 by Masser [Mas1] for the equation

$$x + y - z \ = \ 1 \tag{1.8}$$

with the same K and G. Namely there is a doubly infinite family of solutions

$$x \ = \ t^{(q-1)q'}, \qquad y \ = \ (1-t)^{qq'}, \qquad z \ = \ t^{(q-1)q'}(1-t)^{q'} \tag{1.9}$$

with q, q' ranging independently over $1, p, p^2, \ldots$

The situation here had been clarified in 1992 by Abramovich and Voloch [AbVo] who showed (in a much more general semiabelian context) that such counterexamples can arise only when the equation (1.3) is essentially defined over a finite field; of course (1.6) and (1.8) are literally defined over $\mathbb{F}_p$. See also the papers of Voloch [Vol1] and especially [Vol2] for $n = 2$ in the context of our Appendix C.

A full structure theorem was found at about the same time by Moosa and Scanlon [MS1],[MS2] (also in the more general context). Independently Derksen and Masser [DM] have given an alternative proof in the present context (amounting to that of the multiplicative group $\mathbb{G}_m^n$) which is completely effective in the logical sense. As is well-known, this is not yet possible in zero characteristic. However, see our result on (1.5) in Appendix D.1 published in [Le1]. But as hinted above there are many effective results about counting; for brevity we mention here just [ESS] of Evertse, Schlickewei and Schmidt on (1.3) and the paper [HP] of Hrushovski and Pillay for transcendental points in the more general context.

In Theorem $1(G)$ and Theorem $2(G)$ of the present thesis we give all solutions of (1.6) and (1.8) respectively with x, y, z in the above $G = \langle t, 1-t\rangle$. And indeed we follow broadly the strategy of [DM] in our proof. Things are naturally simpler for the special equation. But what is also new in the present thesis is a uniformity in the characteristic. The results of the authors quoted above are all for fixed p. Thus our work is in tune with an existing vague philosophy that the solution set should not depend too much on p. Indeed Hrushovski [H] (p.669), who substantially generalized the work of [AbVo], has expressed the expectation that *"quantifier elimination and elimination of imaginaries hold already in the differential language, without the distinguished basis, and in this language the proof should become entirely uniform with respect to the characteristic."* As far as we know, our work is a first confirmation of this expectation, albeit at an elementary level. In fact we show that the solution set has a uniform shape independently of the prime $p \geq 5$ (and we also treat fully the cases $p = 2, 3$).

Actually our result for $p = 2$ can also be found in the article [ABB] of Arenas-Carmona, Berend and Bergelson. Thus our Theorem $1(G)$ for $p = 2$ is essentially their Lemma 5.6 (p.348) and our Theorem $2(G)$ for $p = 2$ is essentially their Proposition 4.1 (p.345). Here the S_4-symmetry with 24 elements has reduced our set $\mathcal{T}_2$ with 24 points to the quadrangle Q_1 (compare the point Π^* in Proposition 3) and our set $\mathcal{T}$ with 216 points to 9 quadrangles $Q_2, \ldots, Q_{10}$ (compare the points $\Pi_1, \ldots, \Pi_9$ in Proposition 3).

But before presenting Theorem $1(G)$ and Theorem $2(G)$ we state one of the main results of [DM] for general K and G, for simplicity in affine rather than projective form. Some preliminary definitions are needed.

We define a G-automorphism ψ of K^n by an equation

$$\psi(x_1, \ldots, x_n) \;=\; (g_1 x_1, \ldots, g_n x_n) \tag{1.10}$$

with $g_1, \ldots, g_n$ in G (this is group translation in $\mathbb{G}_m^n$ disguised).

For a power q of the characteristic p we denote by $\varphi = \varphi_q$ the Frobenius with $\varphi(x) = x^q$. Let $\psi_1, \ldots, \psi_h$ be G-automorphisms. Then we imitate commutator brackets by defining the operator

$$[\psi_1, \ldots, \psi_h] \;=\; [\psi_1, \ldots, \psi_h]_q \;=\; \bigcup_{e_1=0}^{\infty} \cdots \bigcup_{e_h=0}^{\infty} (\psi_1^{-1}\varphi^{e_1}\psi_1) \cdots (\psi_h^{-1}\varphi^{e_h}\psi_h), \tag{1.11}$$

with of course the identity interpretation if $h = 0$.

For example with $q = p, h = 1$ and $\psi_1 = \psi$ as the identity automorphism, we have for a point Π

$$[\psi]_p \Pi \;=\; \bigcup_{e=0}^{\infty} \varphi^e \Pi \;=\; \{\Pi, \Pi^p, \Pi^{p^2}, \ldots\}$$

as in (1.7) with $\Pi = (t, 1-t)$. Or with $q = p, h = 2$ and again ψ_1 as the identity automorphism, $[\psi_1, \psi_2]_p \Pi$ is the union over $q = p^{e_2}$ and $q' = p^{e_1}$ of the $\left(\psi_2^{-1}(\psi_2 \Pi)^q\right)^{q'}$. For suitable ψ_2, Π (see (1.13) below) this reduces to (1.9).

We will need the radical $\sqrt{G} = \sqrt[K]{G}$ as above; it is the group of γ in K for which there exists a positive integer s such that γ^s lies in G.

We generalize (1.3) by treating linear varieties V defined by the vanishing of linear polynomials of degree at most 1 in $x_1, \ldots, x_n$. Thus the object of study is $V \cap G^n$, which we abbreviate to $V(G)$. A special role is played when all the equations have the form $x_i = a$ or $x_i = ax_j$ $(a \neq 0, i, j = 1, \ldots, n)$; these we call cosets (they are in fact particular sorts of group cosets in $\mathbb{G}_m^n$). A point is of course a coset.

Theorem (Derksen-Masser, 2012). *Let K be a field of positive characteristic p, let V be a linear variety defined over K, and suppose that G in K^* is a finitely generated group. Then there is a power q of p such that $V(G)$ is an effectively computable finite union of sets $[\psi_1, \ldots, \psi_h]_q T(G)$ with $\sqrt{G}$-automorphisms $\psi_1, \ldots, \psi_h$ $(0 \leq h \leq n-1)$, and cosets T contained in V.*

This follows immediately from Theorem 1 (p.1049) of [DM] on noting that V is defined over a finitely generated extension of $\mathbb{F}_p$ inside which the radical is also finitely generated.

Here are our main results for (1.6) and (1.8) over G, in which ψ_0 denotes the identity automorphism. The results are already published in [Le2]. First for (1.6), whose statement (and proof) is relatively simple.

Theorem 1(G)**.** *Suppose $k = \mathbb{F}_p(t)$, $G = \langle t, 1-t \rangle$ and that the line L is defined by $x + y = 1$. Then $L(G)$ is*

$$[\psi_0]_p \Pi^+ \cup [\psi_0]_p \Pi^-$$

for the points

$$\Pi^+ \ = \ (t, 1-t), \quad \Pi^- \ = \ (1-t, t)$$

provided $p \geq 3$, and is

$$[\psi_0]_p \Pi^+ \ \cup \ [\psi_0]_p \Pi^- \ \cup \ [\psi_0]_p \Pi_1^+ \ \cup \ [\psi_0]_p \Pi_1^- \ \cup \ [\psi_0]_p \Pi_2^+ \ \cup \ [\psi_0]_p \Pi_2^-$$

for the additional points

$$\Pi_1^+ \ = \ \left(\frac{1}{t}, \frac{1-t}{t}\right), \quad \Pi_1^- \ = \ \left(\frac{1-t}{t}, \frac{1}{t}\right),$$

$$\Pi_2^+ \ = \ \left(\frac{1}{1-t}, \frac{t}{1-t}\right), \quad \Pi_2^- \ = \ \left(\frac{t}{1-t}, \frac{1}{1-t}\right)$$

when $p = 2$.

Thus for $p \geq 3$ we get not only (1.7) corresponding to Π^+ but also the extra solutions $x = (1-t)^q$, $y = t^q$ corresponding to Π^-. The reason is of course the symmetry of the equation in x, y. For $p = 2$ we get even more solutions, but these can be considered as coming from more symmetry which arises by writing the equation in homogeneous form as $X + Y + Z = 0$.

It is precisely this sort of symmetry which is responsible for the much more complicated situation in (1.8). Define the cosets T_x, T_y and T_z by

$$T_x : \ x = 1, \ y = z, \qquad T_y : \ y = 1, \ x = z, \qquad T_z : \ z = -1, \ y = -x. \qquad (1.12)$$

Theorem 2(G)**.** *Suppose $k = \mathbb{F}_p(t)$, $G = \langle t, 1-t \rangle$ and that the plane P is defined by $x + y - z = 1$. Then $P(G)$ is*

$$T_x(G) \ \cup \ T_y(G) \ \cup \ \bigcup_{\Pi \in \mathcal{T}} [\psi_0, \psi_\Pi]_p \Pi$$

for a set $\mathcal{T}$ of 40 *points* Π *in* G^3 *with* G*-automorphisms* ψ_Π *provided* $p \geq 5$*, and is*

$$T_x(G) \ \cup \ T_y(G) \ \cup \ \bigcup_{\Pi \in \mathcal{T}_3'} [\psi_0]_p \Pi \ \cup \ \bigcup_{\Pi \in \mathcal{T}} [\psi_0, \psi_\Pi]_p \Pi$$

for a set $\mathcal{T}$ of 40 *points* Π *in* G^3 *with* G*-automorphisms* ψ_Π *and a set* $\mathcal{T}_3'$ *of* 8 *points* Π *in* G^3 *when* $p = 3$*, and is*

$$T_x(G) \ \cup \ T_y(G) \ \cup \ T_z(G) \ \cup \ \bigcup_{\Pi \in \mathcal{T}_2} [\psi_0]_p \Pi \ \cup \ \bigcup_{\Pi \in \mathcal{T}} [\psi_0, \psi_\Pi]_p \Pi$$

for a set $\mathcal{T}$ of 216 *points* Π *in* G^3 *with* G*-automorphisms* ψ_Π *and a set* $\mathcal{T}_2$ *of* 24 *points* Π *in* G^3 *when* $p = 2$.

For example $\mathcal{T}$ (for every p) includes the point $\Pi = (1, 1-t, 1-t)$, with

$$\psi_\Pi(x, y, z) \ = \ \left(tx, y, \frac{t}{1-t} z\right), \tag{1.13}$$

and then $[\psi_0, \psi_\Pi]_p \Pi$ is exactly the set (1.9). But there are in all 40 such classes of solutions when $p \geq 3$, and even 216 when $p = 2$.

As hinted above, the large numbers here arise essentially from the symmetry of the special equation $x+y-z = 1$, which in homogeneous form $X+Y = Z+W$ has a natural dihedral D_4-action. When $p = 2$ this is even an S_4-action. But in addition the nature of the special group $G = \langle t, 1-t \rangle$ can be exploited through field automorphisms, which yield an independent S_2-action and for $p = 2$ even an S_3-action.

In view of the effectivity of [DM] our own results may not seem too significant, and things are naturally simpler for the special equation. Also the work of [DM] includes explicit estimates for everything appearing, and so at first sight it may seem that only a computer is needed. But in fact the matter is more complicated, for two main reasons.

First, the estimates in [DM] are not very small. For example equation (12.1) there involves an upper bound which in our situation is

$$B \ = \ \left(144.3^{10} \left(270.5^{15}\right)^7\right)^{43} p^{86} \ > \ 10^{4185} p^{86}.$$

It follows, for example, that each of the g_i in (1.10) is a quotient of polynomials in t of degree at most B. Thus even for $p = 2$ a very large computer would be needed.

Second, in [DM] there is no uniformity in the characteristic p; the coefficients in the polynomials above lie in $\mathbb{F}_p$ and we get no algorithm for treating all p, even if the bound above were independent of p.

Let us now say a few words about the proof. As already mentioned we follow broadly the strategy of [DM], which in general uses differential operators to replace the study of $V(G)$ by that of $W(G)$ for finitely many proper subvarieties W of V. Here we need only $\frac{\mathrm{d}}{\mathrm{d}t}$. For Theorem $1(G)$ about a line, we get at once points. But for Theorem $2(G)$ about a plane we have to cope with lines. Now there is no reason to suppose that these lines will be defined over finite fields, and so one might expect to encounter equations $ax + by = 1$ more general than (1.6). These might easily have caused problems. But by carefully estimating we are in fact able to reduce to (1.6) itself.

So much for $V(G)$. But what about $V(\sqrt{G}) = V \cap (\sqrt{G})^n$, the subject of Theorem $1(\sqrt{G})$ and Theorem $2(\sqrt{G})$? The radical $\sqrt{G}$ is of course no longer finitely generated, so at least this condition in the Theorem of Derksen and Masser fails.

In zero characteristic however the radical makes no difference; for example the result of Evertse, van der Poorten and Schlickewei for (1.3) remains true.

But in positive characteristic the results on $V(G)$ cannot persist for $V(\sqrt{G})$. In fact for $r = p^{-1}, p^{-2}, \ldots$ any γ^r is uniquely defined and then

$$x \;=\; t^r, \qquad y \;=\; (1-t)^r \;=\; 1 - t^r \tag{1.14}$$

as in (1.7) remain solutions of (1.6). And since $\sqrt{G}$ in $K = \overline{\mathbb{F}_p(t)}$ contains $\overline{\mathbb{F}_p}^*$ we even get solutions

$$x \;=\; a, \qquad y \;=\; 1 - a \tag{1.15}$$

for any $a \neq 0, 1$ in $\overline{\mathbb{F}_p}$. Both (1.14) and (1.15) involve quantities of arbitrarily large degree over $\mathbb{F}_p(t)$, and as the only T in (1.6) are points, they cannot be contained in finitely many $[\psi_1, \ldots, \psi_h]_q T(G)$ or even $[\psi_1, \ldots, \psi_h]_q T(\sqrt{G})$.

Nevertheless we will give in our Theorems $1(\sqrt{G})$ and $2(\sqrt{G})$ the full solution set of (1.6) and (1.8) respectively in the radical (or division group) of G in the algebraic closure K of $\mathbb{F}_p(t)$.

In the more general semiabelian context, the earlier works [AbVo] of Abramovich and Voloch and [H] of Hrushovski on radicals were restricted to the "prime-to-p" radical (consisting of all γ in K for which there exists a positive integer s prime to p such that γ^s lies in G). This restriction was broken for the first time by Voloch [Vol2] for $n = 2$ (see Theorem 2 p.198) and more generally by Scanlon in [Sc] regarding problems of Manin-Mumford type. It was Ghioca and Moosa [GM] (p.20) who first treated the full radical (with an isotriviality condition). Their Theorem 3.20 explains the new solutions (1.14) and (1.15). It mentions no cosets T as above, but it is consistent with a statement of the following kind for linear V. Taking into account (1.14), we extend the single brackets in (1.11) to double brackets by

$$[[\psi_1, \ldots, \psi_h]] \;=\; [[\psi_1, \ldots, \psi_h]]_q \;=\; \bigcup_{e_1=-\infty}^{\infty} \cdots \bigcup_{e_h=-\infty}^{\infty} (\psi_1^{-1}\varphi^{e_1}\psi_1) \cdots (\psi_h^{-1}\varphi^{e_h}\psi_h),$$

with again the identity interpretation if $h = 0$. And taking into account (1.15) we introduce more linear varieties W, with a similar abbreviation $W(\overline{\mathbb{F}_p}^*) = W \cap (\overline{\mathbb{F}_p}^*)^n$. Then Masser has suggested that perhaps $V(\sqrt{G})$ is an effectively computable finite union of sets

$$W(\overline{\mathbb{F}_p}^*) \cdot [[\psi_1, \ldots, \psi_h]]_q T(\sqrt{G})$$

with linear varieties W now defined over $\overline{\mathbb{F}_p}$, $\sqrt{G}$-automorphisms $\psi_1, \ldots, \psi_h$ $(0 \leq h \leq n-1)$, and cosets T, with $W \cdot T$ contained in V; here the dot denotes the product in $\mathbb{G}_m^n$. We shall at any rate verify this statement for V as in (1.6) and (1.8) with $G = \langle t, 1-t \rangle$. We now describe our precise results, already submitted for publication as [Le3].

Here is our first result for (1.6) over $\sqrt{G}$, in which ψ_0 denotes the identity automorphism.

Theorem 1$(\sqrt{G})$**.** *Suppose* $K = \overline{\mathbb{F}_p(t)}$, $G = \langle t, 1-t\rangle$ *and that the line* L *is defined by* $x + y = 1$*. Then* $L(\sqrt{G})$ *is*

$$L(\overline{\mathbb{F}_p}^*) \;\cup\; \bigcup_{\Pi}[[\psi_0]]_p\Pi$$

for the following six points Π

$$(t, 1{-}t), (1{-}t, t), \left(\frac{1}{t}, -\frac{1-t}{t}\right), \left(-\frac{1-t}{t}, \frac{1}{t}\right), \left(\frac{1}{1-t}, -\frac{t}{1-t}\right), \left(-\frac{t}{1-t}, \frac{1}{1-t}\right).$$

This result extends Theorem $1(G)$ on $L(G)$, the new features being $L(\overline{\mathbb{F}_p}^*)$ and the double brackets. As in the proof of Theorem $1(G)$ we will take advantage of the symmetry of the equation in x, y. In fact using -1 in $\sqrt{G}$ its homogeneous form is not just $X + Y = Z$ but we even obtain $X + Y + Z = 0$, so an S_2-action becomes an S_3-action.

Here is our second result for (1.8) over $\sqrt{G}$ with again ψ_0 as the identity automorphism.

Theorem 2$(\sqrt{G})$**.** *Suppose* $K = \overline{\mathbb{F}_p(t)}$, $G = \langle t, 1-t\rangle$ *and that the plane* P *is defined by* $x + y - z = 1$*. Then* $P(\sqrt{G})$ *is*

$$P(\overline{\mathbb{F}_p}^*) \;\cup\; T_x(\sqrt{G}) \;\cup\; T_y(\sqrt{G}) \;\cup\; T_z(\sqrt{G})$$
$$\cup \bigcup_{\Pi\in\mathcal{T}'} M_\Pi(\overline{\mathbb{F}_p}^*)\cdot[[\psi_0]]_p\Pi \;\cup\; \bigcup_{\Pi\in\mathcal{T}_p}[[\psi_0]]_p\Pi \;\cup\; \bigcup_{\Pi\in\mathcal{T}}[[\psi_0, \psi_\Pi]]_p\Pi$$

for a set $\mathcal{T}'$ *of 36 points* Π *in* $(\sqrt{G})^3$ *with lines* M_Π*, a set* $\mathcal{T}_p$ *of points* Π *in* $(\sqrt{G})^3$*, and a set* $\mathcal{T}$ *of 216 points* Π *in* $(\sqrt{G})^3$ *with* $\sqrt{G}$*-automorphisms* ψ_Π*. Further if* $p \geq 5$ *then* $\mathcal{T}_p$ *contains 96 points, if* $p = 3$ *then 72 points, and if* $p = 2$ *then just 24 points.*

This result extends Theorem $2(G)$ on $P(G)$, the new features being lines $M_\Pi(\overline{\mathbb{F}_p}^*)$ and the double brackets. For example $\mathcal{T}'$ (for every p) includes the point $\Pi = (t, 1-t, 1-t)$, with M_Π parametrized by $(1, 1+a, a)$, giving rise to solutions

$$(x, y, z) \;=\; (t^q, (1+a)(1-t)^q, a(1-t)^q)$$

for $q = \ldots, p^{-2}, p^{-1}, 1, p, p^2, \ldots$ and $a \neq -1$ in $\overline{\mathbb{F}_p}^*$. But there are in all 36 such classes of solutions.

As for Theorem 2(G) we may take advantage of the natural dihedral D_4-action coming from the homogeneous form $X + Y = Z + W$ of $x + y - z = 1$. But using -1 in $\sqrt{G}$ this even becomes an S_4-action. In addition the nature of the special group $\langle t, 1-t\rangle$ can be exploited through field automorphisms, which then yield an independent S_3-action.

We should mention that it is comparatively easy to deduce the results of Theorem $1(G)$ and Theorem $2(G)$ from the corresponding Theorems over $\sqrt{G}$. And as there, the results over $\sqrt{G}$ are essentially uniform in p.

Let us now say a few words about the proof. Rather than follow [GM], which contains some model theory, we again follow the strategy of [DM] and again it turns out that just $\frac{\mathrm{d}}{\mathrm{d}t}$ is needed. But while the function $f(t) = t^{1/p}$ implicit in (1.14) is especially well-behaved in characteristic p, it is far from differentiable.

So we have to begin with a study of the set of all differentiable functions in $K = \overline{\mathbb{F}_p(t)}$, which is just the separable closure S of $\mathbb{F}_p(t)$. Given any u in K not in $\overline{\mathbb{F}_p}$, there is a minimal $q = \ldots, p^{-2}, p^{-1}, 1, p, p^2, \ldots$ such that u^q lies in S. We apply this for example to $x + y - z = 1$ to get a differentiable solution $x^q + y^q - z^q = 1$ to which the methods from Theorem $2(G)$ can be applied. It turns out that the $M_\Pi(\overline{\mathbb{F}_p}^*)$ in Theorem $2(\sqrt{G})$ arise from the $L(\overline{\mathbb{F}_p}^*)$ in Theorem $1(\sqrt{G})$.

The present thesis is arranged as follows. After studying the separable closure and giving some preliminary tools in chapter 2, we prove Theorem $1(\sqrt{G})$ and Theorem $1(G)$ in chapter 3. Then we treat the equation $x+y-z=1$ over G in chapter 4. A critical role is played by the field of constants C in S, which is used to define for each solution (x, y, z) in S^3 a quantity

$$d \; = \; d(x,y,z) \; = \; \dim_C(Cx + Cy + Cz)$$

Here we split into the two cases $d = 2$ and $d = 3$. We give the proof of Theorem $2(G)$ in chapter 5. For the case over $\sqrt{G}$, which we treat in chapter 6, we prefer to work with the equivalent equation $x+y+z+1 = 0$ or even the homogenized $X + Y + Z + W = 0$, which shows more clearly the S_4-symmetry. Throughout this chapter we closely follow the earlier argumentation of chapter 4. Finally, we prove Theorem $2(\sqrt{G})$ in chapter 7.

There are also four appendices A, B, C, D. In the first two of these we have segregated for the reader's convenience certain parts of the proofs of Theorems $2(G)$ and $2(\sqrt{G})$.

In Appendix C we go briefly into the new topic of unlikely intersections, which vastly generalizes the viewpoints of the thesis so far; in particular now the group G itself is no longer fixed. The resulting problems are associated with the names Zilber-Pink.

Finally in Appendix D we solve fully the equation (1.5) and also the equation

$$y^2 \; = \; 3^a + 2^b + 1$$

mentioned as a problem by Corvaja and Zannier, in which also y^2 no longer lies in a fixed group.

I would like to thank my research supervisor David Masser for suggesting the problems treated here. Throughout my long time at the mathematical institute in Basel I was allowed to get to know the wide world of number theory from him. I am very grateful for his good advice and his valuable support for this PhD thesis.

2 Preliminaries

2.1 Separability and derivations

For the rest of the thesis we now identify $k = \mathbb{F}_p(t)$ and $K = \overline{\mathbb{F}_p(t)}$ the algebraic closure of k. Throughout this section F is an arbitrary subfield of K.
We then start with the following lemma.

Lemma 1. *Let $f \neq 0$ in $F[x]$. Then f has distinct zeros in K if and only if f and f' have no common zero in any extension field of F.*

For the proof see for example Proposition 1.11 of [La3] (p.179).

We may now introduce the concept of separability. A non-zero polynomial f in $F[x]$ is said to be separable over F if each irreducible factor of f in $F[x]$ has distinct zeros in K.

Let E be a field extension over F. Then an element α in E, algebraic over F, is said to be separable over F if its minimal polynomial is separable over F or, equivalently, has distinct zeros in K. Otherwise α is said to be inseparable.

Thus we may state the following useful remark due to the considerations above.

Lemma 2. *Suppose that some polynomial f over F vanishes at some α but its derivative does not. Then α is separable over F.*

Proof. Of course we may assume $f = gD_\alpha$ for some polynomial g over F and D_α the minimal polynomial of α over F. Then $0 \neq f'(\alpha) = g(\alpha)D'_\alpha(\alpha)$ and Lemma 1 implies that D_α has distinct zeros in K, hence α is separable over F and this completes the proof. □

We already noted that not everything in K can be differentiated with respect to t. This can be remedied by restricting to the separable closure S of k defined by

$$S \;=\; \{\alpha \in K \;;\; \alpha \text{ is separable over } k\}\,.$$

It is known that $\frac{\mathrm{d}}{\mathrm{d}t}$ extends uniquely to S (cf. [St] Proposition IV.1.4(a) p.156). We write $\dot{\alpha} = \frac{\mathrm{d}\alpha}{\mathrm{d}t}$ for short.

For any $q = p^e$ $(e \in \mathbb{Z})$ we write F^q for the set of α^q with α in F. It too is a field. It is then clear that $\dot{\alpha} = 0$ for any α in S^p. The converse is probably well-known, but we include a short proof.

Lemma 3. *The set C of all α in S with $\dot{\alpha} = 0$ is S^p.*

Proof. It suffices to show that if $\dot{\alpha} = 0$ then α is in S^p. Consider $F = \mathbb{F}_p(t, \alpha)$. It is clear that $F^p \subseteq F \cap C \subseteq F$. By [St] Proposition III.10.2c(1) (p.144) we have $[F : F^p] = p$. So $F \cap C$ is F^p or F. But $\dot{t} \neq 0$ so $F \cap C \neq F$. Thus $F \cap C = F^p$. In particular α in $F \cap C$ lies in F^p so in S^p, and this completes the proof. □

Lemma 4. *We have $K = \bigcup_{e=0}^{\infty} S^{1/p^e}$.*

Proof. It is known that K is purely inseparable over S (see for example [St] p.329 or [La3] Proposition 6.6 p.250), and this implies the lemma. □

We also need to know that elements of S cannot be simultaneously p^{th} powers, p^2th powers, and so on, unless they are constants. In $\mathbb{F}_p(t)$ this is clear from

$$\bigcap_{e=0}^{\infty} \mathbb{F}_p(t)^{p^e} \;=\; \bigcap_{e=0}^{\infty} \mathbb{F}_p(t^{p^e}) \;=\; \mathbb{F}_p. \tag{2.1}$$

As S contains all of $\overline{\mathbb{F}_p}$, we are after the following result.

Lemma 5. *We have* $\bigcap_{e=0}^{\infty} S^{p^e} = \overline{\mathbb{F}_p}$.

The proof seems to require hyperderivations, so we pause for a discussion. On a general field $\mathcal{K}$ these are maps $\partial_i : \mathcal{K} \to \mathcal{K}$ $(i = 0, 1, 2, \dots)$ satisfying

$$\partial_i(\alpha + \beta) \;=\; \partial_i(\alpha) + \partial_i(\beta), \qquad \partial_i(\alpha\beta) \;=\; \sum_{r+s=i} \partial_r(\alpha)\partial_s(\beta)$$

with ∂_0 the identity map (see also [GV]).

The last of these generalizes immediately to

$$\partial_i(\alpha_1 \cdots \alpha_m) \;=\; \sum_{r_1+\cdots+r_m=i} \partial_{r_1}(\alpha_1) \cdots \partial_{r_m}(\alpha_m).$$

If $\alpha_1 = \cdots = \alpha_m = \alpha$ then this is a sum of various $\partial_0(\alpha)^{s_0} \cdots \partial_i(\alpha)^{s_i}$ for

$$s_0 + s_1 + \cdots + s_i = m, \qquad s_1 + 2s_2 + \cdots + is_i = i \tag{2.2}$$

multiplied by the multinomial coefficients

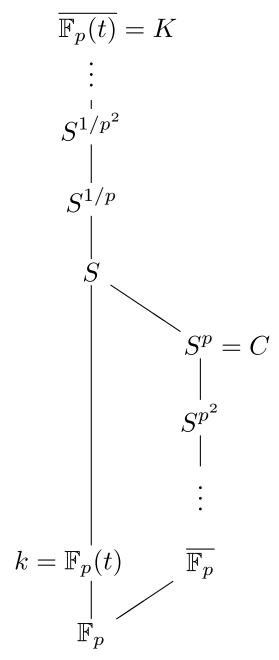
$$\binom{m}{s_0}\binom{m-s_0}{s_1}\binom{m-s_0-s_1}{s_2}\cdots\binom{m-s_0-s_1-\cdots-s_{i-1}}{s_i} \;=\; \binom{m}{s_0, s_1, \dots, s_i}.$$

These are also the coefficients of $X_0^{s_0} X_1^{s_1} \cdots X_i^{s_i}$ in $(X_0 + X_1 + \cdots + X_i)^m$. So if further $m = q \geq 1$ is a power of the characteristic $p > 0$ of $\mathcal{K}$ then we get a non-zero coefficient only if some $s_j = q$ and all others are zero. Then (2.2) implies $jq = i$. If in addition $1 \leq i \leq q$ this means $i = q, j = 1$. We conclude

$$\partial_i(\alpha^q) \;=\; \begin{cases} \partial_1(\alpha)^q & (i = q), \\ 0 & (1 \leq i < q). \end{cases} \tag{2.3}$$

Now for $\mathcal{K} = k$ the ∂_i satisfying $\partial_i(t^m) = \binom{m}{i} t^{m-i}$ are a system of hyperderivatives. This is a "generalized derivation of $\mathcal{K}$ with coefficients in $\mathcal{K}$" in the sense of [G] (p.27). By Corollary 1.3.8 there it extends to the separable closure S, and therefore so do the ∂_i.

We can now prove Lemma 5, wherefore we use the following diagram.



Proof of Lemma 5. As $\overline{\mathbb{F}_p} = \overline{\mathbb{F}_p}^{p^e}$ is in S^{p^e}, it suffices to verify that any α in $S^\infty = \bigcap_{e=0}^\infty S^{p^e}$ is in $\overline{\mathbb{F}_p}$. It satisfies a minimal equation

$$\alpha^d + a_1\alpha^{d-1} + \cdots + a_d \ = \ 0 \tag{2.4}$$

over k. Now for any β in S^∞ and any $s \geq 1$ there is a power $q > s$ of p, and then (2.3) shows that $\partial_s(\beta) = 0$. Then for any γ in S we deduce

$$\partial_i(\gamma\beta) \ = \sum_{r+s=i} \partial_r(\gamma)\partial_s(\beta) \ = \ \partial_i(\gamma)\beta.$$

Applying this to (2.4) with β as the various powers of α we find

$$\partial_i(a_1)\alpha^{d-1} + \cdots + \partial_i(a_d) \ = \ 0 \quad (i = 1, 2, \ldots).$$

These seem to have smaller degree in α. The only way out is $\partial_i(a) = 0$ ($i = 1, 2, \ldots$) for every $a = a_j$.

But we see quickly that this forces each a, already in k, to be in $\mathbb{F}_p$. For example, just taking $i = 1$ gives $a = b^p$ for some b in k. Then taking $i = p$ gives $0 = \partial_p(a) = \partial_1(b)^p$ by (2.3), so $\partial_1(b) = 0$ and $b = c^p$ for some b in k. Then $i = p^2$, and so on; so that each $a = a_j$ lies in (2.1).

Referring back to (2.4) we conclude that α lies in $\overline{\mathbb{F}_p}$, and this completes the proof. □

Lemma 6. *Given any α in K but not in $\overline{\mathbb{F}_p}$ there is e in $\mathbb{Z}$ such that α^{p^e} lies in S but not in C.*

Proof. By Lemma 4 any α in K belongs to some S^{1/p^i} ($i \geq 0$). If $i > 0$ we choose i minimal and put $e = i$. If α^{p^i} were in C then Lemma 3 shows that $\alpha^{p^{i-1}}$ would be in S, contradicting the minimality of i. Otherwise $i = 0$ and (provided α is not in $\overline{\mathbb{F}_p}$) by Lemma 5 there is some maximal $j \geq 0$ with α in S^{p^j}. Here we put $e = -j$. Now if $\alpha^{p^{-j}}$ were in C then we could deduce that $\alpha^{p^{-(j+1)}}$ would be in S, a contradiction again. □

2.2 Wronskians

For the equation (1.8) we require to deal with Wronskians. For us the wronskian $\mathcal{W}(x_1, \ldots, x_n)$ of elements $x_1, \ldots, x_n$ in S is given by the determinant

$$\mathcal{W}(x_1, \ldots, x_n) \;=\; \begin{vmatrix} x_1 & \cdots & x_n \\ D(x_1) & \cdots & D(x_n) \\ \vdots & & \vdots \\ D^{n-1}(x_1) & \cdots & D^{n-1}(x_n) \end{vmatrix}$$

where we use $D^j(x)$ to abbreviate the j^{th} derivative of x with respect to t.

Lemma 7. *Let $x_1, \ldots, x_n$ be in S and $\alpha_1, \ldots, \alpha_n$ be in the field of differential constants C in S. Then*

$$\mathcal{W}(\alpha_1 x_1, \ldots, \alpha_n x_n) \;=\; \alpha_1 \cdots \alpha_n \mathcal{W}(x_1, \ldots, x_n).$$

Proof. The proof results straight from the definition of the Wronskian as well as the fact that $\alpha_1, \ldots, \alpha_n$ are differential constants, namely

$$\mathcal{W}(\alpha_1 x_1, \ldots, \alpha_n x_n) \;=\; \begin{vmatrix} \alpha_1 x_1 & \cdots & \alpha_n x_n \\ D(\alpha_1 x_1) & & D(\alpha_n x_n) \\ \vdots & & \vdots \\ D^{n-1}(\alpha_1 x_1) & \cdots & D^{n-1}(\alpha_n x_n) \end{vmatrix}$$

$$= \begin{vmatrix} \alpha_1 x_1 & \cdots & \alpha_n x_n \\ \alpha_1 D(x_1) & & \alpha_n D(x_n) \\ \vdots & & \vdots \\ \alpha_1 D^{n-1}(x_1) & \cdots & \alpha_n D^{n-1}(x_n) \end{vmatrix} \;=\; \alpha_1 \cdots \alpha_n \mathcal{W}(x_1, \ldots, x_n).$$

□

Lemma 8. *For $y, x_1, \ldots, x_n$ in S we have*

$$\mathcal{W}(y x_1, \ldots, y x_n) \;=\; y^n \mathcal{W}(x_1, \ldots, x_n).$$

Proof. Trivially, the result holds for $y = 0$ and hence we may assume $y \neq 0$. We then define A_m $(1 \leq m \leq n)$ to be the matrix with entries

$$a_{ij} \;=\; \begin{cases} y D^{i-1}(x_j), & i \leq m \\ D^{i-1}(y x_j), & i > m. \end{cases}$$

Thus we see

$$\mathcal{W}(y x_1, \ldots, y x_n) \;=\; \begin{vmatrix} y x_1 & \cdots & y x_n \\ D(y x_1) & \cdots & D(y x_n) \\ \vdots & & \vdots \\ D^{n-1}(y x_1) & \cdots & D^{n-1}(y x_n) \end{vmatrix} \;=\; \det A_1.$$

Writing e_j for the j^{th} row unit vector the row m of A_{m-1} $(2 \leq m \leq n)$ turns out to be

$$\begin{aligned}\sum_{j=1}^{n} e_j D^{m-1}(yx_j) &= \sum_{j=1}^{n} e_j \sum_{i=0}^{m-1} \binom{m-1}{i} D^i(y) D^{m-1-i}(x_j) \\ &= \sum_{j=1}^{n} e_j y D^{m-1}(x_j) + \sum_{i=1}^{m-1} \binom{m-1}{i} \frac{D^i(y)}{y} \sum_{j=1}^{n} e_j y D^{m-1-i}(x_j).\end{aligned}$$

This is row m of A_m modified by linear combinations of the rows $m-1, \ldots, 1$ of A_m. Since the two matrices A_{m-1} and A_m are equal except for row m, it follows that

$$\det A_{m-1} = \det A_m \quad (2 \leq m \leq n).$$

Therefore $\mathcal{W}(yx_1, \ldots, yx_n) = \det A_1 = \cdots = \det A_n = y^n \mathcal{W}(x_1, \ldots, x_n)$, which completes the proof of the present lemma. □

Lemma 9. *For $x_1, \ldots, x_n$ in S we have $\mathcal{W}(x_1, \ldots, x_n) = 0$ if and only if $x_1, \ldots, x_n$ are linearly dependent over the field of differential constants C in S.*

Proof. At first we assume the existence of $\alpha_1, \ldots, \alpha_n$ in C not all zero with $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$. Applying D to this equation we get

$$0 = D(\alpha_1 x_1 + \cdots + \alpha_n x_n) = \alpha_1 D(x_1) + \cdots + \alpha_n D(x_n)$$

and reapplying D we finally see that the columns of $\mathcal{W}(x_1, \ldots, x_n)$ are linearly dependent over C; hence $\mathcal{W}(x_1, \ldots, x_n) = 0$.

For the other direction we use induction on n. For $n = 1$ we have $0 = \mathcal{W}(x_1) = x_1$ and all is trivial. So we consider $n > 1$. If the subdeterminant $\mathcal{W}(x_1, \ldots, x_{n-1})$ is zero, then $x_1, \ldots, x_{n-1}$ are linearly dependent over C and so are $x_1, \ldots, x_n$. Else $\mathcal{W}(x_1, \ldots, x_{n-1}) \neq 0$ and the first $n-1$ columns in $\mathcal{W}(x_1, \ldots, x_n)$ are linearly independent over K. Now $\mathcal{W}(x_1, \ldots, x_n) = 0$ shows that the last column in $\mathcal{W}(x_1, \ldots, x_n)$ is a linear combination of the first $n-1$ columns of $\mathcal{W}(x_1, \ldots, x_n)$; hence there are $\alpha_1, \ldots, \alpha_{n-1}$ in S and $\alpha_n = 1$ with

$$\alpha_1 D^j(x_1) + \cdots + \alpha_n D^j(x_n) = 0 \quad (0 \leq j \leq n-1). \tag{2.5}$$

Applying D to (2.5) and remembering $\alpha_n = 1$ we deduce

$$0 = \sum_{i=1}^{n} \alpha_i D^j(x_i) = \sum_{i=1}^{n} \alpha_i D^{j+1}(x_i) + \sum_{i=1}^{n} D(\alpha_i) D^j(x_i).$$

For $0 \leq j \leq n-2$ the first sum is zero because of (2.5) and so we get

$$D(\alpha_1) D^j(x_1) + \cdots + D(\alpha_{n-1}) D^j(x_{n-1}) = 0 \quad (0 \leq j \leq n-2),$$

a system of equations with variables $D(\alpha_1), \ldots, D(\alpha_{n-1})$ and the determinant $\mathcal{W}(x_1, \ldots, x_{n-1}) \neq 0$. Thus $D(\alpha_1) = \cdots = D(\alpha_{n-1}) = 0$ and so $\alpha_1, \ldots, \alpha_{n-1}$ are in C. On account of (2.5) with $j = 0$ we see that $x_1, \ldots, x_n$ are linearly dependent over C and this completes the proof of the present theorem. □

2.3 More about $\sqrt{G}$

In this section we will procure some of the main tools we will need to prove the theorems.

Henceforth we write $\sqrt[k]{G}$ and $\sqrt[S]{G}$ for the radical of G in k and S respectively.

Lemma 10. *The radical* $\sqrt[k]{G} = \sqrt{G} \cap k$ *is generated by* G *together with the elements of* $\mathbb{F}_p^*$.

Proof. For u in $\sqrt{G}$ we have s in $\mathbb{N}$ such that u^s is in G. Let A be any irreducible polynomial of $\mathbb{F}_p[t]$, which is not a constant multiple of $t, 1-t$. Then the corresponding order function satisfies $\mathrm{ord}_A u^s = 0$, which implies $\mathrm{ord}_A u = 0$. Since this holds for all such A we see that u must lie in the set generated by G and $\mathbb{F}_p^*$. Conversely, we have $G \subset \sqrt{G}$ and further $a^{p-1} = 1$ for a in $\mathbb{F}_p^*$ shows that $\mathbb{F}_p^* \subset \sqrt{G}$, which completes the proof. □

Lemma 11. *Suppose that* q *is a power of* p*, and that* u *is in* k *with* u^q *in* G*. Then* u *is in* G*.*

Proof. By definition u lies in $\sqrt[k]{G}$, so that as we have seen in Lemma 10 $u = ag$ for a in $\mathbb{F}_p^*$ and g in G. But then $a = a^q = \frac{u^q}{g^q}$ lies in G, so $a = 1$. □

Lemma 12. *Let* u *be in the radical* $\sqrt[S]{G} = \sqrt{G} \cap S$*. Then there is* s *in* $\mathbb{N}$ *not divisible by* p *with* u^s *in* G*. Further*

$$\frac{\dot{u}}{u} = \frac{a_0 + a_1 t}{t(1-t)} \qquad \text{and} \qquad \frac{\ddot{u}}{u} = \frac{b_0 + b_1 t + b_2 t^2}{t^2(1-t)^2}$$

for some a_0, a_1, b_0, b_1, b_2 *in* $\mathbb{F}_p$*.*

Proof. There is s in $\mathbb{N}$ with u^s in G. We claim that if s is chosen minimally, then it is not divisible by p. Otherwise with

$$u^s = t^i(1-t)^j \tag{2.6}$$

for integers i, j and $m = \frac{s}{p}$ we get

$$u^m = t^{i/p}(1-t)^{j/p} = (t^{1/p})^i(1-t^{1/p})^j. \tag{2.7}$$

If for example $i \geq 0$ and $j \geq 0$ then this is a polynomial equation $A(t^{1/p}) = 0$ with $A(X) = X^i(1-X)^j - u^m$. Here the derivative (no dot now) $A'(X) = iX^{i-1}(1-X)^j - jX^i(1-X)^{j-1}$ vanishes only if $X = 0$ or $X = 1$ or $i(1-X) = jX$. If i, j in $\mathbb{F}_p$ are not both zero, then the derivative does not vanish at $t^{1/p}$. It would then follow from Lemma 2 that $t^{1/p}$ is separable over S. But this is absurd, as S is the largest separable extension of k and does not contain $t^{1/p}$. It follows that $i = j = 0$ in $\mathbb{F}_p$. But now (2.7) would contradict the minimality of s. Similar arguments work for other sign possibilities; for example if $i \geq 0$ but $j < 0$ then we use the polynomial $A(X) = X^i - u^m(1-X)^{-j}$ and then note that at any point where $A = A' = 0$ but $X \neq 1$ then we also have $f = f' = 0$ for $f(X) = A(X)(1-X)^j = X^i(1-X)^j - u^m$ (which is now only a rational function). This settles the first part of the lemma.

Now the second part of the lemma follows on logarithmically differentiating (2.6) to get

$$\frac{\dot{u}}{u} = \frac{1}{s}\left(\frac{i}{t} - \frac{j}{1-t}\right)$$

and then differentiating to get

$$\frac{\ddot{u}}{u} = \left(\frac{\dot{u}}{u}\right)^2 + \frac{1}{s}\left(-\frac{i}{t^2} + \frac{j}{(1-t)^2}\right).$$

□

Lemma 13. *We have $S^p \cap k = k^p$.*

Proof. It suffices to show that $S^p \cap k \subseteq k^p$. If u is in S^p then $\dot{u} = 0$. But from u in k this means that u is in k^p (cf. [La1] p.185-186). □

Lemma 14. *Let u be in S and suppose $u_1 \neq 0$ in k of degree at most 1 is such that $\frac{u^p}{u_1}$ is in $\sqrt{G}$. Then there is a in $\mathbb{F}_p^*$ such that au_1 belongs to the list*

$$1,\ t,\ 1-t,\ \frac{1}{t},\ -\frac{1-t}{t},\ \frac{1}{1-t},\ -\frac{t}{1-t}. \tag{2.8}$$

Further, if $1-u_1$ lies in $\sqrt{G}$ but not in $\mathbb{F}_p$ then $a=1$ and hence $u_1, 1-u_1$ are both in the sublist

$$t,\ 1-t,\ \frac{1}{t},\ -\frac{1-t}{t},\ \frac{1}{1-t},\ -\frac{t}{1-t}. \tag{2.9}$$

Proof. Let s in $\mathbb{N}$ be as in Lemma 12 not divisible by p and such that $\left(\frac{u^p}{u_1}\right)^s$ is in G. Now u^{sp} is in $S^p \cap k = k^p$ due to Lemma 13 and so u^s lies in k.

Let now A be any irreducible polynomial of $\mathbb{F}_p[t]$ not associate with $t, 1-t$. Then the corresponding order function satisfies

$$0 = \mathrm{ord}_A \frac{u^{ps}}{u_1^s} = p\,\mathrm{ord}_A u^s - s\,\mathrm{ord}_A u_1.$$

But as $|\mathrm{ord}_A u_1| \leq 1$ and p does not divide s this implies $\mathrm{ord}_A u_1 = 0$. Since this holds for all such A we see that u_1 is associate to one of the list (2.8), which completes the first part of the proof.

If further $1-u_1$ lies in $\sqrt{G}$ then Lemma 10 shows that $1-u_1$ is associate to one of the list (2.8). Suppose now a in $\mathbb{F}_p^*$ is such that au_1 is in the list (2.8) then it is easily checked that $a=1$ and that $u_1, 1-u_1$ are in the sublist (2.9). □

3 Proofs of Theorem 1(G) and Theorem 1($\sqrt{G}$)

Lemma 15. *Let x, y in $\sqrt{G}$ satisfy $x + y = 1$ and assume that x and y are in S but not both in C. Then (x, y) is one of the six points Π in Theorem 1($\sqrt{G}$).*

Proof. First, we mention that neither x nor y are in C owing to $x + y = 1$. Now, the derivation with respect to t leads from $x + y = 1$ to the new equation

$$\left(\frac{\dot{x}}{x}\right) x + \left(\frac{\dot{y}}{y}\right) y \ = \ \dot{x} + \dot{y} \ = \ 0. \tag{3.1}$$

Hence we have a linear system

$$\begin{pmatrix} 1 & 1 \\ \frac{\dot{x}}{x} & \frac{\dot{y}}{y} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ = \ \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

with determinant

$$\Delta \ = \ \frac{\dot{y}}{y} - \frac{\dot{x}}{x}.$$

Suppose now $\Delta = 0$. Then, since $\dot{x} \neq 0$, we can divide the equation (3.1) by $\frac{\dot{x}}{x}$ getting $0 = x + y = 1$, a contradiction! Thus we conclude $\Delta \neq 0$ and we get in the usual way the identities

$$x \ = \ \frac{\frac{\dot{y}}{y}}{\frac{\dot{y}}{y} - \frac{\dot{x}}{x}}, \quad y \ = \ \frac{-\frac{\dot{x}}{x}}{\frac{\dot{y}}{y} - \frac{\dot{x}}{x}}. \tag{3.2}$$

Further, Lemma 12 implies that x and y are of the form

$$\frac{a_0 + a_1 t}{b_0 + b_1 t} \quad (a_0, a_1, b_0, b_1 \in \mathbb{F}_p). \tag{3.3}$$

Thus by Lemma 14 with $u = 1$ and $u_1 = x$ there is a in $\mathbb{F}_p^*$ such that ax belongs to the list (2.8). And then the fact that $1 - x = y$ lies in $\sqrt{G}$ but not in $\mathbb{F}_p \subset C$ shows that x and y are in the sublist (2.9). In the end we find that (x, y) is one of the six points in Theorem 1($\sqrt{G}$) as requested. □

We are now prepared to prove Theorem 1($\sqrt{G}$).

Proof of Theorem 1($\sqrt{G}$). We clearly have $L(\overline{\mathbb{F}_p}^*) \cup \bigcup_\Pi [[\psi_0]]_p \Pi \subset L(\sqrt{G})$.

Let now x, y be in $\sqrt{G}$ with $x + y = 1$. If x is not in $\overline{\mathbb{F}_p}$, then Lemma 6 provides e in $\mathbb{Z}$ such that $\widetilde{x} = x^{p^e}$ is in S but not in C. Further $\widetilde{y} = y^{p^e} = 1 - x^{p^e}$ is in S and Lemma 15 shows that $(\widetilde{x}, \widetilde{y})$ is one of the six points in Theorem 1($\sqrt{G}$), which settles the first part of the proof.

Otherwise $x \neq 1$ is in $\overline{\mathbb{F}_p}^* \subset \sqrt{G}$. Then, of course, $y = 1 - x$ is in $\overline{\mathbb{F}_p}^*$ as well and therefore $(x, y) = (a, 1 - a)$ with $a \neq 1$ in $\overline{\mathbb{F}_p}^*$; and this completes the proof. □

It is comparatively easy to deduce Theorem 1(G) on G in k from Theorem 1($\sqrt{G}$). To illustrate this we prove the following result on the radical $\sqrt[S]{G}$ of G in S, which will be applied in section 4. Compare also Lemma 15.

Lemma 16. *Suppose Π_0 is in $L(\sqrt[S]{G})$. Then either Π_0 is in $L(\overline{\mathbb{F}_p}^*)$ or it has the form Π^q for one of the six points Π in Theorem 1($\sqrt{G}$) with $q = 1, p, p^2, \ldots$.*

Proof. By Theorem $1(\sqrt{G})$ it suffices to check that if x is in the list (2.9) and x^q is in $\sqrt[S]{G}$ for $q = p^e$ ($e \in \mathbb{Z}$) then $e \geq 0$. But certainly $x^{p^{-1}}$ is not even in S because then x would be in $S^p \cap k = k^p$ by Lemma 13, an absurdity. And now x^{p^e} cannot be in S for any $e \leq -1$, else $(x^{p^e})^{p^{-1-e}} = x^{p^{-1}}$ would also be in S. This completes the proof □

4 The equation $x + y - z = 1$ over G

Now we want to investigate x, y and z in G with $x + y - z = 1$.
We have to exploit the symmetry, which becomes clearer by writing formally

$$x \;=\; \frac{X}{W}, \quad y \;=\; \frac{Y}{W}, \quad z \;=\; \frac{Z}{W} \tag{4.1}$$

Then the equation (1.8) becomes

$$X + Y \;=\; Z + W \tag{4.2}$$

and we note that this equation is invariant under the action of the dihedral group D_4 with eight elements acting on the square with vertices X, Z, Y, W in an anti-clockwise direction. This group therefore acts on the solutions of (4.2) and this means that there is a D_4-action on $P(G)$.

Let now X, Y, Z, W in k satisfy (4.2). We then define d as

$$d \;=\; d(X, Y, Z, W) \;=\; \dim_C CX + CY + CZ + CW, \tag{4.3}$$

which is of course stable under D_4 in (4.2); and indeed it is easily checked that this is the dimension $d(x, y, z)$ of $Cx + Cy + Cz$. Actually, if we further assume that not all of x, y, z are in C, then $d = 2$ or 3.

In the following sections we first focus on the case $d = 3$ and then treat the case $d = 2$.

4.1 The case $d = 3$

Let $\mathcal{H}$ be the set of polynomials

$$t^r(1-t)^s \quad (r \geq 0, s \geq 0, r + s \leq 3) \tag{4.4}$$

in $\mathbb{F}_p[t]$. For A in $\mathbb{F}_p[t]$ let $r(A)$ be the number of (X, Y) in $\mathcal{H}^2$ with $A = X + Y$. The following is the basic reason for our uniformity in p.

Lemma 17. *Suppose $p \geq 5$. Then $r(A) = 0, 1, 2$ apart from $r(A) = 4$ for the following*

$$\begin{aligned}
A \;&=\; 1 - t + t^2 \;=\; t^2 + (1-t) \;=\; (1-t)^2 + t, \\
A \;&=\; t(1 - t + t^2) \;=\; t^3 + t(1-t) \;=\; t(1-t)^2 + t^2, \\
A \;&=\; (1-t)(1 - t + t^2) \;=\; t^2(1-t) + (1-t)^2 \;=\; (1-t)^3 + t(1-t).
\end{aligned}$$

Proof. The analogous assertion for the corresponding set $\widetilde{\mathcal{H}}$ defined by (4.4) in $\mathbb{Z}[t]$ is readily checked by machine. This means that an equation $\widetilde{A} = \widetilde{X} + \widetilde{Y} = \widetilde{Z} + \widetilde{W}$ with $\widetilde{X}, \widetilde{Y}, \widetilde{Z}, \widetilde{W}$ in $\widetilde{\mathcal{H}}$ implies $\widetilde{Z} = \widetilde{X}$ or $\widetilde{Z} = \widetilde{Y}$ except as indicated when $\widetilde{A}$ is the canonical pullback of one of the three A shown above.

But now suppose $A = X + Y = Z + W$ in with X, Y, Z, W in $\mathcal{H}$. Each term $t^r(1-t)^s$ has a canonical pullback $t^r(1-t)^s$ to $\widetilde{\mathcal{H}}$ with coefficients of absolute values at most 3. Then the polynomial $P = \widetilde{X} + \widetilde{Y} - \widetilde{Z} - \widetilde{W}$ lies in $p\mathbb{Z}[t]$ and its coefficients have absolute values at most 12. So if $p \geq 13$ this forces $P = 0$. Now the conclusion for $\widetilde{\mathcal{H}}$ immediately implies the conclusion for $\mathcal{H}$.

One can cover $p = 11$ by noting that the only element of $\widetilde{\mathcal{H}}$ with a coefficient of absolute value 3 is $(1-t)^3$. So if P has a coefficient of absolute value bigger than 10 then at least three of $\widetilde{X}, \widetilde{Y}, \widetilde{Z}, \widetilde{W}$ must be $(1-t)^3$; and this forces $r(A) \leq 2$.

The cases $p = 5, 7$ can be checked by hand. □

Proposition 1. *Suppose* $p \geq 5$. *Then the set* $P^*(G)$ *of solutions of the equation* $x + y - z = 1$ *with* $d = 3$ *is* $D_4(\Pi)$ *with*

$$\Pi \;=\; \left(t, \frac{1-t}{t}, \frac{(1-t)^2}{t}\right).$$

Proof. We write down $x + y - z = 1$ and its derivative $\frac{\dot{x}}{x}x + \frac{\dot{y}}{y}y - \frac{\dot{z}}{z}z = 0$ as well as the second derivative $\frac{\ddot{x}}{x}x + \frac{\ddot{y}}{y}y - \frac{\ddot{z}}{z}z = 0$. There is an associated determinant

$$\Delta \;=\; \begin{vmatrix} 1 & 1 & -1 \\ \frac{\dot{x}}{x} & \frac{\dot{y}}{y} & -\frac{\dot{z}}{z} \\ \frac{\ddot{x}}{x} & \frac{\ddot{y}}{y} & -\frac{\ddot{z}}{z} \end{vmatrix},$$

and by multiplying by $-xyz$ we get the Wronskian of x, y, z. Since these latter are linearly independent over our field C of differential constants, Lemma 9 provides that $\Delta \neq 0$. It follows that

$$x \;=\; \frac{\Delta_x}{\Delta}, \quad y \;=\; \frac{\Delta_y}{\Delta}, \quad z \;=\; \frac{\Delta_z}{\Delta} \tag{4.5}$$

for

$$\Delta_x \;=\; \begin{vmatrix} 1 & 1 & -1 \\ 0 & \frac{\dot{y}}{y} & -\frac{\dot{z}}{z} \\ 0 & \frac{\ddot{y}}{y} & -\frac{\ddot{z}}{z} \end{vmatrix}, \quad \Delta_y \;=\; \begin{vmatrix} 1 & 1 & -1 \\ \frac{\dot{x}}{x} & 0 & -\frac{\dot{z}}{z} \\ \frac{\ddot{x}}{x} & 0 & -\frac{\ddot{z}}{z} \end{vmatrix}, \quad \Delta_z \;=\; \begin{vmatrix} 1 & 1 & 1 \\ \frac{\dot{x}}{x} & \frac{\dot{y}}{y} & 0 \\ \frac{\ddot{x}}{x} & \frac{\ddot{y}}{y} & 0 \end{vmatrix}.$$

Then Lemma 12 implies that each of $\Delta, \Delta_x, \Delta_y, \Delta_z$ has the form

$$\frac{a_0 + a_1 t + a_2 t^2 + a_3 t^3}{t^3(1-t)^3}$$

for a_0, a_1, a_2, a_3 in $\mathbb{F}_p$. Therefore each of x, y, z is a rational function of t of degree at most 3.

In (3.3) with a rational function of degree at most 1 it was easy to see when it lies in G. To deal with higher degree we note that $t^r(1-t)^s$ has degree $\max\{|r|, |s|, |r+s|\}$. This leads to 37 possibilities for (r, s) in $\mathbb{Z}^2$. So all we have to do is check the $37^3 = 50653$ possibilities for (x, y, z) in $x + y - z = 1$ (not forgetting $d = 3$).

To reduce this work we use (4.1), now with X, Y, Z, W in $\mathbb{F}_p[t]$ having no common factor. Each can be chosen to lie in the set $\mathcal{H}$ defined by (4.4). Now there are only 10 possibilities for (r, s), so $10^4 = 10000 < 50653$ in all. However Lemma 17 implies $Z = X$ or $Z = Y$ or $A = X + Y$ is one of the list of three. But $Z = X$ means $z = x$ contradicting $d = 3$, and similarly $Z \neq Y$. Thus X, Y, Z, W are as in the list. This actually reduces to a single projective (X, Y, Z, W) under the action of D_4, which can be taken as $(t^2, 1-t, (1-t)^2, t)$. So dividing by $W = t$ we get our $(x, y, z) = \Pi$; and for this the case $d = 3$ is quickly checked. □

4.2 The case $d = 2$

Let N be the set of solutions (X, Y, Z, W) of (4.2) in G^4 with $d \neq 1$ and

$$\{X, Y\} \neq \{Z, W\}. \tag{4.6}$$

We mention that N is stable under the D_4-action from there.

Next, we define an equivalence relation on k^* by two elements having their quotient in C. We then state the following simple lemma.

Lemma 18. *Suppose $p \geq 3$. Then every D_4-orbit in N contains a point where the equivalence classes in $\{X, Y, Z, W\}$ are described by one of*

(1) $\{X, Y\}, \{Z\}, \{W\}$,

(2) $\{Y, W\}, \{X\}, \{Z\}$.

(3) $\{X\}, \{Y\}, \{Z\}, \{W\}$,

Proof. Take any (X, Y, Z, W) in N, and h be the number of classes in $\{X, Y, Z, W\}$. Then $h \neq 1$ due to the condition that $d \neq 1$ in (4.6).

If $h = 4$ then we are in case (3) at once.

If $h = 3$ then there must be two singletons and one pair. Under D_4 we can assume that the pair is either $\{X, Y\}$ (opposite points of the square) or $\{Y, W\}$ (adjacent points), leading to cases (1) and (2).

It remains only to exclude $h = 2$. This could arise from one singleton and one triplet; but then the equation (4.2) would destroy the singleton. Or we could have two pairs. Under D_4 these could be taken as either $\{X, Y\}, \{Z, W\}$ (opposite points equivalent) or $\{X, Z\}, \{Y, W\}$ (adjacent points). The first means $X = \alpha Y, Z = \beta W$ for α, β in C, but then $(1 + \alpha)Y = (1 + \beta)W$ forcing $\alpha = \frac{X}{Y} = -1$ and $\beta = \frac{Z}{W} = -1$ which however are not in G as $p \geq 3$. The second means similarly $X = \alpha Z, Y = \beta W$ but then $(1 - \alpha)Z + (1 - \beta)W = 0$ forcing $\alpha = \beta = 1$ and $X = Z, Y = W$ contrary to the second condition in (4.6). This completes the proof. □

For the following proposition we need a small modification of our notation. Our coset T_x is the set of $(1, y, y)$ in k^3; we define T_x^* as the subset with y not in C. Similarly for T_y^*. Further we define

$$[\psi]_p^* = \bigcup_{e=1}^{\infty} \psi^{-1} \varphi^e \psi$$

as in (1.11) for $h = 1$ but omitting $e = 0$.

Proposition 2. *Suppose $p \geq 3$. Then the set $P^{**}(G)$ of solutions of the equation $x + y - z = 1$ with $d = 2$ is*

$$T_x^*(G) \cup T_y^*(G) \cup \bigcup_{\Pi} D_4([\psi_\Pi]_p^* \Pi)$$

with the following five points and automorphisms

$$\begin{aligned}
\Pi &= \left(1, \frac{1-t}{t}, \frac{1-t}{t}\right), & \psi_\Pi(x,y,z) &= \left(tx, ty, \frac{t}{1-t}z\right),\\
\Pi &= \left(1, \frac{1}{t}, \frac{1}{t}\right), & \psi_\Pi(x,y,z) &= \left(\frac{1-t}{t}x, y, (1-t)z\right),\\
\Pi &= \left(\frac{t^2}{(1-t)^2}, \frac{1}{1-t}, \frac{t}{(1-t)^2}\right), & \psi_\Pi(x,y,z) &= \left(\frac{1-t}{t}x, y, (1-t)z\right),\\
\Pi &= \left(1, \frac{1}{1-t}, \frac{1}{1-t}\right), & \psi_\Pi(x,y,z) &= \left(\frac{t}{1-t}x, y, tz\right),\\
\Pi &= \left(\frac{(1-t)^2}{t^2}, \frac{1}{t}, \frac{1-t}{t^2}\right), & \psi_\Pi(x,y,z) &= \left(\frac{t}{1-t}x, y, tz\right).
\end{aligned}$$

Proof. Let (x,y,z) be in $P^{**}(G)$, and use (4.1) with X,Y,Z,W also in G. Then $\{X,Y\} = \{Z,W\}$ would mean we are not just in $T_x(G) \cup T_y(G)$ but even in $T_x^*(G) \cup T_y^*(G)$ because $d \neq 1$. Thus we can assume all of (4.6).

So after adjusting by D_4 we can assume by Lemma 18 that we are in one of the cases (1),(2),(3). We distribute these over the next three subsections.

4.2.1 The case (1) of Lemma 18

In case (1) we have $x = \alpha y$ for some α in C. It follows that

$$(1+\alpha)y - z \;=\; 1. \tag{4.7}$$

Further α is in G so $\alpha \neq -1$. Since $1+\alpha$ is a differential constant we can easily differentiate, and since $\frac{z}{y} = \frac{Z}{Y}$ is not in C the arguments in section 3 yield

$$(1+\alpha)y \;=\; \frac{\frac{\dot z}{z}}{\frac{\dot z}{z} - \frac{\dot y}{y}}, \qquad -z \;=\; \frac{-\frac{\dot y}{y}}{\frac{\dot z}{z} - \frac{\dot y}{y}}$$

as in (3.2). In particular Lemma 12 shows that $u_1 = (1+\alpha)y$ has degree at most 1. This gives only finitely many possibilities for $z = u_1 - 1$, thus reducing to finitely many lines M on the plane P. In the context of a general variety V, these are the W mentioned at the end of section 1 [Adjust!]. However their number may depend on the characteristic p.

To cut down this dependence we note that $\frac{1+\alpha}{u_1} = \frac{1}{y}$ lies in G. Further $1 - u_1 = -z$ lies in $\sqrt{G}$ but not in $\mathbb{F}_p$ because $z = \frac{Z}{W}$ is not in C. So by Lemma 14 we conclude that u_1 lies in (2.9). But actually $u_1 - 1 = z$ lies in G, which reduces the choice to

$$u_1 \;=\; \frac{1}{t} \qquad \text{or} \qquad u_1 \;=\; \frac{1}{1-t}. \tag{4.8}$$

Take first $u_1 = \frac{1}{t}$. Now temporarily with general coordinates x,y,z the line M is defined by the equations $x + y - z = 1$ and $z = \frac{1-t}{t}$, or equivalently

$$x + y \;=\; \frac{1}{t}, \quad z \;=\; \frac{1-t}{t}.$$

So $M' = \psi(M)$ is defined over $\mathbb{F}_p$, where

$$\psi(x,y,z) \;=\; \left(tx, ty, \frac{t}{1-t}z\right)$$

is as in the first in the list of Proposition 2; in fact if we call this (x',y',z') then the equations become

$$x'+y' \;=\; 1, \quad z' \;=\; 1. \tag{4.9}$$

Here we see a copy of the line L, and so M' has the points $(x',y',z') = (t, 1-t, 1)$, $(1-t,t,1)$. These give rise via ψ^{-1} to points

$$\Pi \;=\; \left(1, \frac{1-t}{t}, \frac{1-t}{t}\right), \;\; \left(\frac{1-t}{t}, 1, \frac{1-t}{t}\right)$$

on $\psi^{-1}(M') = M$ so on P; note that the first Π here is also as in the first in the list of Proposition 2.

Now return to our point (x,y,z) of $P^{**}(G)$, here in $M(G)$. Then $\psi(x,y,z)$ is in $M'(G)$ and from the equations (4.9) and Theorem 1(G) we see that this is one of

$$(t^q, (1-t)^q, 1), \quad ((1-t)^q, t^q, 1) \qquad (q = p^e, \; e = 0,1,2,\ldots). \tag{4.10}$$

The first of these is, in the notation of (1.11), just $\varphi^e\psi(\Pi)$ with the first ψ above. So we get the family

$$(x,y,z) \;=\; \psi^{-1}\varphi^e\psi(\Pi) \;=\; \left(t^{q-1}, \frac{(1-t)^q}{t}, \frac{1-t}{t}\right). \tag{F1}$$

Taking the union over all e gives precisely $[\psi]_p(\Pi)$. But in fact $\frac{x}{y} = \alpha$ lies in C, so $q=1$ is excluded and we end up in $[\psi]_p^*(\Pi)$ as in Proposition 2. The D_4-action (which may however take us out of case (1) of Lemma 18) then provides us with the whole $D_4([\psi]_p^*(\Pi))$.

But what if $\psi(x,y,z)$ is the second of (4.10)? Then it is easily seen, in fact through the interchange of x and y, that we get something in the same D_4-orbit.

We can deal with $u_1 = \frac{1}{1-t}$ in (4.8) by noting that k has an automorphism ω taking t to $1-t$ which preserves P and G and therefore acts on $P(G)$. It also preserves $C \cap k = k^p$ and so acts on $P^{**}(G)$. Now if $u_1 = z+1 = \frac{1}{1-t}$ then $\omega(z)+1 = \frac{1}{t}$ and so for $\omega(x,y,z)$ we are in the case just considered. Therefore $\omega(x,y,z)$ lies in $\mathcal{D} = D_4([\psi]_p^*(\Pi))$; and by applying $\omega^{-1} = \omega$ we see that (x,y,z) lies in $\omega(\mathcal{D})$. However $\omega(\mathcal{D}) = \mathcal{D}$; for example we get from (F1) the point

$$\left((1-t)^{q-1}, \frac{t^q}{1-t}, \frac{t}{1-t}\right).$$

But in terms of (4.2) already (F1) says

$$t^q + (1-t)^q \;=\; (1-t)+t$$

and so dividing this by $1-t$ gives again the same orbit.

Thus case (1) of Lemma 18 therefore leads to only the first in the list of Proposition 2.

4.2.2 The case (3) of Lemma 18

We next treat the third case from Lemma 18 temporarily taking in the second case as well. Now x, y are linearly independent over C and because $d = 2$ there are α, β in C with

$$z \;=\; \alpha x + \beta y. \tag{4.11}$$

We note that $\alpha \neq 0$ because y, z are linearly independent over C; similarly we see that $\beta \neq 0$. Then for $x_z = \frac{x}{z},\ y_z = \frac{y}{z}$ we get

$$\alpha x_z + \beta y_z \;=\; 1. \tag{4.12}$$

Here $\frac{y_z}{x_z} = \frac{y}{x}$ is not in C and so with the same arguments as in section 3 we get

$$\alpha x_z \;=\; \frac{\frac{\dot{y}_z}{y_z}}{\frac{\dot{y}_z}{y_z} - \frac{\dot{x}_z}{x_z}}, \quad \beta y_z \;=\; \frac{-\frac{\dot{x}_z}{x_z}}{\frac{\dot{y}_z}{y_z} - \frac{\dot{x}_z}{x_z}} \tag{4.13}$$

as in (3.2). Further $x_1 = \alpha x_z \neq 0$, $y_1 = \beta y_z \neq 0$ and in particular Lemma 12 guarantees that they are in k with degree at most 1. Note however that $\alpha = 1$ or $\beta = 1$ are not yet excluded (see below).

Substituting (4.11) into $x + y - z = 1$ gives

$$(1-\alpha)x + (1-\beta)y \;=\; 1, \tag{4.14}$$

and the same arguments give

$$(1-\alpha)x \;=\; \frac{\frac{\dot{y}}{y}}{\frac{\dot{y}}{y} - \frac{\dot{x}}{x}}, \quad (1-\beta)y \;=\; \frac{-\frac{\dot{x}}{x}}{\frac{\dot{y}}{y} - \frac{\dot{x}}{x}} \tag{4.15}$$

with $u_1 = (1-\alpha)x,\ v_1 = (1-\beta)y$ of degree at most 1.

Now we have

$$u_1 \;=\; x - x_1 z, \quad v_1 \;=\; y - y_1 z \tag{4.16}$$

(adding up to our original $1 = x + y - z$) which again reduces to finitely many lines in P. Again we must cut down the dependence on p.

Using Lemma 14 on $\frac{\beta}{y_1}$ provides a in $\mathbb{F}_p^*$ such that ay_1 is in the list (2.8). Further $\frac{\alpha}{x_1} = \frac{z}{x}$ is in $G \subset \sqrt{G}$ and by Lemma 10 $1 - x_1 = a^{-1}(ay_1)$ is in $\sqrt{G}$ but not in $\mathbb{F}_p$ because $y_1 = \beta\frac{Y}{Z}$ is not in C. Thus Lemma 14 implies that x_1, y_1 lie in the sublist (2.9).

So far we could do the cases (2) and (3) from Lemma 18 at once. But now we restrict to the case (3).

Then (4.14) yields $\alpha \neq 1$, $\beta \neq 1$ because $y = \frac{Y}{W}$ and $x = \frac{X}{W}$ are not in C. So Lemma 14 on $\frac{1-\beta}{v_1}$ provides b in $\mathbb{F}_p^*$ such that bv_1 is in the list (2.8). Further $\frac{1+\alpha}{u_1} = \frac{1}{x}$ is in $G \subset \sqrt{G}$ and Lemma 10 shows that $1 - u_1 = b^{-1}(bv_1)$ is in $\sqrt{G}$ but not in $\mathbb{F}_p$ because $v_1 = (1-\beta)\frac{Y}{W}$ is not in C. So Lemma 14 implies that u_1, v_1 belong to the sublist (2.9).

In particular x_1, y_1, as well as u_1, v_1, lie in the sublist (2.9). This eliminates completely the dependence in the equations (4.16) on p. Still, the lines don't look like L.

But when we write these equations as

$$\frac{x}{u_1} + \left(-\frac{x_1 z}{u_1}\right) \;=\; 1, \quad \frac{y}{v_1} + \left(-\frac{y_1 z}{v_1}\right) \;=\; 1, \tag{4.17}$$

then we do after all observe two points on $L(\sqrt[k]{G})$. But by Lemma 16 this means that there are integral powers q_x, q_y of p and points $\Pi_x = (\xi, \zeta_x)$, $\Pi_y = (\eta, \zeta_y)$ in either $L(\overline{\mathbb{F}_p}^*)$ or among the six points in Theorem $1(\sqrt{G})$ such that

$$x \;=\; u_1\xi^{q_x}, \;\; z \;=\; -\frac{u_1}{x_1}\zeta_x^{q_x}, \qquad y \;=\; v_1\eta^{q_y}, \;\; z \;=\; -\frac{v_1}{y_1}\zeta_y^{q_y}. \tag{4.18}$$

In particular comparing the z-values gives

$$\frac{\zeta_x^{q_x}}{\zeta_y^{q_y}} \;=\; \frac{x_1v_1}{u_1y_1}. \tag{4.19}$$

The right-hand side w here certainly has degree at most 4; but in fact (4.13) and (4.15) show that

$$w \;=\; \frac{\frac{\dot{x}}{x}\left(\frac{\dot{y}}{y}-\frac{\dot{z}}{z}\right)}{\frac{\dot{y}}{y}\left(\frac{\dot{x}}{x}-\frac{\dot{z}}{z}\right)}. \tag{4.20}$$

So w has degree at most 2 due to Lemma 12. Furthermore it cannot be in $\overline{\mathbb{F}_p}$, because then $w = 1$ (see the last table in Appendix A), and this would lead at once to

$$\frac{\dot{z}}{z}\left(\frac{\dot{x}}{x}-\frac{\dot{y}}{y}\right) \;=\; 0$$

which is ruled out in our current case (3). In particular, it follows that Π_x, Π_y cannot both lie in $L(\overline{\mathbb{F}_p}^*)$.

Next, we derive from (4.18) that

$$\alpha \;=\; x_1\frac{z}{x} \;=\; \left(\frac{\zeta_x}{\xi}\right)^{q_x}, \qquad \beta \;=\; y_1\frac{z}{y} \;=\; \left(\frac{\zeta_y}{\eta}\right)^{q_y}. \tag{4.21}$$

Suppose now that $\Pi_x = (\xi, \zeta_x)$ is one of the six points in Theorem $1(\sqrt{G})$. Then one easily sees that (4.21) forces $q_x > 1$ because α is in C. If now $\Pi_y = (\eta, \zeta_y)$ were in $L(\overline{\mathbb{F}_p}^*)$ then the degree of w would be at least $p \geq 3$, a contradiction. And the same argument shows that there are no solutions in the case with Π_x in $L(\overline{\mathbb{F}_p}^*)$ and Π_y one of the six points in Theorem $1(\sqrt{G})$.

Finally, we have the situation with Π_x, Π_y both among the six points in Theorem $1(\sqrt{G})$. As above it follows that $q_x > 1$ and (by the same argument) $q_y > 1$. Since $p \geq 3$ we then have on one hand $q_x = q_y$, which implies that either $w = \frac{\zeta_x^{q_x}}{\zeta_y^{q_y}}$ has degree at least 3 (see the first two tables in Appendix A) or $w = 1$; both are impossible. And if on the other hand $q_x \neq q_y$, then w has degree at least 6, which is ruled out again.

This means that we find no points of $P^{**}(G)$ in this case (3).

4.2.3 The case (2) of Lemma 18

We finally turn to case (2), which we left halfway through the discussion above and which implies that $y = \frac{Y}{W}$ is in C. So by (4.15) we have $\alpha = 1$ and hence $u_1 = 0$, $v_1 = 1$. Strangely enough it is this somewhat degenerate-looking case which provides most of the points of $P^{**}(G)$.

From (4.16) we see now that $x_1 = \frac{x}{z}$ lies in G. Inspection of (2.9) shows that x_1 must be in the sublist

$$t, \; 1-t, \; \frac{1}{t}, \; \frac{1}{1-t} \tag{4.22}$$

of (2.9). We look at each of these in turn.

Suppose first that $x_1 = t$, so that $y_1 = 1-t$. Thus from (4.16) we are now on the line M defined by the equations

$$x \;=\; tz, \quad y-(1-t)z \;=\; 1. \tag{4.23}$$

So $M' = \psi(M)$ is defined over $\mathbb{F}_p$, where

$$\psi(x,y,z) \;=\; \left(\frac{1-t}{t}x, y, (1-t)z\right) \tag{4.24}$$

is as in the second and third in the list of Proposition 2; in fact also with (x',y',z') then the equations become

$$x' \;=\; z', \quad y'-z' \;=\; 1. \tag{4.25}$$

Here we don't see exactly the line L. However,

$$\left(\frac{1}{t}, -\frac{1-t}{t}\right) \qquad \text{and} \qquad \left(\frac{1}{1-t}, -\frac{t}{1-t}\right)$$

from Theorem $1(\sqrt{G})$ lead to the following solutions over G

$$(x',y',z') \;=\; \left(\frac{1-t}{t}, \frac{1}{t}, \frac{1-t}{t}\right), \; \left(\frac{t}{1-t}, \frac{1}{1-t}, \frac{t}{1-t}\right).$$

These give rise via ψ^{-1} to points

$$\Pi \;=\; \left(1, \frac{1}{t}, \frac{1}{t}\right), \; \left(\frac{t^2}{(1-t)^2}, \frac{1}{1-t}, \frac{t}{(1-t)^2}\right)$$

on $\psi^{-1}(M') = M$ so on P; note that these are also as in the second and third in the list of Proposition 2.

Now return to our point (x,y,z) of $P^{**}(G)$. Then $\psi(x,y,z)$ is on $M'(G)$ and from the equations (4.25) and Theorem $1(\sqrt{G})$ we see that this is one of

$$\left(\frac{(1-t)^q}{t^q}, \frac{1}{t^q}, \frac{(1-t)^q}{t^q}\right), \; \left(\frac{t^q}{(1-t)^q}, \frac{1}{(1-t)^q}, \frac{t^q}{(1-t)^q}\right) \quad (q = p^e, \; e = 0,1,2,\ldots).$$

Again these are just $\varphi^e\psi(\Pi)$. The first gives

$$(x,y,z) \;=\; \psi^{-1}\varphi^e\psi(\Pi) \;=\; \left(\frac{(1-t)^{q-1}}{t^{q-1}}, \frac{1}{t^q}, \frac{(1-t)^{q-1}}{t^q}\right), \tag{F2}$$

and the second gives

$$(x,y,z) \;=\; \psi^{-1}\varphi^e\psi(\Pi) \;=\; \left(\frac{t^{q+1}}{(1-t)^{q+1}}, \frac{1}{(1-t)^q}, \frac{t^q}{(1-t)^{q+1}}\right). \tag{F3}$$

Taking the union over all e gives again the $[\psi]_p(\Pi)$. But this time y lies in C, so $q \neq 1$ and we end up with the $[\psi_\Pi]_p^*(\Pi)$ as in Proposition 2. The D_4-action (which as before may take us out of case (2) of Lemma 18) then provides us with the whole $D_4([\psi_\Pi]_p^*(\Pi))$.

Suppose next that $x_1 = \frac{1}{t}$ in (4.22), so that $y_1 = -\frac{1-t}{t}$. Thus from (4.16) we are now on the line M defined by the equations

$$x \ = \ \frac{1}{t}z, \quad y + \frac{1-t}{t}z \ = \ 1.$$

So $M' = \psi(M)$ is defined over $\mathbb{F}_p$, where

$$\psi(x,y,z) \ = \ \left((1-t)x, y, \frac{1-t}{t}z\right)$$

now is not in the list of Proposition 2; anyway with (x', y', z') then the equations become

$$x' \ = \ z', \quad y' + z' \ = \ 1.$$

Now return to our point (x, y, z) of $P^{**}(G)$. Then $\psi(x, y, z)$ is on $M'(G)$ and from the equations immediately above and Theorem $1(G)$ we see that this is one of

$$(x', y', z') = (t^q, (1-t)^q, t^q), \ ((1-t)^q, t^q, (1-t)^q) \quad (q = p^e, \ e = 0, 1, 2, \ldots).$$

And via ψ^{-1} they give

$$\left(\frac{t^q}{1-t}, (1-t)^q, \frac{t^{q+1}}{1-t}\right), \ \left((1-t)^{q-1}, t^q, t(1-t)^{q-1}\right),$$

again with $q = 1$ excluded because y is in C.

However these result in the same D_4-orbits as the second and third respectively above, which is easily seen considering (F2) and (F3) respectively in terms of (4.2), namely

$$\begin{aligned} t(1-t)^{q-1} + 1 \ &= \ (1-t)^{q-1} + t^q, \\ t^{q+1} + (1-t) \ &= \ t^q + (1-t)^{q+1}. \end{aligned}$$

Finally we deal with the remaining $x_1 = 1-t, \frac{1}{1-t}$ in (4.22) simply by applying our automorphism ω, which yields on (F2), (F3)

$$(x, y, z) \ = \ \left(\frac{t^{q-1}}{(1-t)^{q-1}}, \frac{1}{(1-t)^q}, \frac{t^{q-1}}{(1-t)^q}\right), \tag{F4}$$

$$(x, y, z) \ = \ \left(\frac{(1-t)^{q+1}}{t^{q+1}}, \frac{1}{t^q}, \frac{(1-t)^q}{t^{q+1}}\right), \tag{F5}$$

corresponding to the fourth and fifth in Proposition 2. This is thereby proved. □

5 Proof of Theorem 2(G)

We are now prepared to prove Theorem 2(G). However, we preferably give the proof for $p = 2$ in the later chapter 7 as it can be deduced from Theorem 2$(\sqrt{G})$ in a comparatively easy way.

We could also do this for $p \geq 3$ as we did for Theorem 1(G) in chapter 3, but we have preferred to arrange the exposition of this thesis so that the reader can first follow the situation for G, already complicated enough, without getting into the technicalities of $\sqrt{G}$ in K and the separable closure S of k. Furthermore it turns out that the deduction for $p \geq 3$ is less simple than the deduction for $p = 2$.

5.1 Proof of Theorem 2(G) for $p \geq 5$

We first prove Theorem 2(G) for $p \geq 5$. Take a point (x, y, z) in $P(G)$, with as above $d = d(x, y, z) = \dim_C(Cx+Cy+Cz)$. We already treated the cases $d = 3$ and $d = 2$. The case $d = 1$ is treated as in the proof of Theorem 1$(\sqrt{G})$. For then x, y, z lie in C. If they are all in $\mathbb{F}_p^*$, then also in $\mathbb{F}_p^* \cap G$, so $x = y = z = 1$ and we are certainly in $T_x(G) \cup T_y(G)$. Otherwise Lemma 6 provides e_x, e_y, e_z in $\mathbb{Z}$ such that $x^{p^{e_x}}$, $y^{p^{e_y}}$, $z^{p^{e_z}}$ lie in S but not in C. Therefore we conclude that with $e = \max\{e_x, e_y, e_z\}$ the triple

$$(\widetilde{x}, \widetilde{y}, \widetilde{z}) \ = \ (x^{p^e}, y^{p^e}, z^{p^e})$$

is in S^3 but not in C^3. In our current situation however, this means that $\widetilde{x}$, $\widetilde{y}$, $\widetilde{z}$ are all in k with $\widetilde{x} + \widetilde{y} - \widetilde{z} = 1$ and $d(\widetilde{x}, \widetilde{y}, \widetilde{z}) \geq 2$. Due to Lemma 11 $\widetilde{x}, \widetilde{y}, \widetilde{z}$ are still in G and it follows from the above discussion that $(\widetilde{x}, \widetilde{y}, \widetilde{z})$ is as in Proposition 1 or Proposition 2.

Now in Proposition 2 we see T_x^*, T_y^*, which on raising to power q' ($q' = 1, p, p^2, \ldots$) end up in T_x, T_y as in Theorem 2(G).

We also see various $\delta([\psi_\Pi]_p^*\Pi)$ for δ in D_4. But by going back to projective X, Y, Z, W it is not difficult to see that this is $[\psi_{\Pi,\delta}]_p^*\Pi_\delta$ for some $\psi_{\Pi,\delta}$ and $\Pi_\delta = \delta(\Pi)$. This is $[\psi_{\Pi,\delta}]_p\Pi_\delta$ with just Π_δ removed. And the set of q'th powers of elements of $[\psi_{\Pi,\delta}]_p\Pi_\delta$ is nothing else than $[\psi_0, \psi_{\Pi,\delta}]_p\Pi_\delta$. So we get all the $[\psi_0, \psi_\Pi]_p\Pi$ in Theorem 2(G) except that it seems that the q'th powers of the Π_δ are missing. However these are supplied by Proposition 1, because the Π there has the same D_4-orbit as the third and fifth Π in Proposition 2.

What about the first, second and fourth Π in Proposition 2? These belong anyway in T_x, which we have already taken into account. This completes the proof.

5.2 Proof of Theorem 2(G) for $p = 3$

We can follow the arguments of the preceding section, noting that Proposition 2 has been proved for $p = 3$ as well. However, Proposition 1 fails because Lemma 17 fails. Hand computation yields exactly six further examples with $r(A) = 4$, which come from

$$\begin{aligned}
1+t(1-t) &= (1-t)^2+t^2,\\
t+t^2(1-t) &= t(1-t)^2+t^3,\\
(1-t)+t(1-t)^2 &= (1-t)^3+t^2(1-t),\\
1+t^2(1-t) &= (1-t)^3+t^2,\\
1+t(1-t)^2 &= (1-t)^2+t^3,\\
t+(1-t) &= (1-t)^3+t^3.
\end{aligned}$$

Here the second and third equations give rise to the same projective points as the first, so we may ignore them. Further the fourth, fifth and sixth equations do not have $d=3$. The first equation produces the point

$$\left(\frac{1}{t^2}, \frac{1-t}{t}, \frac{(1-t)^2}{t^2}\right),$$

and its D_4-orbit accounts for the extra set $\mathcal{T}_3'$ in Theorem 2(G).

6 The equation $x+y+z=-1$ over $\sqrt{G}$

Dealing with the equation

$$x+y+z \;=\; -1 \tag{6.1}$$

over $\sqrt{G}$ we follow almost the same line of argumentation as we did for the equation $x+y-z=1$ over G in section 4.

We start our investigations by considering the projective form of (6.1), which is

$$X+Y+Z+W \;=\; 0. \tag{6.2}$$

Here we immediately see an S_4-action. And with (4.1) it is clear that S_4 acts as well on solutions (x,y,z) of (6.1).

Let now X,Y,Z,W in K satisfy (6.2). We then consider the dimension d as in (4.3) which is of course stable under S_4 in (6.2). Again this is the dimension $d(x,y,z)$ of $Cx+Cy+Cz$ and $d=2$ or 3 as long as not all of x,y,z are in C.

Contrary to section 4 we first focus on the case $d=2$ and then treat the case $d=3$.

Furthermore, we mention that two quadruples over K satisfying (6.2) give rise to the same S_4-orbit, if one of them can be obtained from the other by multiplying some non-zero factor and ordering its elements by S_4. It is just this consideration which helps us to avoid counting the same S_4-orbit twice.

6.1 The case $d=2$

We start with the analogue of Lemma 18 while as there we define an equivalence relation on K^* by two elements having their quotient in C.

Lemma 19. *Let (X,Y,Z,W) in $\sqrt{G}^4$ be a solution of (6.2) with $d=2$. Then its S_4-orbit contains a point where the equivalence classes in $\{X,Y,Z,W\}$ are described by one of*

(1) $\{X,Z\},\{Y,W\}$,

(2) $\{Y,W\},\{X\},\{Z\}$,

(3) $\{X\},\{Y\},\{Z\},\{W\}$.

Proof. Of course, $d=2$ implies that there are at least two classes due to (6.2). If we have just two classes, this could not arise from one singleton and one triplet, because then (6.2) would destroy the singleton. Thus there must be two pairs and our S_4-action allows us to take $\{X,Z\},\{Y,W\}$. If there are three classes, then we have two singletons and one pair, which by S_4 can be chosen as $\{X\},\{Z\}$, $\{Y,W\}$. Finally, if the number of classes is four we see $\{X\},\{Z\}$, $\{Y\}$, $\{W\}$ and this completes the proof. □

For the following proposition we define in a similar manner as in (1.12) the cosets $\widetilde{T}_x,\widetilde{T}_y$ and $\widetilde{T}_z$ by

$$\widetilde{T}_x:\; x=-1,\; y+z=0, \qquad \widetilde{T}_y:\; y=-1,\; x+z=0, \qquad \widetilde{T}_z:\; z=-1,\; x+y=0.$$

Further, if Γ is a subgroup of $\sqrt{G}$ then $\widetilde{T}_x(\Gamma)$ denotes the set of all $(-1,y,-y)$ in Γ^3 and we define $\widetilde{T}_x^*(\Gamma)$ as the subset with y not in C. Similarly we define $\widetilde{T}_y^*(\Gamma)$ and $\widetilde{T}_z^*(\Gamma)$ respectively.

Proposition 3. *Let x, y, z in $\sqrt[S]{G}$ satisfy $x+y+z=-1$ and assume that $d=\dim_C Cx+Cy+Cz=2$. If $p\geq 3$ then (x,y,z) is in the set*

$$\widetilde{T}_x^*(\sqrt[S]{G}) \;\cup\; \widetilde{T}_y^*(\sqrt[S]{G}) \;\cup\; \widetilde{T}_z^*(\sqrt[S]{G}) \;\cup\; \bigcup_{\substack{a\in\overline{\mathbb{F}_p}^* \\ a\neq 1}} \bigcup_{i=1}^{3} S_4(\Pi_i(a)) \;\cup\; \bigcup_{j=1}^{9} S_4([\psi_j]_p^*\Pi_j)$$

with

$$\begin{aligned} \Pi_1(a) &= (-t,(a-1)(1-t),-a(1-t))\,, \\ \Pi_2(a) &= (-(1-t),(a-1)t,-at)\,, \\ \Pi_3(a) &= (-a(1-t),a-1,-at)\,, \end{aligned}$$

and the following points and $\sqrt{G}$-automorphisms

$$\begin{aligned}
\Pi_1 &= (t,-t,-1)\,, & \psi_1(x,y,z) &= \left(\frac{1-t}{t}x,-y,-(1-t)z\right), \\
\Pi_2 &= \left(\frac{(1-t)^2}{t},-t,-\frac{1-t}{t}\right), & \psi_2(x,y,z) &= \left(\frac{t}{1-t}x,-y,-tz\right), \\
\Pi_3 &= \left(-(1-t)^2,-t,-t(1-t)\right), & \psi_3(x,y,z) &= \left(-\frac{1}{1-t}x,-y,-\frac{1}{t}z\right), \\
\Pi_4 &= (1-t,-(1-t),-1)\,, & \psi_4(x,y,z) &= \left(\frac{t}{1-t}x,-y,-tz\right), \\
\Pi_5 &= \left(-\frac{1-t}{t},\frac{1-t}{t},-1\right), & \psi_5(x,y,z) &= \left(-\frac{1}{1-t}x,-y,-\frac{1}{t}z\right), \\
\Pi_6 &= \left(\frac{t^2}{1-t},-(1-t),-\frac{t}{1-t}\right), & \psi_6(x,y,z) &= \left(\frac{1-t}{t}x,-y,-(1-t)z\right) \\
\Pi_7 &= \left(-\frac{1}{t(1-t)},\frac{1-t}{t},\frac{1}{1-t}\right), & \psi_7(x,y,z) &= \left(-(1-t)x,-y,\frac{1-t}{t}z\right), \\
\Pi_8 &= \left(\frac{t^2}{1-t},-\frac{1}{1-t},t\right), & \psi_8(x,y,z) &= \left(-\frac{1}{t}x,-y,-\frac{1}{1-t}z\right), \\
\Pi_9 &= \left(-\frac{1}{t(1-t)},\frac{t}{1-t},\frac{1}{t}\right), & \psi_9(x,y,z) &= \left(-tx,-y,\frac{t}{1-t}z\right).
\end{aligned}$$

And if $p=2$ then (x,y,z) is in the set

$$\widetilde{T}_x^*(\sqrt[S]{G}) \cup \widetilde{T}_y^*(\sqrt[S]{G}) \cup \widetilde{T}_z^*(\sqrt[S]{G}) \cup \bigcup_{\substack{a\in\overline{\mathbb{F}_p}^* \\ a\neq 1}} \bigcup_{i=1}^{3} S_4(\Pi_i(a)) \cup S_4(\Pi^*) \cup \bigcup_{j=1}^{9} S_4([\psi_j]_p^*\Pi_j)$$

for the additional point

$$\Pi^* \;=\; \left(t(1-t),(1-t)^3,t^3\right).$$

Proof. First, we mention that not all of x, y, z lie in C because otherwise $d=1$. Now, taking the projective form we may assume that X, Y, Z, W are in $\sqrt[S]{G}$ satisfying (6.2) and (4.1). Next, after adjusting by S_4, we can assume that we are in one of the three cases of Lemma 19 above.

In the first case we have $Z=\alpha X$ and $W=\beta Y$ with α,β in C. Thus

$$0 \;=\; X+Y+Z+W \;=\; (1+\alpha)X+(1+\beta)Y$$

and because $\frac{X}{Y}$ is not in C we conclude $\alpha = \beta = -1$. Therefore (4.1) gives rise to the set $\widetilde{T}_y^*(\sqrt[S]{G})$ and S_4 provides the additional sets $\widetilde{T}_x^*(\sqrt[S]{G})$ and $\widetilde{T}_z^*(\sqrt[S]{G})$ respectively.

The second and third case are treated in the following two subsections.

6.1.1 The case (3) of Lemma 19

Turning to the third case from Lemma 19 we temporarily take in the second case as well. Here x, y are linearly independent over C and since $d = 2$ we see (4.11) with α, β in C leading again to (4.13) with $x_1 = \alpha x_z \neq 0$ and $y_1 = \beta y_z \neq 0$ in k of degree at most 1.

Substituting (4.11) into $x + y + z = -1$ we now get the slightly different

$$(1+\alpha)x + (1+\beta)y \;=\; -1 \tag{6.3}$$

leading to

$$(1+\alpha)x \;=\; \frac{-\frac{\dot y}{y}}{\frac{\dot y}{y} - \frac{\dot x}{x}}, \qquad (1+\beta)y \;=\; \frac{\frac{\dot x}{x}}{\frac{\dot y}{y} - \frac{\dot x}{x}} \tag{6.4}$$

with $u_1 = (1+\alpha)x$, $v_1 = (1+\beta)y$ in k of degree at most 1 again.

Similar to (4.16) above we then have

$$u_1 \;=\; x + x_1 z, \qquad v_1 \;=\; y + y_1 z. \tag{6.5}$$

We now restrict to the case (3). Again we can cut down the dependence of (6.5) on p by deducing from Lemma 14 that x_1, y_1 and $-u_1, -v_1$ belong to the sublist (2.9).

Similar to (4.17) we write these equations as

$$\frac{x}{u_1} + \frac{x_1 z}{u_1} \;=\; 1, \qquad \frac{y}{v_1} + \frac{y_1 z}{v_1} \;=\; 1.$$

Then Lemma 16 provides integral powers q_x, q_y of p and points $\Pi_x = (\xi, \zeta_x)$, $\Pi_y = (\eta, \zeta_y)$ in either $L(\overline{\mathbb{F}_p}^*)$ or among the six points in Theorem $1(\sqrt{G})$ such that

$$x \;=\; u_1 \xi^{q_x}, \quad z \;=\; \frac{u_1}{x_1}\zeta_x^{q_x}, \qquad y \;=\; v_1 \eta^{q_y}, \quad z \;=\; \frac{v_1}{y_1}\zeta_y^{q_y}. \tag{6.6}$$

Again, comparing the z-values gives (4.19) and we get w from (4.20) of degree at most 2 not in $\overline{\mathbb{F}_p}$. Therefore Π_x, Π_y cannot both lie in $L(\overline{\mathbb{F}_p}^*)$.

Further, for $\Pi_x = (\xi, \zeta_x)$ one of the six points in Theorem $1(\sqrt{G})$ we deduce $q_x > 1$ from (4.21). But if now $\Pi_y = (\eta, \zeta_y)$ is in $L(\overline{\mathbb{F}_p}^*)$ we conclude by considering the degree of w that $q_x = 2$. With the last table in Appendix A we then deduce from $\zeta_x^2 = \zeta_y^{q_y} w$ that $\zeta_y^{q_y} = 1$ and so $\zeta_y = 1$, a contradiction to $\Pi_y \in L(\overline{\mathbb{F}_p}^*)$.

The same argument shows that there are no solutions in the case with Π_x in $L(\overline{\mathbb{F}_p}^*)$ and Π_y one of the six points in Theorem $1(\sqrt{G})$.

Finally, we have the situation with Π_x, Π_y both among the six points in Theorem $1(\sqrt{G})$. Again we have $q_x > 1$ and $q_y > 1$ and if $p \geq 3$ this leads to a contradiction by degrees.

Therefore q_x, q_y are powers of 2 in $\mathbb{Z}$; and since $w = \frac{\zeta_x^{q_x}}{\zeta_y^{q_y}}$ has degree at most 2 it is the square of an element which by inspection of the last table of

Appendix A we see must lie in (2.9). Further it is easily seen from (4.19) and the calculations in Appendix A that $(q_x, q_y) = (2,2), (2,4), (4,2)$. But on a closer look we actually see that the last two cases lead to the same solutions with just x and y exchanged. Although our (x, y, z) has already been adjusted in its S_4-orbit, we stay in this orbit and also in the current case (3) of Lemma 19 if we interchange x and y; and therefore we can restrict to $q_x = 2$.

Next, we note that for each ξ in the list (2.9) there is an automorphism ω_ξ of $\overline{\mathbb{F}_p}(t)$ taking t to ξ. Further ω_ξ preserves $\sqrt{G} \cap \overline{\mathbb{F}_p}(t)$ as well as each of the cases (2), (3). We get an automorphism group Σ_3 isomorphic to S_3.

Now the action of Σ_3 allows us to assume $\zeta_x = t$. Nevertheless we still have the six possibilities for ζ_y in the list (2.9) each with an exponent $q_y = 2, 4$.

Taking first $\zeta_y = t$ we conclude that $q_y \neq 2$ because $w \neq 1$. And comparing the last table in Appendix A we find that $x_1 = \frac{1}{1-t}$, $u_1 = \frac{t}{1-t}$ for $q_y = 4$. This provides the point

$$\Pi^* \;=\; \big(t(1-t), (1-t)^3, t^3\big)\,.$$

Actually, the three cases $\zeta_y = \frac{1}{t}, \frac{1}{1-t}, \frac{1-t}{t}$ are ruled out at once because here the degree of w is bigger than 2. And further the same considerations for the remaining values $\zeta_y = 1-t, \frac{t}{1-t}$ lead to points in the orbit $S_4(\Pi^*)$. Furthermore, we note that the S_4-orbit of Π^* is even invariant under Σ_3, and hence only $S_4(\Pi^*)$ turns up in our current case (3) when we reverse the Σ_3-action.

6.1.2 The case (2) of Lemma 19

We now get back to case (2) of Lemma 19, which we left halfway through the discussion above. Here $y = \frac{Y}{W}$ is in C and hence by (6.4) we have $\alpha = -1$ and so $u_1 = 0, v_1 = -1$. Again it is this second case which provides most of the points.

However, recalling that $x_1 + y_1 = 1$ with x_1 in the list (2.9) the equations in (6.5) become

$$x \;=\; -\,x_1 z, \qquad -\,y - (1-x_1)z \;=\; 1;$$

and moreover, with the $\sqrt{G}$-automorphism ψ defined by

$$\psi(x,y,z) \;=\; \left(\frac{1-x_1}{x_1}x, -y, -(1-x_1)z\right)$$

and $(x', y', z') = \psi(x, y, z)$ we see

$$x' \;=\; z', \qquad y' + z' \;=\; 1.$$

Here Theorem $1(\sqrt{G})$ shows that (y', z') is either in $L(\overline{\mathbb{F}_p}^*)$ or is a q^{th} power of one of the six points there because y' in C.

Suppose first $(y', z') = (1-b, b)$ with $b \neq 1$ in $\overline{\mathbb{F}_p}^*$. Then by Σ_3 we may assume that $x_1 = t$, which by ψ^{-1} leads to the point

$$(x,y,z) \;=\; \left(\frac{bt}{1-t}, b-1, -\frac{b}{1-t}\right)$$

with projective form

$$(bt, (b-1)(1-t), -b, 1-t)\,. \tag{6.7}$$

Then with $a = \frac{1}{b} \neq 1$ in $\overline{\mathbb{F}_p}^*$ and applying S_4 we may replace this point by

$$\Pi_1(a) \;=\; (-t, (a-1)(1-t), -a(1-t))\,.$$

However, the application of Σ_3 to (6.7) gives rise to the additional projective quadruples (up to S_4)

$$(b(1-t), (b-1)t, -b, t)$$

and

$$(-b(1-t), b-1, -bt, 1)\,.$$

These lead (by S_4 and with $a = \frac{1}{b}$ and $a = b$ respectively) to the points

$$\Pi_2(a) \;=\; (-(1-t), (a-1)t, -at)$$

and

$$\Pi_3(a) \;=\; (-a(1-t), a-1, -at)$$

respectively.

Suppose next that (y', z') is a q^{th} power of one of the six points in Theorem 1. Due to Σ_3 we may assume that $(y', z') = (t^q, (1-t)^q)$ with $q = p^e$ and since $y' = -y$ is in C we have $e \in \mathbb{N}$. We find

$$(x, y, z) \;=\; \psi^{-1}(x', y', z') \;=\; \left(\frac{x_1(1-t)^q}{1-x_1}, -t^q, -\frac{(1-t)^q}{1-x_1}\right)$$

where x_1 is in the list (2.9). Taking each of these in turn we find three families of solutions (up to S_4). The first is

$$(x, y, z) \;=\; (\psi_1^{-1}\varphi^e\psi_1)\Pi_1 \;=\; \big(t(1-t)^{q-1}, -t^q, -(1-t)^{q-1}\big)$$

with

$$\Pi_1 \;=\; (t, -t, -1) \qquad \text{and} \qquad \psi_1(x, y, z) \;=\; \left(\frac{1-t}{t}x, -y, -(1-t)z\right),$$

the second is

$$(x, y, z) \;=\; (\psi_2^{-1}\varphi^e\psi_2)\Pi_2 \;=\; \left(\frac{(1-t)^{q+1}}{t}, -t^q, -\frac{(1-t)^q}{t}\right)$$

with

$$\Pi_2 \;=\; \left(\frac{(1-t)^2}{t}, -t, -\frac{1-t}{t}\right) \qquad \text{and} \qquad \psi_2(x, y, z) \;=\; \left(\frac{t}{1-t}x, -y, -tz\right),$$

and the third is

$$(x, y, z) \;=\; (\psi_3^{-1}\varphi^e\psi_3)\Pi_3 \;=\; \big(-(1-t)^{q+1}, -t^q, -t(1-t)^q\big)$$

with

$$\Pi_3 \;=\; \big(-(1-t)^2, -t, -t(1-t)\big) \qquad \text{and} \qquad \psi_3(x, y, z) \;=\; \left(-\frac{1}{1-t}x, -y, -\frac{1}{t}z\right).$$

Again we have to reverse the Σ_3-action. As above we consider the projective form of each new family to prevent counting the same S_4-orbit twice. All in all we find the following six additional families.

1. $$(x,y,z) \;=\; (\psi_4^{-1}\varphi^e\psi_4)\Pi_4 \;=\; \big(t^{q-1}(1-t), -(1-t)^q, -t^{q-1}\big)$$
   with $\Pi_4 = (1-t, -(1-t), -1)$ and $\psi_4 = \psi_2$.

2. $$(x,y,z) \;=\; (\psi_5^{-1}\varphi^e\psi_5)\Pi_5 \;=\; \left(-\frac{1-t}{t^q}, \frac{(1-t)^q}{t^q}, -\frac{1}{t^{q-1}}\right)$$
   with $\Pi_5 = \big(-\frac{1-t}{t}, \frac{1-t}{t}, -1\big)$ and $\psi_5 = \psi_3$.

3. $$(x,y,z) \;=\; (\psi_6^{-1}\varphi^e\psi_6)\Pi_6 \;=\; \left(\frac{t^{q+1}}{1-t}, -(1-t)^q, -\frac{t^q}{1-t}\right)$$
   with $\Pi_6 = \left(\frac{t^2}{1-t}, -(1-t), -\frac{t}{1-t}\right)$ and $\psi_6 = \psi_1$.

4. $$(x,y,z) \;=\; (\psi_7^{-1}\varphi^e\psi_7)\Pi_7 \;=\; \left(-\frac{1}{t^q(1-t)}, \frac{(1-t)^q}{t^q}, \frac{1}{t^{q-1}(1-t)}\right)$$
   with $\Pi_7 = \left(-\frac{1}{t(1-t)}, \frac{1-t}{t}, \frac{1}{1-t}\right)$ and $\psi_7(x,y,z) = \big(-(1-t)x, -y, \frac{1-t}{t}z\big)$.

5. $$(x,y,z) \;=\; (\psi_8^{-1}\varphi^e\psi_8)\Pi_8 \;=\; \left(\frac{t^{q+1}}{(1-t)^q}, -\frac{1}{(1-t)^q}, \frac{t^q}{(1-t)^{q-1}}\right)$$
   with $\Pi_8 = \left(\frac{t^2}{1-t}, -\frac{1}{1-t}, t\right)$ and $\psi_8(x,y,z) = \left(-\frac{1}{t}x, -y, -\frac{1}{1-t}z\right)$.

6. $$(x,y,z) \;=\; (\psi_9^{-1}\varphi^e\psi_9)\Pi_9 \;=\; \left(-\frac{1}{t(1-t)^q}, \frac{t^q}{(1-t)^q}, \frac{1}{t(1-t)^{q-1}}\right)$$
   with $\Pi_9 = \left(-\frac{1}{t(1-t)}, \frac{t}{1-t}, \frac{1}{t}\right)$ and $\psi_9(x,y,z) = \left(-tx, -y, \frac{t}{1-t}z\right)$.

Thus everything in Proposition 3 turned up and its proof is thereby completed. □

6.2 The case $d = 3$

Proposition 4. *Let x, y, z in $\sqrt[S]{G}$ satisfy $x + y + z = -1$ and assume that $d = \dim_C Cx + Cy + Cz = 3$. If $p \geq 5$ then (x,y,z) is in the set*

$$S_4(\Pi_2) \;\cup\; S_4(\Pi_3) \;\cup\; S_4(\Pi_8) \;\cup\; \bigcup_{i=0}^{3} S_4(\Pi_i^*)$$

for the points Π_2, Π_3, Π_8 from Proposition 3 and

$$\begin{aligned}
\Pi_0^* &= \big(-t^3, -3t(1-t), -(1-t)^3\big)\,, & \Pi_1^* &= \big(-t^2, -2t(1-t), -(1-t)^2\big)\,,\\
\Pi_2^* &= \big(t^2, -2t, -(1-t)^2\big)\,, & \Pi_3^* &= \big((1-t)^2, -2(1-t), -t^2\big)\,.
\end{aligned}$$

If $p = 3$ then (x, y, z) is in the set

$$S_4(\Pi_2) \;\cup\; S_4(\Pi_3) \;\cup\; S_4(\Pi_8) \;\cup\; \bigcup_{i=1}^{3} S_4(\Pi_i^*).$$

Further there are no solutions for $p = 2$.

We need a preliminary lemma in which we use the set $\mathcal{H}$ from (4.4).

Lemma 20. *Suppose X_0, Y_0, Z_0, W_0 are coprime in $\mathcal{H}$ with X_0, Y_0, Z_0 linearly independent over C. If the space of (a_0, b_0, c_0, d_0) in $\mathbb{F}_p^4$ with*

$$a_0X_0 + b_0Y_0 + c_0Z_0 + d_0W_0 \;=\; 0 \tag{6.8}$$

contains a point with $a_0b_0c_0d_0 \neq 0$ then this space has dimension 1 and

$$\left(\frac{a_0X_0}{d_0W_0}, \frac{b_0Y_0}{d_0W_0}, \frac{c_0Z_0}{d_0W_0}\right)$$

is S_4-equivalent to one of $\Pi_2, \Pi_3, \Pi_8, \Pi_1^*, \Pi_2^*, \Pi_3^*$ and (only if $p \neq 3$) Π_0^*.

Proof. It is clear that the space has dimension at most 1 and that X_0, Y_0, Z_0, W_0 in $\mathcal{H}$ are different, otherwise X_0, Y_0, Z_0 would be linearly dependent over $\mathbb{F}_p$ and so over C.
We arrange the 10 elements of $\mathcal{H}$ in some order and consider the 210 quadruples (X_0, Y_0, Z_0, W_0) with different X_0, Y_0, Z_0, W_0 in ascending order. Forgetting for the moment about the last entry W_0 we calculate for each of these the Wronskian $\mathcal{W}(X_0, Y_0, Z_0)$ considered in $\mathbb{Z}$. We reject those where this Wronskian is zero mod p (if $p \geq 5$ this turns out to be equivalent to being zero in $\mathbb{Z}$), else X_0, Y_0, Z_0 would be linearly dependent over C due to Lemma 9. Further we sort out all the quadruples where X_0, Y_0, Z_0, W_0 are not coprime. There remain 169 quadruples (X_0, Y_0, Z_0, W_0) provided $p \geq 5$ and just 144 provided $p = 3$. For each of these we equate coefficients in (6.8) to obtain a system of four homogeneous linear equations in a_0, b_0, c_0, d_0. We calculate the determinant in $\mathbb{Z}$, and we reject those with determinant non-zero mod p (again if $p \geq 5$ this turns out to be equivalent to being non-zero in $\mathbb{Z}$). For the remaining systems we calculate a generator (a_0, b_0, c_0, d_0) in $\mathbb{Z}^4$ and we reject those with $a_0b_0c_0d_0$ zero mod p (again automatic if $p \geq 5$). We find 7 different quadruples $(a_0X_0, b_0Y_0, c_0Z_0, d_0W_0)$ provided $p \geq 5$ and just 6 provided $p = 3$ (See however our calculations in Appendix B). The lemma follows. □

Proof of Proposition 4. First of all we mention that $p \geq 3$ because $[S : C] = p = 2$ would imply that x, y and z are linearly dependent over C.

Similar to the proof of Proposition 1 we start by taking $x + y + z = -1$ as well as its first and second derivative. We then see an associated determinant

$$\Delta \;=\; \begin{vmatrix} 1 & 1 & 1 \\ \frac{\dot{x}}{x} & \frac{\dot{y}}{y} & \frac{\dot{z}}{z} \\ \frac{\ddot{x}}{x} & \frac{\ddot{y}}{y} & \frac{\ddot{z}}{z} \end{vmatrix}$$

and multiplying by xyz yields the Wronskian of x, y, z. Due to $d = 3$ these latter are linearly independent over our field C of differential constants and we deduce by Lemma 9 that $\Delta \neq 0$. Therefore we get in the usual way (4.5) with now

$$\Delta_x \;=\; \begin{vmatrix} -1 & 1 & 1 \\ 0 & \frac{\dot{y}}{y} & \frac{\dot{z}}{z} \\ 0 & \frac{\ddot{y}}{y} & \frac{\ddot{z}}{z} \end{vmatrix}, \qquad \Delta_y \;=\; \begin{vmatrix} 1 & -1 & 1 \\ \frac{\dot{x}}{x} & 0 & \frac{\dot{z}}{z} \\ \frac{\ddot{x}}{x} & 0 & \frac{\ddot{z}}{z} \end{vmatrix}, \qquad \Delta_z \;=\; \begin{vmatrix} 1 & 1 & -1 \\ \frac{\dot{x}}{x} & \frac{\dot{y}}{y} & 0 \\ \frac{\ddot{x}}{x} & \frac{\ddot{y}}{y} & 0 \end{vmatrix}.$$

Again Lemma 12 then implies that x, y, z are in k of degree at most 3. And by Lemma 10 we know that $\sqrt[k]{G}$ is generated by G together with the elements of $\mathbb{F}_p^*$. Thus we may assume that in terms of (4.1) we have

$$a_0X_0 + b_0Y_0 + c_0Z_0 + d_0W_0 \;=\; 0$$

with a_0, b_0, c_0, d_0 in $\mathbb{F}_p^*$ and X_0, Y_0, Z_0, W_0 in $\mathcal{H}$. Furthermore Lemma 7 and Lemma 8 imply

$$0 \;\neq\; \mathcal{W}(x, y, z) \;=\; \mathcal{W}\left(\frac{a_0X_0}{d_0W_0}, \frac{b_0Y_0}{d_0W_0}, \frac{c_0Z_0}{d_0W_0}\right) \;=\; \frac{a_0b_0c_0}{d_0^3W_0^3}\mathcal{W}(X_0, Y_0, Z_0).$$

Therefore X_0, Y_0, Z_0 are linearly independent over C, and by (4.1) it is also clear that X_0, Y_0, Z_0, W_0 can be assumed to be coprime. Now the proof of Proposition 4 follows by Lemma 20. □

7 Proof of Theorem $2(\sqrt{G})$

We start with the analogue of Theorem $2(\sqrt{G})$ for (1.8).

Theorem $\widetilde{2}(\sqrt{G})$. *Suppose $K = \overline{\mathbb{F}_p(t)}$, $G = \langle t, 1-t\rangle$ and that the plane $\widetilde{P}$ is defined by $x+y+z=-1$. Then $\widetilde{P}(\sqrt{G})$ is*

$$\begin{aligned}\widetilde{P}(\overline{\mathbb{F}_p}^*) \;\cup\; \widetilde{T}_x(\sqrt{G}) \;\cup\; \widetilde{T}_y(\sqrt{G}) \;\cup\; \widetilde{T}_z(\sqrt{G})&\\ \cup \bigcup_{\Pi\in\widetilde{\mathcal{T}}'} \widetilde{M_\Pi}(\overline{\mathbb{F}_p}^*)\cdot[[\psi_0]]_p\Pi \;\cup\; \bigcup_{\Pi\in\widetilde{\mathcal{T}}_p}[[\psi_0]]_p\Pi \;\cup\; \bigcup_{\Pi\in\widetilde{\mathcal{T}}}[[\psi_0]]_p[\psi_\Pi]_p\Pi&\end{aligned}$$

for a set $\widetilde{\mathcal{T}}'$ of 36 points Π in $(\sqrt{G})^3$ with lines $\widetilde{M_\Pi}$, a set $\widetilde{\mathcal{T}}_p$ of points Π in $(\sqrt{G})^3$, and a set $\widetilde{\mathcal{T}}$ of 216 points Π in $(\sqrt{G})^3$ with $\sqrt{G}$-automorphisms ψ_Π. Further if $p \geq 5$ then $\widetilde{\mathcal{T}}_p$ contains 96 points, if $p=3$ then 72 points, and if $p=2$ then just 24 points.

Proof. We first show that $\widetilde{P}(\sqrt{G})$ is contained in the above union. Accordingly let x, y, z in $\sqrt{G}$ satisfy $x+y+z=-1$. If they are all in $\overline{\mathbb{F}_p}^* \subset \sqrt{G}$, then it is rather clear that we may write

$$(x,y,z) \;=\; (\alpha,\beta,-1-\alpha-\beta)$$

with α,β in $\overline{\mathbb{F}_p}^*$ satisfying $\alpha+\beta \neq -1$. Otherwise Lemma 6 provides e_x, e_y, e_z in $\mathbb{Z}$ such that $x^{p^{e_x}}$, $y^{p^{e_y}}$, $z^{p^{e_z}}$ lie in S but not in C. Therefore we conclude that with $e = \max\{e_x,e_y,e_z\}$ the triple

$$(\widetilde{x},\widetilde{y},\widetilde{z}) \;=\; (x^{p^e}, y^{p^e}, z^{p^e})$$

is in S^3 but not in C^3. Furthermore, we note that $\widetilde{x}+\widetilde{y}+\widetilde{z}=-1$ and that the dimension d of $C\widetilde{x}+C\widetilde{y}+C\widetilde{z}$ is either 2 or 3. Thus $(\widetilde{x},\widetilde{y},\widetilde{z})$ is as in Proposition 3 or Proposition 4; and we then get back to our original (x,y,z) by raising to the power p^{-e}. We shall look at these two Propositions in more detail now.

First, it is easily seen that from the set $\widetilde{T}^*_x(\sqrt[S]{G})$ we get the set $\widetilde{T}_x(\sqrt{G})$ of Theorem $\widetilde{2}(\sqrt{G})$ and similarly for the sets $\widetilde{T}^*_y(\sqrt[S]{G})$ and $\widetilde{T}^*_z(\sqrt[S]{G})$.

Next, supposing $(\widetilde{x},\widetilde{y},\widetilde{z}) = \Pi^*_0$ provided $p \geq 5$ we clearly get the set $[[\psi_0]]\Pi^*_0$ as well as its S_4-orbit; and similarly for the points Π^*_1, Π^*_2, Π^*_3 provided $p \geq 3$ as well as Π^* provided $p=2$. Then the S_4-orbits of these points lead to the set

$$\bigcup_{\Pi\in\widetilde{\mathcal{T}}_p}[[\psi_0]]_p\Pi$$

in Theorem $\widetilde{2}(\sqrt{G})$ with $\widetilde{\mathcal{T}}_p$ a set of 96 points in $\sqrt{G}^3$ provided $p \geq 5$ and $\widetilde{\mathcal{T}}_3$ a set of 72 points in $\sqrt{G}^3$ as well as $\widetilde{\mathcal{T}}_2$ a set of 24 points in $\sqrt{G}^3$.

In almost the same manner we can deal with $(\widetilde{x},\widetilde{y},\widetilde{z}) = \Pi_1(a)$ ($a \neq 1$ in $\overline{\mathbb{F}_p}^*$). First we see $\Pi_1(a) = \widetilde{M_\Pi}\cdot\Pi$ with $\Pi = (t, 1-t, 1-t)$ and a line $\widetilde{M_\Pi}$ parametrized by $(-1, a-1, -a)$. Here it is rather clear that the S_4-orbit of the point Π has just $|S_4|/2 = 12$ elements, because its second and third coordinate are equal. However, this does not hold for the S_4-orbit of $\widetilde{M_\Pi}$. But taking $b = 1-a$ in

$\overline{\mathbb{F}_p}^*$ we see $\widetilde{M_\Pi} = (-1,-b,b-1)$. Thus $(\widetilde{x},\widetilde{y},\widetilde{z})$ is in the union of $\widetilde{M_\Pi}(\overline{\mathbb{F}_p}^*)\cdot \Pi$ for 12 points Π; and going back to (x,y,z) we get a first subset of

$$\bigcup_{\Pi\in\widetilde{\mathcal{T}}'} \widetilde{M_\Pi}(\overline{\mathbb{F}_p}^*)\cdot[[\psi_0]]_p\Pi.$$

A second subset comes from $(\widetilde{x},\widetilde{y},\widetilde{z}) = \Pi_2(a)$ ($a \neq 1$ in $\overline{\mathbb{F}_p}^*$) by the exactly same considerations.

In a similar way we can handle $(\widetilde{x},\widetilde{y},\widetilde{z}) = \Pi_3(a)$ ($a \neq 1$ in $\overline{\mathbb{F}_p}^*$). Here we see a point $\Pi = (1-t,1,t)$ with a line $\widetilde{M_\Pi} = (-a,a-1,-a)$. Then the second and fourth coordinate of the projective Π are both 1. And taking $b = \frac{a}{a-1} \neq 1$ in $\overline{\mathbb{F}_p}^*$ in the projective $\widetilde{M_\Pi} = (-a,a-1,-a,1)$ we see $\widetilde{M_\Pi} = (-b,1,-b,b-1)$. This completes the union over $\widetilde{\mathcal{T}}'$ in Theorem $\widetilde{2}(\sqrt{G})$.

Finally, we have the situation where $(\widetilde{x},\widetilde{y},\widetilde{z})$ is in the set

$$\bigcup_{j=1}^{9} S_4([\psi_j]_p^*\Pi_j)$$

from Proposition 3. First we consider the missing case $e=0$ in $[\psi_j]_p^*$ there. Here we note that the points Π_1,Π_4,Π_5 are in the set $\widetilde{T}_z(\sqrt[S]{G})$ of Proposition 3 and the points $\Pi_2,\Pi_3,\Pi_6,\Pi_7,\Pi_8,\Pi_9$ turn up in Proposition 4 while $S_4(\Pi_6) = S_4(\Pi_2)$, $S_4(\Pi_7) = S_4(\Pi_3)$, and $S_4(\Pi_9) = S_4(\Pi_8)$. Therefore one may expect the set

$$\bigcup_{j=1}^{9} S_4([[\psi_0]]_p[\psi_j]_p\Pi_j) \tag{7.1}$$

in Theorem $\widetilde{2}(\sqrt{G})$.

But for e in $\mathbb{N}$ for example the point

$$(\widetilde{x},\widetilde{y},\widetilde{z}) \;=\; (\psi_1^{-1}\varphi^{-e}\psi_1)\Pi_1 \;=\; \Big(t(1-t)^{p^{-e}-1}, -t^{p^{-e}}, -(1-t)^{p^{-e}-1}\Big)$$

satisfies $\widetilde{x}+\widetilde{y}+\widetilde{z} = -1$ as well. So why do we not get $[[\psi_0,\psi_j]]_p$ in (7.1)? Actually, applying φ^e yields

$$\varphi^e(\psi_1^{-1}\varphi^{-e}\psi_1)\Pi_1 \;=\; \left(\frac{t^{p^e}}{(1-t)^{p^e-1}}, -t, -\frac{1}{(1-t)^{p^e-1}}\right),$$

which is in $S_4((\psi_1^{-1}\varphi^{e}\psi_1)\Pi_1)$; and thus we see that

$$S_4\big((\psi_1^{-1}\varphi^{-e}\psi_1)\Pi_1\big) \;=\; S_4\big(\varphi^{-e}[\psi_1]_p^*\Pi_1\big).$$

And similarly we find

$$\begin{aligned}
S_4\big((\psi_2^{-1}\varphi^{-e}\psi_2)\Pi_2\big) &= S_4\big(\varphi^{-e}[\psi_6]_p^*\Pi_6\big),\\
S_4\big((\psi_3^{-1}\varphi^{-e}\psi_3)\Pi_3\big) &= S_4\big(\varphi^{-e}[\psi_7]_p^*\Pi_7\big),\\
S_4\big((\psi_4^{-1}\varphi^{-e}\psi_4)\Pi_4\big) &= S_4\big(\varphi^{-e}[\psi_4]_p^*\Pi_4\big),\\
S_4\big((\psi_5^{-1}\varphi^{-e}\psi_5)\Pi_5\big) &= S_4\big(\varphi^{-e}[\psi_5]_p^*\Pi_5\big),\\
S_4\big((\psi_6^{-1}\varphi^{-e}\psi_6)\Pi_6\big) &= S_4\big(\varphi^{-e}[\psi_2]_p^*\Pi_2\big),\\
S_4\big((\psi_7^{-1}\varphi^{-e}\psi_7)\Pi_7\big) &= S_4\big(\varphi^{-e}[\psi_3]_p^*\Pi_3\big),\\
S_4\big((\psi_8^{-1}\varphi^{-e}\psi_8)\Pi_8\big) &= S_4\big(\varphi^{-e}[\psi_9]_p^*\Pi_9\big),\\
S_4\big((\psi_9^{-1}\varphi^{-e}\psi_9)\Pi_9\big) &= S_4\big(\varphi^{-e}[\psi_8]_p^*\Pi_8\big).
\end{aligned}$$

Therefore, it turns out that $[[\psi_0,\psi_j]]_p$ is not needed in (7.1) above.

Nevertheless, (7.1) still does not look like the corresponding set in Theorem $\widetilde{2}(\sqrt{G})$. But going back to the projective form of some $\sigma([[\psi_0]]_p[\psi_j]_p\Pi_j)$ for $\sigma\in S_4$ it is not difficult to see that this is $[[\psi_0]]_p[\psi_{j,\sigma}]_p\Pi_{j,\sigma}$ for some point $\Pi_{j,\sigma}$ and some $\sqrt{G}$-automorphism $\psi_{j,\sigma}$. Therefore we get the set

$$\bigcup_{\Pi\in\widetilde{\mathcal{T}}}[[\psi_0]]_p[\psi_\Pi]_p\Pi$$

as requested and this settles the first part of the proof.

It remains to show that all these sets above are contained in $\widetilde{P}(\sqrt{G})$. First, it is obvious that $\widetilde{P}(\overline{\mathbb{F}_p}^*), \widetilde{T}_x(\sqrt{G})$, $\widetilde{T}_y(\sqrt{G})$ and $\widetilde{T}_z(\sqrt{G})$ are in $\widetilde{P}(\sqrt{G})$. Next, if some Π is in $\widetilde{P}(\sqrt{G})$, then because $\widetilde{P}$ is defined over $\mathbb{F}_p$ clearly $[[\psi_0]]_p\Pi$ is in $\widetilde{P}(\sqrt{G})$. Finally, if some Π is in $\widetilde{P}(\sqrt{G})$ and there is a line L defined over $\mathbb{F}_p$ and a $\sqrt{G}$-automorphism ψ with $\psi(\Pi)\in L\subset\psi(P)$, then $[[\psi_0,\psi]]_p\Pi$ is in $\widetilde{P}(\sqrt{G})$. This is because any $\varphi^e\psi(\Pi)$ lies in $\varphi^e(L)=L$ so $\psi^{-1}\varphi\psi(\Pi)$ lies in $\psi^{-1}(L)$ and so in $\widetilde{P}$ thus also in $\widetilde{P}(\sqrt{G})$. This can be checked for the Π_i,ψ_i $(i=1,\dots,9)$ and in fact all the lines L that arise are the one in (6.5). This completes the proof of Theorem $\widetilde{2}(\sqrt{G})$. □

Proof of Theorem 2($\sqrt{G}$). Finally, one can quickly deduce Theorem $2(\sqrt{G})$ from Theorem $\widetilde{2}(\sqrt{G})$. For example $P=\widetilde{\psi}(\widetilde{P})$ and $\widetilde{P}=\widetilde{\psi}(P)$ with $\widetilde{\psi}(x,y,z)=(-x,-y,z)$. And because $\widetilde{\psi}$ (like any automorphism) commutes with any ψ and also (like any $\mathbb{F}_p^*$-automorphism) commutes with φ, it suffices just to change $\widetilde{T}_x$ to $T_x=\widetilde{\psi}(\widetilde{T}_x)$ and similar for T_y, T_z as well as for the other occurrent sets in Theorem $\widetilde{2}(\sqrt{G})$. Thereby Theorem $2(\sqrt{G})$ is proved. □

7.1 Proof of Theorem 2(G) for $p = 2$

We finally prove Theorem $2(G)$ on G for $p=2$ which now can be easily deduced from Theorem $2(\sqrt{G})$. Since $P(G)$ is a subset of $P(\sqrt{G})$ we just have to put out all the points not lying in G^3.

First, we mention that the set $\widetilde{P}(\overline{\mathbb{F}_p}^*)$ provides no solutions over G because $\overline{\mathbb{F}_2}^*\cap G$ is empty. Next, the sets $T_x(\sqrt{G}), T_y(\sqrt{G})$ and $T_z(\sqrt{G})$ become of course

$T_x(G), T_y(G)$ and $T_z(G)$ respectively.

Turning to the set

$$\bigcup_{\Pi \in \mathcal{T}'} M_\Pi(\overline{\mathbb{F}_2}^*) \cdot [[\psi_0]]_p \Pi$$

we obtain no solutions over G again because $\overline{\mathbb{F}_2}^* \cap G$ is empty.

For the last two sets

$$\bigcup_{\Pi \in \mathcal{T}_2} [[\psi_0]]_2 \Pi \qquad \text{and} \qquad \bigcup_{\Pi \in \mathcal{T}} [[\psi_0, \psi_\Pi]]_2 \Pi$$

we can argue similarly as we did in Lemma 16. It is then rather clear that the double brackets become single brackets while the points in $\mathcal{T}_2$ and $\mathcal{T}$ as well as the G-automorphisms ψ_Π remain exactly the same. Theorem $2(G)$ for $p = 2$ is thereby proved.

A Tables for (4.19)

Here we present the calculations mentioned above in the sections 4.2.2 and 6.1.1 respectively.

In the first two tables below we calculate for all ζ_x, ζ_y in the list (2.9), however **without regarding the signs**, the expression

$$\frac{\zeta_x^{q_x}}{\zeta_y^{q_y}}$$

from (4.19), while q_x and q_y are assumed to be powers of p in $\mathbb{Z}$.

$\zeta_y \backslash \zeta_x$	t	$1-t$	$\frac{1}{t}$
t	$t^{q_x-q_y}$	$t^{-q_y}(1-t)^{q_x}$	$t^{-q_x-q_y}$
$1-t$	$t^{q_x}(1-t)^{-q_y}$	$(1-t)^{q_x-q_y}$	$t^{-q_x}(1-t)^{-q_y}$
$\frac{1}{t}$	$t^{q_x+q_y}$	$t^{q_y}(1-t)^{q_x}$	$t^{-q_x+q_y}$
$\frac{1-t}{t}$	$t^{q_x+q_y}(1-t)^{-q_y}$	$t^{q_y}(1-t)^{q_x-q_y}$	$t^{-q_x+q_y}(1-t)^{-q_y}$
$\frac{1}{1-t}$	$t^{q_x}(1-t)^{q_y}$	$(1-t)^{q_x+q_y}$	$t^{-q_x}(1-t)^{q_y}$
$\frac{t}{1-t}$	$t^{q_x-q_y}(1-t)^{q_y}$	$t^{-q_y}(1-t)^{q_x+q_y}$	$t^{-q_x-q_y}(1-t)^{q_y}$

$\zeta_y \backslash \zeta_x$	$\frac{1-t}{t}$	$\frac{1}{1-t}$	$\frac{t}{1-t}$
t	$t^{-q_x-q_y}(1-t)^{q_x}$	$t^{-q_y}(1-t)^{-q_x}$	$t^{q_x-q_y}(1-t)^{-q_x}$
$1-t$	$t^{-q_x}(1-t)^{q_x-q_y}$	$(1-t)^{-q_x-q_y}$	$t^{q_x}(1-t)^{-q_x-q_y}$
$\frac{1}{t}$	$t^{-q_x+q_y}(1-t)^{q_x}$	$t^{q_y}(1-t)^{-q_x}$	$t^{q_x+q_y}(1-t)^{-q_x}$
$\frac{1-t}{t}$	$t^{-q_x+q_y}(1-t)^{q_x-q_y}$	$t^{q_y}(1-t)^{-q_x-q_y}$	$t^{q_x+q_y}(1-t)^{-q_x-q_y}$
$\frac{1}{1-t}$	$t^{-q_x}(1-t)^{q_x+q_y}$	$(1-t)^{-q_x+q_y}$	$t^{q_x}(1-t)^{-q_x+q_y}$
$\frac{t}{1-t}$	$t^{-q_x-q_y}(1-t)^{q_x+q_y}$	$t^{-q_y}(1-t)^{-q_x+q_y}$	$t^{q_x-q_y}(1-t)^{-q_x+q_y}$

In the following table we calculate for all $x_1, -u_1$ in the list (2.9) the expression

$$\frac{x_1 v_1}{u_1 y_1} \quad = \quad -\frac{x_1(1+u_1)}{u_1(1-x_1)}$$

from (4.19) (recall that $x_1 + y_1 = 1$ and $u_1 + v_1 = -1$ from (4.12) and (6.3) respectively).

x_1 $-u_1$	t	$1-t$	$\frac{1}{t}$	$-\frac{1-t}{t}$	$\frac{1}{1-t}$	$-\frac{t}{1-t}$
t	1	$\frac{(1-t)^2}{t^2}$	$-\frac{1}{t}$	$-\frac{(1-t)^2}{t}$	$-\frac{1-t}{t^2}$	$-(1-t)$
$1-t$	$\frac{t^2}{(1-t)^2}$	1	$-\frac{t}{(1-t)^2}$	$-t$	$-\frac{1}{1-t}$	$-\frac{t^2}{1-t}$
$\frac{1}{t}$	$-t$	$-\frac{(1-t)^2}{t}$	1	$(1-t)^2$	$\frac{1-t}{t}$	$t(1-t)$
$-\frac{1-t}{t}$	$-\frac{t}{(1-t)^2}$	$-\frac{1}{t}$	$\frac{1}{(1-t)^2}$	1	$\frac{1}{t(1-t)}$	$\frac{t}{1-t}$
$\frac{1}{1-t}$	$-\frac{t^2}{1-t}$	$-(1-t)$	$\frac{t}{1-t}$	$t(1-t)$	1	t^2
$-\frac{t}{1-t}$	$-\frac{1}{1-t}$	$-\frac{1-t}{t^2}$	$\frac{1}{t(1-t)}$	$\frac{1-t}{t}$	$\frac{1}{t^2}$	1

B Calculations for Lemma 20

Here we present the calculations we mentioned in the proof of Lemma 20. First, we order the elements of $\mathcal{H}$ in the following way

$$1, t, 1-t, t^2, t(1-t), (1-t)^2, t^3, t^2(1-t), t(1-t)^2, (1-t)^3.$$

Taking the 210 quadruples (X_0, Y_0, Z_0, W_0) with different X_0, Y_0, Z_0, W_0 in ascending order we reject those where the Wronskian $\mathcal{W}(X_0, Y_0, Z_0)$ is zero mod p. Further we sort out all the quadruples where X_0, Y_0, Z_0, W_0 are not coprime. For $p = 3$ there remain the following 144 quadruples (X_0, Y_0, Z_0, W_0).

1. $\big(1, t, t^2, t(1-t)\big)$,
2. $\big(1, t, t^2, (1-t)^2\big)$,
3. $\big(1, t, t^2, t^3\big)$,
4. $\big(1, t, t^2, t^2(1-t)\big)$,
5. $\big(1, t, t^2, t(1-t)^2\big)$,
6. $\big(1, t, t^2, (1-t)^3\big)$,
7. $\big(1, t, t(1-t), (1-t)^2\big)$,
8. $\big(1, t, t(1-t), t^3\big)$,
9. $\big(1, t, t(1-t), t^2(1-t)\big)$,
10. $\big(1, t, t(1-t), t(1-t)^2\big)$,
11. $\big(1, t, t(1-t), (1-t)^3\big)$,
12. $\big(1, t, (1-t)^2, t^3\big)$,
13. $\big(1, t, (1-t)^2, t^2(1-t)\big)$,
14. $\big(1, t, (1-t)^2, t(1-t)^2\big)$,
15. $\big(1, t, (1-t)^2, (1-t)^3\big)$,
16. $\big(1, t, t^2(1-t), t(1-t)^2\big)$,
17. $\big(1, t, t^2(1-t), (1-t)^3\big)$,
18. $\big(1, t, t(1-t)^2, (1-t)^3\big)$,
19. $\big(1, 1-t, t^2, t(1-t)\big)$,
20. $\big(1, 1-t, t^2, (1-t)^2\big)$,
21. $\big(1, 1-t, t^2, t^3\big)$,
22. $\big(1, 1-t, t^2, t^2(1-t)\big)$,
23. $\big(1, 1-t, t^2, t(1-t)^2\big)$,
24. $\big(1, 1-t, t^2, (1-t)^3\big)$,
25. $\big(1, 1-t, t(1-t), (1-t)^2\big)$,
26. $\big(1, 1-t, t(1-t), t^3\big)$,
27. $\big(1, 1-t, t(1-t), t^2(1-t)\big)$,
28. $\big(1, 1-t, t(1-t), t(1-t)^2\big)$,
29. $\big(1, 1-t, t(1-t), (1-t)^3\big)$,
30. $\big(1, 1-t, (1-t)^2, t^3\big)$,
31. $\big(1, 1-t, (1-t)^2, t^2(1-t)\big)$,
32. $\big(1, 1-t, (1-t)^2, t(1-t)^2\big)$,
33. $\big(1, 1-t, (1-t)^2, (1-t)^3\big)$,
34. $\big(1, 1-t, t^2(1-t), t(1-t)^2\big)$,
35. $\big(1, 1-t, t^2(1-t), (1-t)^3\big)$,
36. $\big(1, 1-t, t(1-t)^2, (1-t)^3\big)$,
37. $\big(1, t^2, t(1-t), (1-t)^2\big)$,
38. $\big(1, t^2, t(1-t), t^3\big)$,
39. $\big(1, t^2, t(1-t), t^2(1-t)\big)$,
40. $\big(1, t^2, t(1-t), t(1-t)^2\big)$,
41. $\big(1, t^2, t(1-t), (1-t)^3\big)$,
42. $\big(1, t^2, (1-t)^2, t^3\big)$,
43. $\big(1, t^2, (1-t)^2, t^2(1-t)\big)$,
44. $\big(1, t^2, (1-t)^2, t(1-t)^2\big)$,
45. $\big(1, t^2, (1-t)^2, (1-t)^3\big)$,
46. $\big(1, t^2, t(1-t)^2, (1-t)^3\big)$,

47. $\big(1, t(1-t), (1-t)^2, t^3\big)$,

48. $\big(1, t(1-t), (1-t)^2, t^2(1-t)\big)$,

49. $\big(1, t(1-t), (1-t)^2, t(1-t)^2\big)$,

50. $\big(1, t(1-t), (1-t)^2, (1-t)^3\big)$,

51. $\big(1, t(1-t), t^2(1-t), t(1-t)^2\big)$,

52. $\big(1, t(1-t), t^2(1-t), (1-t)^3\big)$,

53. $\big(1, t(1-t), t(1-t)^2, (1-t)^3\big)$,

54. $\big(1, (1-t)^2, t^2(1-t), t(1-t)^2\big)$,

55. $\big(1, (1-t)^2, t^2(1-t), (1-t)^3\big)$,

56. $\big(1, t^2(1-t), t(1-t)^2, (1-t)^3\big)$,

57. $\big(t, 1-t, t^2, t(1-t)\big)$,

58. $\big(t, 1-t, t^2, (1-t)^2\big)$,

59. $\big(t, 1-t, t^2, t^3\big)$,

60. $\big(t, 1-t, t^2, t^2(1-t)\big)$,

61. $\big(t, 1-t, t^2, t(1-t)^2\big)$,

62. $\big(t, 1-t, t^2, (1-t)^3\big)$,

63. $\big(t, 1-t, t(1-t), (1-t)^2\big)$,

64. $\big(t, 1-t, t(1-t), t^3\big)$,

65. $\big(t, 1-t, t(1-t), t^2(1-t)\big)$,

66. $\big(t, 1-t, t(1-t), t(1-t)^2\big)$,

67. $\big(t, 1-t, t(1-t), (1-t)^3\big)$,

68. $\big(t, 1-t, (1-t)^2, t^3\big)$,

69. $\big(t, 1-t, (1-t)^2, t^2(1-t)\big)$,

70. $\big(t, 1-t, (1-t)^2, t(1-t)^2\big)$,

71. $\big(t, 1-t, (1-t)^2, (1-t)^3\big)$,

72. $\big(t, 1-t, t^2(1-t), t(1-t)^2\big)$,

73. $\big(t, 1-t, t^2(1-t), (1-t)^3\big)$,

74. $\big(t, 1-t, t(1-t)^2, (1-t)^3\big)$,

75. $\big(t, t^2, (1-t)^2, t^3\big)$,

76. $\big(t, t^2, (1-t)^2, t^2(1-t)\big)$,

77. $\big(t, t^2, (1-t)^2, t(1-t)^2\big)$,

78. $\big(t, t^2, (1-t)^2, (1-t)^3\big)$,

79. $\big(t, t^2, t^3, (1-t)^3\big)$,

80. $\big(t, t^2, t^2(1-t), (1-t)^3\big)$,

81. $\big(t, t^2, t(1-t)^2, (1-t)^3\big)$,

82. $\big(t, t(1-t), (1-t)^2, t^3\big)$,

83. $\big(t, t(1-t), (1-t)^2, t^2(1-t)\big)$,

84. $\big(t, t(1-t), (1-t)^2, t(1-t)^2\big)$,

85. $\big(t, t(1-t), (1-t)^2, (1-t)^3\big)$,

86. $\big(t, t(1-t), t^3, (1-t)^3\big)$,

87. $\big(t, t(1-t), t^2(1-t), (1-t)^3\big)$,

88. $\big(t, t(1-t), t(1-t)^2, (1-t)^3\big)$,

89. $\big(t, (1-t)^2, t^3, t^2(1-t)\big)$,

90. $\big(t, (1-t)^2, t^3, t(1-t)^2\big)$,

91. $\big(t, (1-t)^2, t^3, (1-t)^3\big)$,

92. $\big(t, (1-t)^2, t^2(1-t), t(1-t)^2\big)$,

93. $\big(t, (1-t)^2, t^2(1-t), (1-t)^3\big)$,

94. $\big(t, (1-t)^2, t(1-t)^2, (1-t)^3\big)$,

95. $\big(t, t^3, t^2(1-t), (1-t)^3\big)$,

96. $\big(t, t^3, t(1-t)^2, (1-t)^3\big)$,

97. $\big(t, t^2(1-t), t(1-t)^2, (1-t)^3\big)$,

98. $\big(1-t, t^2, t(1-t), (1-t)^2\big)$,

99. $\big(1-t, t^2, t(1-t), t^3\big)$,

100. $\big(1-t, t^2, t(1-t), t^2(1-t)\big)$,

101. $\big(1-t, t^2, t(1-t), t(1-t)^2\big)$,

102. $\big(1-t, t^2, t(1-t), (1-t)^3\big)$,

103. $\big(1-t, t^2, (1-t)^2, t^3\big)$,

104. $\big(1-t, t^2, (1-t)^2, t^2(1-t)\big)$,

105. $\big(1-t, t^2, (1-t)^2, t(1-t)^2\big)$,

106. $\big(1-t, t^2, (1-t)^2, (1-t)^3\big)$,

107. $\big(1-t, t^2, t^3, t^2(1-t)\big)$,

108. $\big(1-t, t^2, t^3, t(1-t)^2\big)$,

109. $\big(1-t, t^2, t^3, (1-t)^3\big)$,

110. $\big(1-t, t^2, t^2(1-t), t(1-t)^2\big)$,

111. $\big(1-t, t^2, t^2(1-t), (1-t)^3\big)$,

112. $\big(1-t, t^2, t(1-t)^2, (1-t)^3\big)$,

113. $\big(1-t, t(1-t), t^3, t^2(1-t)\big)$,

114. $\big(1-t, t(1-t), t^3, t(1-t)^2\big)$,

115. $\big(1-t, t(1-t), t^3, (1-t)^3\big)$,

116. $\big(1-t, (1-t)^2, t^3, t^2(1-t)\big)$,

117. $\big(1-t, (1-t)^2, t^3, t(1-t)^2\big)$,

118. $\big(1-t, (1-t)^2, t^3, (1-t)^3\big)$,

119. $\big(1-t, t^3, t^2(1-t), t(1-t)^2\big)$,

120. $\big(1-t, t^3, t^2(1-t), (1-t)^3\big)$,

121. $\big(1-t, t^3, t(1-t)^2, (1-t)^3\big)$,

122. $\big(t^2, t(1-t), (1-t)^2, t^3\big)$,

123. $\big(t^2, t(1-t), (1-t)^2, t^2(1-t)\big)$,

124. $\big(t^2, t(1-t), (1-t)^2, t(1-t)^2\big)$,

125. $\big(t^2, t(1-t), (1-t)^2, (1-t)^3\big)$,

126. $\big(t^2, t(1-t), t^3, (1-t)^3\big)$,

127. $\big(t^2, t(1-t), t^2(1-t), (1-t)^3\big)$,

128. $\big(t^2, t(1-t), t(1-t)^2, (1-t)^3\big)$,

129. $\big(t^2, (1-t)^2, t^3, t^2(1-t)\big)$,

130. $\big(t^2, (1-t)^2, t^3, t(1-t)^2\big)$,

131. $\big(t^2, (1-t)^2, t^3, (1-t)^3\big)$,

132. $\big(t^2, (1-t)^2, t^2(1-t), t(1-t)^2\big)$,

133. $\big(t^2, (1-t)^2, t^2(1-t), (1-t)^3\big)$,

134. $\big(t^2, (1-t)^2, t(1-t)^2, (1-t)^3\big)$,

135. $\big(t^2, t^3, t(1-t)^2, (1-t)^3\big)$,

136. $\big(t^2, t^2(1-t), t(1-t)^2, (1-t)^3\big)$,

137. $\big(t(1-t), (1-t)^2, t^3, t^2(1-t)\big)$,

138. $\big(t(1-t), (1-t)^2, t^3, t(1-t)^2\big)$,

139. $\big(t(1-t), (1-t)^2, t^3, (1-t)^3\big)$,

140. $\big(t(1-t), t^3, t^2(1-t), (1-t)^3\big)$,

141. $\big(t(1-t), t^3, t(1-t)^2, (1-t)^3\big)$,

142. $\big((1-t)^2, t^3, t^2(1-t), t(1-t)^2\big)$,

143. $\big((1-t)^2, t^3, t^2(1-t), (1-t)^3\big)$,

144. $\big(t^3, t^2(1-t), t(1-t)^2, (1-t)^3\big)$.

And for $p \geq 5$ the following 25 quadruples (X_0, Y_0, Z_0, W_0) are added.

1. $\big(1, t, t^3, t^2(1-t)\big)$,

2. $\big(1, t, t^3, t(1-t)^2\big)$,

3. $\big(1, t, t^3, (1-t)^3\big)$,

4. $\big(1, 1-t, t^3, t^2(1-t)\big)$,

5. $\big(1, 1-t, t^3, t(1-t)^2\big)$,

6. $\big(1, 1-t, t^3, (1-t)^3\big)$,

7. $\big(1, t^2, t^3, t^2(1-t)\big)$,

8. $\big(1, t^2, t^3, t(1-t)^2\big)$,

9. $\big(1, t^2, t^3, (1-t)^3\big)$,

10. $\big(1, t^2, t^2(1-t), t(1-t)^2\big)$,

11. $\big(1, t^2, t^2(1-t), (1-t)^3\big)$,

12. $\big(1, t(1-t), t^3, t^2(1-t)\big)$,

13. $\big(1, t(1-t), t^3, t(1-t)^2\big)$,

14. $\big(1, t(1-t), t^3, (1-t)^3\big)$,

15. $\big(1, (1-t)^2, t^3, t^2(1-t)\big)$,

16. $\big(1, (1-t)^2, t^3, t(1-t)^2\big)$,

17. $\big(1,(1-t)^2,t^3,(1-t)^3\big)$,

18. $\big(1,(1-t)^2,t(1-t)^2,(1-t)^3\big)$,

19. $\big(1,t^3,t^2(1-t),t(1-t)^2\big)$,

20. $\big(1,t^3,t^2(1-t),(1-t)^3\big)$,

21. $\big(1,t^3,t(1-t)^2,(1-t)^3\big)$,

22. $\big(t,1-t,t^3,t^2(1-t)\big)$,

23. $\big(t,1-t,t^3,t(1-t)^2\big)$,

24. $\big(t,1-t,t^3,(1-t)^3\big)$,

25. $\big((1-t)^2,t^3,t(1-t)^2,(1-t)^3\big)$.

For each of these we equate coefficients in (6.8) to obtain a system of four homogeneous linear equations in a_0,b_0,c_0,d_0. We calculate the determinant in $\mathbb{Z}$, and we reject those with determinant non-zero mod p (again if $p\geq 5$ this turns out to be equivalent to being non-zero in $\mathbb{Z}$).
Among the remaining systems we find in 16 cases a generator (a_0,b_0,c_0,d_0) in $\mathbb{Z}^4$ for $p=3$, namely

(X_0,Y_0,Z_0,W_0)	(a_0,b_0,c_0,d_0)
$\big(1,t,t^2,t(1-t)\big)$	$(0,-1,1,1)$
$\big(1,t,t^2,(1-t)^2\big)$	$(-1,2,-1,1)$
$\big(1,t,t(1-t),(1-t)^2\big)$	$(-1,1,1,1)$
$\big(1,1-t,t^2,t(1-t)\big)$	$(-1,1,1,1)$
$\big(1,1-t,t^2,(1-t)^2\big)$	$(1,-2,-1,1)$
$\big(1,1-t,t(1-t),(1-t)^2\big)$	$(0,-1,1,1)$
$\big(1,t^2,t(1-t),(1-t)^2\big)$	$(-1,1,2,1)$
$\big(1,t(1-t),t^2(1-t),t(1-t)^2\big)$	$(0,-1,1,1)$
$\big(t,1-t,t^2,t(1-t)\big)$	$(-1,0,1,1)$
$\big(t,1-t,t^2,(1-t)^2\big)$	$(1,-1,-1,1)$
$\big(t,1-t,t(1-t),(1-t)^2\big)$	$(0,-1,1,1)$
$\big(t,(1-t)^2,t(1-t)^2,(1-t)^3\big)$	$(0,-1,1,1)$
$\big(1-t,t^2,t(1-t),(1-t)^2\big)$	$(-1,0,1,1)$
$\big(1-t,t^2,t^3,t^2(1-t)\big)$	$(0,-1,1,1)$
$\big(t^2,(1-t)^2,t^3,t^2(1-t)\big)$	$(-1,0,1,1)$
$\big(t^2,(1-t)^2,t(1-t)^2,(1-t)^3\big)$	$(0,-1,1,1)$

For $p\geq 5$ the following four additional cases with a generator (a_0,b_0,c_0,d_0) in $\mathbb{Z}^4$ arise.

(X_0, Y_0, Z_0, W_0)	(a_0, b_0, c_0, d_0)
$\big(1, t^2, t^3, t^2(1-t)\big)$	$(0, -1, 1, 1)$
$\big(1, t(1-t), t^3, (1-t)^3\big)$	$(-1, 3, 1, 1)$
$\big(1, (1-t)^2, t(1-t)^2, (1-t)^3\big)$	$(0, -1, 1, 1)$
$\big((1-t)^2, t^3, t(1-t)^2, (1-t)^3\big)$	$(-1, 0, 1, 1)$

After rejecting those with $a_0b_0c_0d_0$ zero mod p (again automatic if $p \geq 5$) there remain the following quadruples (X_0, Y_0, Z_0, W_0) and (a_0, b_0, c_0, d_0) for $p \geq 5$.

(X_0, Y_0, Z_0, W_0)	(a_0, b_0, c_0, d_0)
$\big(1, t, t^2, (1-t)^2\big)$	$(-1, 2, -1, 1)$
$\big(1, t, t(1-t), (1-t)^2\big)$	$(-1, 1, 1, 1)$
$\big(1, 1-t, t^2, t(1-t)\big)$	$(-1, 1, 1, 1)$
$\big(1, 1-t, t^2, (1-t)^2\big)$	$(1, -2, -1, 1)$
$\big(1, t^2, t(1-t), (1-t)^2\big)$	$(-1, 1, 2, 1)$
$\big(1, t(1-t), t^3, (1-t)^3\big)$	$(-1, 3, 1, 1)$
$\big(t, 1-t, t^2, (1-t)^2\big)$	$(1, -1, -1, 1)$

These lead in this order to the points $\Pi_2^*, \Pi_3, \Pi_8, \Pi_3^*, \Pi_1^*, \Pi_0^*$ and Π_2 respectively.

For $p = 3$ we obtain the same list, while however

$$(X_0, Y_0, Z_0, W_0) \;=\; \big(1, t(1-t), t^3, (1-t)^3\big)\,, \qquad (a_0, b_0, c_0, d_0) \;=\; (-1, 3, 1, 1)$$

is missing because here $a_0b_0c_0d_0 = 0$.

C Intersection of curves in $x+y-z=1$ with tori

When one intersects an algebraic variety V in affine space $\mathbb{A}^n$ (or equivalently the multiplicative group $\mathbb{G}_m^n$) with a set of the form G^n, where G is a finitely generated multiplicative group, one is in the situation associated with the names Mordell-Lang. This terminology is also sometimes applied when intersecting V with $(\sqrt{G})^n$, where $\sqrt{G}$ is rather the radical or division group inside some large field of some finitely generated G. The special case when G is the trivial group is sometimes associated with the names Manin-Mumford, and amounts to the study of points on V whose coordinates are roots of unity (or in a broader context torsion points in some ambient semiabelian variety).

In zero characteristic these intersections are comparatively well-understood, and are usually studied with the aid of the Subspace Theorem or generalizations of it. This often results in lack of effectivity, especially if the dimension of V is at least two.

In positive characteristic our knowledge is not so precise. Indeed the main results for zero characteristic are usually no longer valid without some sort of extra assumptions, and the proofs often involve tools from logic such as Model Theory. This can also result in lack of effectivity.

Contrary to this we would like to remind of the work of Derksen and Masser [DM] in 2012. There they gave an alternative approach to Mordell-Lang in positive characteristic, at least for linear varieties V, which does lead to effective results. We stated their main Theorem in the introduction above and gave some examples for it in the main part of the present work.

Now since the fundamental papers of Zilber [Zi] and Pink [P] it is recognised that problems of Mordell-Lang type and Manin-Mumford type can be put in a wider context sometimes known as that of Unlikely Intersections (see for example the recent book [Za] of Zannier). Here we should mention the sets $V \cap G^3$ and even $V \cap (\sqrt{G})^3$ from our Theorems 2 (G) and 2 ($\sqrt{G}$) respectively when V is the plane in $\mathbb{A}^3$ defined by $x+y-z=1$. These can be examined in this context by somewhat artificially embedding V in $\mathbb{A}^5$ by means of two extra variables u, v, which take constant values $u=t, v=1-t$. Then between the values of the five variables x, y, z, u, v there are at least three independent multiplicative relations. The same trick can be performed when G is replaced by any G' with two generators, and for more generators we just have to increase the embedding dimension.

Now in zero characteristic the problems for surfaces in $\mathbb{A}^5$ have not been completely solved. So we will not attempt to investigate $V \cap (\sqrt{G'})^3$ by these methods. In fact in this Appendix C we will restrict ourselves to curves.

In zero characteristic the main conjecture for curves even in $\mathbb{A}^n$ has been proved essentially by Maurin [Mau] (see also Bombieri-Habegger-Masser-Zannier [BHMZ]). His result, when combined with the main result of Bombieri, Masser and Zannier [BMZ], gives the following.

Let $\mathcal{K}$ be an algebraically closed field of zero characteristic and let $\mathcal{C}$ in $\mathbb{G}_m^n$ be an absolutely irreducible curve defined over $\mathcal{K}$. Assume that for any non-zero $(r_1, \ldots, r_n)$ in $\mathbb{Z}^n$ the monomial

$$x_1^{r_1} \cdots x_n^{r_n}$$

in the function field $\mathcal{K}(\mathcal{C})$ is not 1. Then there are at most finitely many points $(\xi_1, \ldots, \xi_n)$ in $\mathcal{C}(\mathcal{K})$ for which there exist linearly independent $(a_1, \ldots, a_n)$,

$(b_1,\ldots,b_n)$ in $\mathbb{Z}^n$ with

$$\xi_1^{a_1}\cdots\xi_n^{a_n} \;=\; \xi_1^{b_1}\cdots\xi_n^{b_n} \;=\; 1.$$

However all this work on Unlikely Intersections is in zero characteristic, and as might be guessed the conjectures for zero characteristic are no longer valid in positive characteristic. Indeed for $n=2$ the conditions on $\xi_1,\ldots,\xi_n$ are equivalent to them being roots of unity, and already the set $L(\overline{\mathbb{F}_p}^*)$ in Theorem 1 ($\sqrt{G}$) for the curve $x+y=1$ gives a simple counterexample.

Masser [Mas1] has made a start on formulating some conjectures for general V in $\mathbb{G}_m^n$. Here is the version for curves, in which the non-constant condition on a single monomial is replaced by a new algebraic independence condition on a pair of monomials.

Conjecture. *Let $\mathcal{K}$ be an algebraically closed field of positive characteristic p and let $\mathcal{C}$ in $\mathbb{G}_m^n$ be an absolutely irreducible curve defined over $\mathcal{K}$. Assume that for any linearly independent $(r_1,\ldots,r_n)$, $(s_1,\ldots,s_n)$ in $\mathbb{Z}^n$ the monomials*

$$x_1^{r_1}\cdots x_n^{r_n}, \quad x_1^{s_1}\cdots x_n^{s_n}$$

in the function field $\mathcal{K}(\mathcal{C})$ are algebraically independent over $\overline{\mathbb{F}_p}$. Then there are at most finitely many points $(\xi_1,\ldots,\xi_n)$ in $\mathcal{C}(\mathcal{K})$ for which there exist linearly independent $(a_1,\ldots,a_n)$, $(b_1,\ldots,b_n)$ in $\mathbb{Z}^n$ with

$$\xi_1^{a_1}\cdots\xi_n^{a_n} \;=\; \xi_1^{b_1}\cdots\xi_n^{b_n} \;=\; 1.$$

Masser has shown the necessity of the new condition (which of course breaks down for $x+y=1$), and given evidence for its sufficiency by proving the conjecture for $n=2$ and $n=3$.

The main object of this Appendix C is again to work out some examples when $\mathcal{K}$ is the algebraic closure $K=\overline{\mathbb{F}_p(t)}$ of $\mathbb{F}_p(t)$ and $n=3$. This time we do not take a specific curve $\mathcal{C}$, but we do make the assumption that $\mathcal{C}$ in $\mathbb{G}_m^3$ is contained in a plane defined over $\overline{\mathbb{F}_p}$. This is not quite as restrictive as it looks. For example we can regard a curve over $\overline{\mathbb{F}_p}(t)$ as a surface over $\overline{\mathbb{F}_p}$ and so there is certainly some non-trivial equation $f(x,y,z)=0$ over $\overline{\mathbb{F}_p}$. We are essentially assuming that f has degree 1 so this surface is a plane. If this plane has a zero coefficient then Masser's condition is not satisfied, so we shall assume that all the coefficients are non-zero. Then after a simple change of coordinates it can be assumed to be our old friend $x+y-z=1$. In that case it turns out that Masser's new condition can be slightly weakened, and then we will obtain some quite strong explicit bounds for the cardinality of the finite set in the above conjecture. They involve the degree $\deg\mathcal{C}$ of $\mathcal{C}$. It is not so easy to find a treatment in the literature of this concept of degree in affine space. In two dimensions it is simply the degree of the unique irreducible defining equation. Already in three dimensions the defining equations are not unique. But in our situation with $\mathcal{C}$ contained in the plane $x+y-z=1$ we can project to the (x,y)-plane; we get a curve $\mathcal{C}'$ there, and as it can be shown that $\deg\mathcal{C}=\deg\mathcal{C}'$ it suffices here simply to define the former as the latter.

Here is our main result, which may remind one of Theorems 1 and 2 of Voloch's paper [Vol2].

Theorem 3. *Let $\mathcal{C}$ be an absolutely irreducible curve in $\mathbb{G}_m^3$ defined over K and lying in the plane P defined by $x+y-z=1$. Assume that x,y in the function field $K(\mathcal{C})$ are algebraically independent over $\overline{\mathbb{F}_p}$. Then there are at most*

$$(\deg \mathcal{C})^2 + 2p^2 \deg \mathcal{C}$$

points (ξ,η,ζ) in $\mathcal{C}(K)$ for which there exist linearly independent (a_1,b_1,c_1), (a_2,b_2,c_2) in $\mathbb{Z}^3$ with

$$\xi^{a_1}\eta^{b_1}\zeta^{c_1} \ = \ \xi^{a_2}\eta^{b_2}\zeta^{c_2} \ = \ 1. \tag{C.1}$$

This result becomes false when we consider a general plane P defined over $\overline{\mathbb{F}_p}$. For a counterexample take the plane $x+y=z$ and the curve defined by $y=t$ in this plane. Thus the curve is parametrized by $(x,t,x+t)$ where the first and the second coordinate are algebraically independent over $\overline{\mathbb{F}_p}$. But when we take $x=\alpha t$ for any α in $\overline{\mathbb{F}_p}$ we see the point $(x,y,z)=(\alpha t,t,(\alpha+1)t)$ and there are of course two relations

$$\left(\frac{x}{z}\right)^{a_1} = \left(\frac{y}{z}\right)^{b_2} = 1 \tag{C.2}$$

for suitable a_1 and b_2 in $\mathbb{N}$, while $(a_1,0,-a_1)$ and $(0,b_2,-b_2)$ are linearly independent in $\mathbb{Z}^3$.

We prove Theorem 3 in section C.2 and also verify the necessity of the algebraic independence condition.

Of course we would prefer to know the finite set itself in Theorem 3 instead of estimates for its cardinality. It is a familiar feature of these problems in zero characteristic that this is usually impossible. But we already showed in this work that in positive characteristic it is possible, at least in the Mordell-Lang and Manin-Mumford situation. This carries over to Unlikely Intersections, and to illustrate this we give the following example. It treats (in disguise) the line $\mathcal{C}$ parametrized by x in

$$(x,y,z)=(x,x-t,2x-t-1),$$

lying in the plane P defined by $x+y-z=1$.

Theorem 4. *Let $x\neq 0, x-t\neq 0, 2x-t-1\neq 0$ be in K such that*

$$x^{a_1}(x-t)^{b_1}(2x-t-1)^{c_1} \ = \ x^{a_2}(x-t)^{b_2}(2x-t-1)^{c_2} \ = \ 1$$

for linearly independent (a_1,b_1,c_1), (a_2,b_2,c_2) in $\mathbb{Z}^3$. Then $x=1, t+1$ and in addition $x=\frac{1}{2}t$ provided $p\geq 3$.

As there is hardly any dependence on p here this result suggests that the dependence on p in Theorem 3 might be improved.

C.1 Preliminaries

We start with an effective version of the above Conjecture for $n=2$ which essentially involves roots of unity. It is also reminiscent of [Vol2].

Proposition 5. *Let $\mathcal{K}$ be an algebraically closed field of characteristic p and let $\mathcal{C}$ be an absolutely irreducible curve in $\mathbb{G}_m^2$ defined over $\mathcal{K}$. Assume that the variables x, y in the function field $\mathcal{K}(\mathcal{C})$ are algebraically independent over $\overline{\mathbb{F}_p}$. Then there are at most $(\deg \mathcal{C})^2$ points (ξ, η) in $\mathcal{C}(\mathcal{K})$ for which there exist linearly independent (a_1, b_1), (a_2, b_2) in $\mathbb{Z}^2$ with*

$$\xi^{a_1}\eta^{b_1} \ = \ \xi^{a_2}\eta^{b_2} \ = \ 1. \tag{C.3}$$

Proof. At first let (a_1, b_1), (a_2, b_2) in $\mathbb{Z}^2$ be linearly independent and let $\pi = (\xi, \eta)$ on $\mathcal{C}$ satisfy (C.3). We then claim that ξ, η are roots of unity. To see this we first eliminate η from $(C.3)$ to get

$$\xi^{a_1 b_2 - b_1 a_2} \ = \ 1$$

with $a_1 b_2 - b_1 a_2 \neq 0$ because (a_1, b_1) and (a_2, b_2) are linearly independent; and this means that ξ is a root of unity. The same argument works for η and hence ξ, η are in $\overline{\mathbb{F}_p}^*$ as claimed.

We may describe $\mathcal{C}$ by an equation $f(x, y) = 0$ where $f \neq 0$ is in $\mathcal{K}[x, y]$. More precisely we have $d = \deg \mathcal{C}$ in $\mathbb{N}$ and

$$f(x, y) \ = \ \sum_{\substack{i,j \geq 0 \\ i+j \leq d}} f_{ij} x^i y^j$$

for f_{ij} in $\mathcal{K}$. Next let $\pi_1 = (\xi_1, \eta_1), \ldots, \pi_l = (\xi_l, \eta_l)$ in $\overline{\mathbb{F}_p}^2$ be l points on $\mathcal{C}$ as above. Consider the $l \times m$ matrix

$$\begin{pmatrix} 1 & \xi_1 & \eta_1 & \xi_1^2 & \xi_1\eta_1 & \eta_1^2 & \cdots & \xi_1^d & \cdots & \eta_1^d \\ 1 & \xi_2 & \eta_2 & \xi_2^2 & \xi_2\eta_2 & \eta_2^2 & \cdots & \xi_2^d & \cdots & \eta_2^d \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 1 & \xi_l & \eta_l & \xi_l^2 & \xi_l\eta_l & \eta_l^2 & \cdots & \xi_l^d & \cdots & \eta_l^d \end{pmatrix}$$

with $m = \frac{1}{2}(d+1)(d+2)$. If the rank of this matrix is m then our equations $f(\pi_i) = 0$ $(i = 1, \ldots, l)$ would imply $f = 0$ which is not the case. So the rank is strictly less than m. This means that we can find $f_0 \neq 0$ in $\overline{\mathbb{F}_p}[x, y]$ of total degree at most d such that $f_0(\pi_i) = 0$ $(i = 1, \ldots, l)$. Let $\mathcal{C}_0$ in $\mathbb{G}_m^2$ be the curve defined by $f_0(x, y) = 0$.

Suppose that $l > d^2 \geq \deg f \deg f_0$. We then deduce from the well known theorem of Bézout (see for example Walker [W] p.59) that $\mathcal{C} \cap \mathcal{C}_0$ is again a curve in $\mathbb{G}_m^2$. But $\mathcal{C}$ is assumed to be an absolutely irreducible curve and hence $\mathcal{C}$ is a component of $\mathcal{C}_0$. In particular it follows that $\mathcal{C}$ is defined over $\overline{\mathbb{F}_p}$, which means that the variables x and y are algebraically dependent over $\overline{\mathbb{F}_p}$ in contradiction to the assumption in the proposition. Therefore $l \leq (\deg \mathcal{C})^2$ and this completes the proof. □

We can check the necessity of the independence condition in Proposition 5 as follows. Indeed if now x, y are not algebraically independent over $\overline{\mathbb{F}_p}$ then we can take f over $\overline{\mathbb{F}_p}$. We can assume that f involves y. Now the polynomial $f(x, 0)$ is not identically zero otherwise y would vanish identically on $\mathcal{C}$. We can therefore find infinitely many ξ in $\overline{\mathbb{F}_p}^*$ with $f(\xi, 0) \neq 0$. We can further ensure that $f(\xi, y)$ involves y for infinitely many ξ. Pick one of these ξ. If every η in $\overline{\mathbb{F}_p}$

with $f(\xi, \eta) = 0$ (if any) satisfies also $\eta = 0$ then by the Nullstellensatz $f(\xi, y)$ would divide some power of y in $\overline{\mathbb{F}_p}[y]$. Thus $f(\xi, y) = \gamma y^b$ for some γ in $\overline{\mathbb{F}_p}^*$ and some non-negative integer b (possibly depending on ξ).

However y does not divide $f(\xi, y)$ as $f(\xi, 0) \neq 0$. Therefore $f(\xi, y) = \gamma$, contradicting one of the conditions above on ξ.

Thus for infinitely many ξ in $\overline{\mathbb{F}_p}^*$ we can find η in $\overline{\mathbb{F}_p}$ with $\eta \neq 0$. Now we have infinitely many points (ξ, η) in $\mathcal{C}(K)$ with independent relations $\xi^{a_1} = \eta^{b_2} = 1$ for suitable non-zero integers a_1, b_2.

In other words, if $\mathcal{C}$ is defined over $\overline{\mathbb{F}_p}$ then $\mathcal{C}(\overline{\mathbb{F}_p}^*)$ is infinite.

To give an extremal example for Proposition 5 let A, B be two sets each with d elements in $\overline{\mathbb{F}_p}^*$, and pick t transcendental over $\mathbb{F}_p$. Then

$$\prod_{\alpha \in A} (x - \alpha) = t \prod_{\beta \in B} (y - \beta)$$

defines a curve $\mathcal{C}$ not over $\overline{\mathbb{F}_p}$ with degree d and exactly d^2 torsion points (α, β) $(\alpha \in A, \beta \in B)$. We show that $\mathcal{C}$ is irreducible by means of a trick which actually uses Proposition 5. Suppose that $\mathcal{C}$ splits into irreducible components $\mathcal{C}_1 \cup \cdots \cup \mathcal{C}_r$. Then none of these could be defined over $\overline{\mathbb{F}_p}$ otherwise if for example $\mathcal{C}_1$ was defined over $\overline{\mathbb{F}_p}$ then $\mathcal{C}_1(\overline{\mathbb{F}_p}^*)$ and so $\mathcal{C}(\overline{\mathbb{F}_p}^*)$ would be infinite from the remark above. Thus by Proposition 5 applied to the components, say of degrees $d_1, \ldots, d_r$ respectively, we would see that $|\mathcal{C}(\overline{\mathbb{F}_p}^*)| \leq d_1^2 + \cdots + d_r^2$. However $|\mathcal{C}(\overline{\mathbb{F}_p}^*)| = d^2 = (d_1 + \cdots + d_r)^2$; and this forces $r = 1$. Hence indeed $\mathcal{C}$ is irreducible, and thus we see that Proposition 5 is the best possible result.

The next result, over $K = \overline{\mathbb{F}_p(t)}$, is the main ingredient for the proof of Theorem 3. But we specifically exclude torsion points. This enables us to get by with a hypothesis of linear rather than algebraic independence.

Proposition 6. *Let $\mathcal{C}$ be an absolutely irreducible curve in $\mathbb{G}_m^3$ defined over K lying in a plane P defined over $\overline{\mathbb{F}_p}$. Assume that any three of $1, x, y, z$ in the function field $K(\mathcal{C})$ are linearly independent over $\overline{\mathbb{F}_p}$. Then there are at most $(p^2 + p + 1) \deg \mathcal{C}$ points $\pi = (\xi, \eta, \zeta)$ in $\mathcal{C}(K)$, $\pi \notin (\overline{\mathbb{F}_p}^*)^3$, for which there exist linearly independent (a_1, b_1, c_1), (a_2, b_2, c_2) in $\mathbb{Z}^3$ with (C.1).*

Before we prove Proposition 6 we state the following lemma.

Lemma 21. *Let $\pi = (\xi, \eta, \zeta)$ in K^3 satisfy (C.1) with linearly independent (a_1, b_1, c_1), (a_2, b_2, c_2) in $\mathbb{Z}^3$.*

1. *Then we always find another linearly independent pair (a_1, b_1, c_1), (a_2, b_2, c_2) in $\mathbb{Z}^3$ such that (C.1) still holds and not all the minors*

$$\rho = b_1 c_2 - c_1 b_2, \quad \sigma = c_1 a_2 - a_1 c_2, \quad \tau = a_1 b_2 - b_1 a_2$$

are divisible by p.

2. *If further π is not in $\overline{\mathbb{F}_p}^3$ and satisfies $\xi + \eta - \zeta = 1$ then also $\rho\xi + \sigma\eta - \tau\zeta = 0$ holds, i.e. π lies on $P \cap P'$ where P and P' are planes given by*

$$P : x + y - z \ = \ 1, \quad P' : \rho x + \sigma y - \tau z \ = \ 0. \tag{C.4}$$

Proof. Certainly, by Frobenius we may assume that not all of a_1, b_1, c_1 are divisible by p. Similarly for a_2, b_2, c_2.

Next, we show how to make sure that not all the minors are divisible by p. Let $\Lambda = \mathbb{Z}(a_1, b_1, c_1) + \mathbb{Z}(a_2, b_2, c_2)$ in $\mathbb{Z}^3$ be the corresponding two-dimensional lattice. Its determinant $\Delta(\Lambda)$ is given by $\rho^2 + \sigma^2 + \tau^2$. Further by elementary divisor theory there are a basis $(\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \boldsymbol{\lambda}_3)$ of $\mathbb{Z}^3$ and positive integers d_1, d_2, such that $(d_1\boldsymbol{\lambda}_1, d_2\boldsymbol{\lambda}_2)$ is a basis of Λ. For $\Lambda_0 = \mathbb{Z}\boldsymbol{\lambda}_1 + \mathbb{Z}\boldsymbol{\lambda}_2$ we can write

$$[\Lambda_0 : \Lambda] \; = \; d_1 d_2 \; = \; p^r s$$

with integers $r, s \geq 0$ and p not dividing s. However, writing $d_i = p^{r_i} s_i$ $(i = 1, 2)$ in integers $r_i \geq 0$ and s_i not divisible by p we get a group

$$\Lambda' \; = \; \mathbb{Z}s_1\boldsymbol{\lambda}_1 + \mathbb{Z}s_2\boldsymbol{\lambda}_2$$

in between Λ_0 and Λ with $[\Lambda_0 : \Lambda'] = s_1 s_2 = s$ and $[\Lambda' : \Lambda] = p^{r_1+r_2} = p^r$. We further have $\Delta(\Lambda') = s^2 = \rho'^2 + \sigma'^2 + \tau'^2$ with ρ', σ', τ' the minors of the matrix formed by $s_1\boldsymbol{\lambda}_1, s_2\boldsymbol{\lambda}_2$. Thus ρ', σ', τ' are not all divisible by p and these are the new ρ, σ, τ.

Further for any $\boldsymbol{\lambda}' = (\lambda_1', \lambda_2', \lambda_3')$ in Λ' we see that $p^r\boldsymbol{\lambda}'$ lies in Λ and so from (C.1) we have

$$\xi^{p^r\lambda_1'}\eta^{p^r\lambda_2'}\zeta^{p^r\lambda_3'} = 1.$$

Hence $\xi^{\lambda_1'}\eta^{\lambda_2'}\zeta^{\lambda_3'} = 1$ for all $(\lambda_1', \lambda_2', \lambda_3')$ in Λ'. So the effect is simply to increase the Λ implicit in (C.1) to Λ'. This completes the first part of the proof with the new $(a_1, b_1, c_1), (a_2, b_2, c_2)$ as $s_1\boldsymbol{\lambda}_1, s_2\boldsymbol{\lambda}_2$.

Turning to the second part, we mention that due to our assumption that π is not in $\overline{\mathbb{F}_p}^3$ Lemma 6 enables us to choose $q = p^e$ $(e \in \mathbb{Z})$ minimal such that $\xi_q = \xi^q$, $\eta_q = \eta^q$, $\zeta_q = \zeta^q$ all lie in the maximal separable algebraic extension S of $\mathbb{F}_p(t)$. We then have

$$\xi_q^{a_1}\eta_q^{b_1}\zeta_q^{c_1} \; = \; \xi_q^{a_2}\eta_q^{b_2}\zeta_q^{c_2} \; = \; 1$$

and we can differentiate logarithmically with respect to t to get

$$0 \; = \; a_1\frac{\dot{\xi}_q}{\xi_q} + b_1\frac{\dot{\eta}_q}{\eta_q} + c_1\frac{\dot{\zeta}_q}{\zeta_q} \; = \; a_2\frac{\dot{\xi}_q}{\xi_q} + b_2\frac{\dot{\eta}_q}{\eta_q} + c_2\frac{\dot{\zeta}_q}{\zeta_q}. \qquad \text{(C.5)}$$

Further from $\xi + \eta - \zeta = 1$ we see by Frobenius that $\xi_q + \eta_q - \zeta_q = 1$ and by differentiating with respect to t we get $\dot{\zeta}_q = \dot{\xi}_q + \dot{\eta}_q$. Together with (C.5) this implies

$$0 \; = \; \left(\frac{a_1}{\xi_q} - \frac{c_1}{\zeta_q}\right)\dot{\xi}_q + \left(\frac{b_1}{\eta_q} - \frac{c_1}{\zeta_q}\right)\dot{\eta}_q$$
$$0 \; = \; \left(\frac{a_2}{\xi_q} - \frac{c_2}{\zeta_q}\right)\dot{\xi}_q + \left(\frac{b_2}{\eta_q} - \frac{c_2}{\zeta_q}\right)\dot{\eta}_q$$

a linear system in $\dot{\xi}_q, \dot{\eta}_q$ with determinant say Δ.

Now $\dot{\xi}_q, \dot{\eta}_q$ cannot both be zero; otherwise ξ_q, η_q and so ζ_q would all three be in the field of constants C of S, which by Lemma 3 is S^p. But then $\xi^{q/p}$,

$\eta^{q/p}$, $\zeta^{q/p}$ would all be in S, contradicting the minimality of q. Thus

$$\begin{aligned} 0 \;=\; \Delta \;=\; & \left(\frac{a_1}{\xi_q} - \frac{c_1}{\zeta_q}\right)\left(\frac{b_2}{\eta_q} - \frac{c_2}{\zeta_q}\right) - \left(\frac{b_1}{\eta_q} - \frac{c_1}{\zeta_q}\right)\left(\frac{a_2}{\xi_q} - \frac{c_2}{\zeta_q}\right) \\ =\; & \frac{b_1c_2 - c_1b_2}{\zeta_q\eta_q} + \frac{c_1a_2 - a_1c_2}{\xi_q\zeta_q} + \frac{a_1b_2 - b_1a_2}{\xi_q\eta_q} \end{aligned}$$

and this emerges as $\rho\xi_q + \sigma\eta_q - \tau\zeta_q = 0$. Then reversing Frobenius yields the requested relation. Indeed, the equation $\rho x + \sigma y - \tau z = 0$ stands for a plane P' because ρ, σ, τ are not all divisible by p (and hence are not all zero in $\overline{\mathbb{F}_p}$); this completes the proof of the lemma. □

Proof of Proposition 6. It is clear that P cannot go through the origin, because otherwise its equation would force x, y, z to be linearly dependent over $\overline{\mathbb{F}_p}$. Thus P is given by an equation

$$\alpha x + \beta y + \gamma z \;=\; 1 \quad (\alpha, \beta, \gamma \in \overline{\mathbb{F}_p}).$$

We then would deduce from $\gamma = 0$ that $1, x, y$ are linearly dependent over $\overline{\mathbb{F}_p}$. Similarly if $\alpha = 0$ or $\beta = 0$; and therefore α, β, γ are all non-zero. After a possible transformation of coordinates however (which does not affect the hypotheses or conclusions of the proposition) we may assume that P is given by $x + y - z = 1$.

Let now π in $\mathcal{C}(K)$ satisfy (C.1). We then deduce from Lemma 21 that π lies on $P \cap P'$ with (C.4). Write $\mathcal{C} \cap P'$ as a union $X_1 \cup \cdots \cup X_r$ of algebraic sets. Suppose the dimension of $X_1 \cup \cdots \cup X_r$ is 1. This means that X_i is a curve for some $i \in \{1, \ldots, r\}$. But then $X_i \subset \mathcal{C}$ implies $X_i = \mathcal{C}$ because the curve $\mathcal{C}$ is assumed to be absolutely irreducible. Therefore $\mathcal{C}$ lies in the plane P' through the origin implying that the variables x, y, z are linearly dependent over $\overline{\mathbb{F}_p}$; but this is excluded by assumption. Therefore the dimension of $\mathcal{C} \cap P'$ is zero. We could further deduce from Bézout's theorem that the intersection of our curve $\mathcal{C}$ and the line $P' \cap P$ contains at most $\deg \mathcal{C}$ points π; but actually in our situation we can again reduce to the two-dimensional situation with $f(x, y) = 0$ and $(\tau - \rho)x + (\tau - \sigma)y = \tau$.

But where does the factor $p^2 + p + 1$ in the proposition come from? Going back to the equation $\rho x + \sigma y - \tau z = 0$ for P' in (C.4) we mention that there are $p^3 - 1$ possibilities to choose ρ, σ, τ because not all of them can be zero in $\mathbb{F}_p$ at the same time. Thus we have to consider several planes depending on the choice of ρ, σ, τ. Here two such equations define the same plane if and only if one of them can be obtained from the other by multiplication with an element in $\mathbb{F}_p^*$. This means that we have $|\mathbb{P}_2(\mathbb{F}_p)| = (p^3 - 1)/(p - 1) = p^2 + p + 1$ different planes and this completes the proof. □

The condition that any three of $1, x, y, z$ in the function field $K(\mathcal{C})$ are linearly independent over $\overline{\mathbb{F}_p}$ is indeed crucial for the validity of Proposition 6 as the following examples show.

Going back to the counterexample, which we gave right after Theorem 3 we mention that the coordinates x, y, z there are linearly dependent over $\overline{\mathbb{F}_p}$. Further, for any $\alpha \neq -1$ in $\overline{\mathbb{F}_p}^*$ the point $\pi = (\alpha t, t, (\alpha + 1)t)$ is not in $(\overline{\mathbb{F}_p}^*)^3$ and satisfies the relations (C.2) for suitable a_1, b_2 in $\mathbb{N}$.

Next we give a counterexample when it is $1, x, y$ that are linearly dependent over $\overline{\mathbb{F}_p}$. Consider the plane $y = x + 1$ over $\overline{\mathbb{F}_p}$ and take the curve defined by $z = t$ in this plane. Thus the curve is parametrized by $(x, x + 1, t)$ and certainly contains no points in $(\overline{\mathbb{F}_p}^*)^3$. Then for any $\alpha \neq -1$ in $\overline{\mathbb{F}_p}^*$ and the point $\pi = (\alpha, \alpha + 1, t)$ we find the independent relations $\alpha^{a_1} = (\alpha + 1)^{b_2} = 1$ for suitable a_1, b_2 in $\mathbb{N}$.

On grounds of symmetry we find similar counterexamples with $1, x, z$ and $1, y, z$ linearly dependent over $\overline{\mathbb{F}_p}$.

We were not able however to find extremal examples which show that the dependence on either p or $\deg \mathcal{C}$ is necessary.

C.2 Proof of Theorems 3 and 4

We start with Theorem 3.

Proof of Theorem 3. We first mention that because x, y in $K(\mathcal{C})$ are algebraically independent over $\overline{\mathbb{F}_p}$ then so are any two of the variables x, y, z. This is of course due to the relation $x + y - z = 1$.

Let π on $\mathcal{C}(K)$ be a point not in $(\overline{\mathbb{F}_p}^*)^3$. Suppose now that x, y, z are linearly dependent over $\overline{\mathbb{F}_p}$. Then substituting $z = x + y - 1$ into this dependence relation would imply the forbidden algebraic dependence of x and y over $\overline{\mathbb{F}_p}$. And furthermore any linear dependence relation between 1 and any two of x, y, z is an algebraic dependence relation over $\overline{\mathbb{F}_p}$ between these two variables. Thus we may apply Proposition 6 giving rise to at most

$$(p^2 + p + 1) \deg \mathcal{C} \leq 2p^2 \deg \mathcal{C}$$

points π.

Now to the points π in $(\overline{\mathbb{F}_p}^*)^3$. As $x + y - z = 1$ on the curve $\mathcal{C}$ it is clear that the projection down to $\mathbb{G}_m^2$ with coordinates x, y is also a curve $\mathcal{C}'$, defined say by an absolutely irreducible polynomial f in $K[x, y]$. In fact $\mathcal{C}$ is then defined by the pair of equations

$$x + y - z = 1, \quad f(x, y) = 0 \tag{C.6}$$

and as discussed above we have $\deg \mathcal{C} = \deg \mathcal{C}'$.

Furthermore x, y in $K(\mathcal{C}')$ remain algebraically independent over $\overline{\mathbb{F}_p}$. Hence all the conditions in Proposition 5 are satisfied and so we get at most $(\deg \mathcal{C}')^2$ points (ξ, η) in $\mathcal{C}'(\overline{\mathbb{F}_p})$. But as we see from (C.6) there is a one-to-one correspondence between the two sets $\mathcal{C}'(\overline{\mathbb{F}_p})$ and $\mathcal{C}(\overline{\mathbb{F}_p})$. This completes the proof. □

Now we check the necessity of the algebraic independence condition in Theorem 3, rather as we did for Proposition 5.

Indeed if now x, y are not algebraically independent over $\overline{\mathbb{F}_p}$ then (C.6) continues to hold and now we can take f over $\overline{\mathbb{F}_p}$. We can assume that f involves y. Now the polynomials $f(x, 0)$ and $f(x, 1 - x)$ are not identically zero otherwise y or $x + y - 1 = z$ would vanish identically on $\mathcal{C}$. We can therefore find infinitely many ξ in $\overline{\mathbb{F}_p}^*$ with $f(\xi, 0)f(\xi, 1 - \xi) \neq 0$. We can further ensure that $f(\xi, y)$ involves y for infinitely many ξ. Pick one of these ξ. If every η in $\overline{\mathbb{F}_p}$ with $f(\xi, \eta) = 0$ (if any) satisfies also $\eta(\eta - 1 + \xi) = 0$ then by the Nullstellensatz $f(\xi, y)$ would divide some power of $y(y - 1 + \xi)$ in $\overline{\mathbb{F}_p}[y]$. Thus

$f(\xi,y)=\gamma y^b(y-1+\xi)^c$ for some γ in $\overline{\mathbb{F}_p}^*$ and some non-negative integers b,c (possibly depending on ξ).

However y does not divide $f(\xi,y)$ as $f(\xi,0)\neq 0$; and similarly $y-1+\xi$ does not divide $f(\xi,y)$ as $f(\xi,1-\xi)\neq 0$. Therefore $f(\xi,y)=\gamma$, contradicting one of the conditions above on ξ.

Thus for infinitely many ξ in $\overline{\mathbb{F}_p}^*$ we can find η in $\overline{\mathbb{F}_p}^*$ with $\zeta=\eta-1+\xi\neq 0$. Now we have infinitely many points (ξ,η,ζ) in $\mathcal{C}(K)$ with independent relations $\xi^{a_1}=\eta^{b_2}=1$ for suitable non-zero integers a_1,b_2 (and even $\zeta^{c_3}=1$ too).

Now for Theorem 4.

Proof of Theorem 4. Here we deduce from Lemma 21

$$\xi+\eta-\zeta=1,\quad \rho\xi+\sigma\eta-\tau\zeta=0$$

for $(\xi,\eta,\zeta)=(x,x-t,2x-t-1)$ while ρ,σ,τ are not all zero. Thus

$$0\ =\ \rho x+\sigma(x-t)-\tau(2x-t-1)\ =\ (\rho+\sigma-2\tau)x+(\tau-\sigma)t+\tau.$$

Here $\rho+\sigma-2\tau=0$ would immediately force $\tau-\sigma=\tau=0$ and so $\rho=\sigma=\tau=0$, which is impossible. Therefore it follows that $x=\alpha t+\beta$ with α,β in $\mathbb{F}_p$.

Now we can eliminate $2x-t-1=(2\alpha-1)t+2\beta-1$ from the relations in Theorem 4 to get a non-trivial multiplicative relation between $x=\alpha t+\beta$ and $x-t=(\alpha-1)t+\beta$. If $\alpha\neq 0,\alpha-1\neq 0$ these have degree 1 in $\mathbb{F}_p[t]$. By unique factorization this implies that the polynomials are associate and thus

$$0\ =\ \begin{vmatrix}\alpha & \beta\\ \alpha-1 & \beta\end{vmatrix}\ =\ \beta.$$

Similarly by eliminating $x-t$ we find

$$0\ =\ \begin{vmatrix}\alpha & \beta\\ 2\alpha-1 & 2\beta-1\end{vmatrix}\ =\ -\alpha+\beta$$

if $\alpha\neq 0, 2\alpha-1\neq 0$. And

$$0\ =\ \begin{vmatrix}\alpha-1 & \beta\\ 2\alpha-1 & 2\beta-1\end{vmatrix}\ =\ -\alpha-\beta+1$$

if $\alpha-1\neq 0,2\alpha-1\neq 0$. But these three equations are inconsistent.

If $p\geq 3$ it follows that $\alpha=0,1,\frac{1}{2}$.

If $\alpha=0$ then the third equation gives $\beta=1$ and so $x=1$ as in Theorem 4. Similarly if $\alpha=1,\frac{1}{2}$ we get the other two solutions $x=t+1,\frac{1}{2}t$ respectively.

The case $p=2$ is left to the reader. □

D Two exponential diophantine equations

In this section we find all solutions of the equation

$$3^a + 5^b - 7^c = 1 \tag{D.1}$$

in non-negative integers a, b, c, and also all solutions of the equation

$$y^2 = 3^a + 2^b + 1. \tag{D.2}$$

in integers y and non-negative integers a, b.

The equation (D.1) has been mentioned by Masser [Mas1] (p.203) as an example for which there is still no algorithm to solve completely. It can be interpreted as a special case of an S-unit equation, or, in a broader context, an equation of the type covered by the classical results of Mordell-Lang type. The structure of the solution set can be determined using the Subspace Theorem applied to the more general S-unit equation

$$x_0 + x_1 + \cdots + x_n = 0 \tag{D.3}$$

in non-zero rational integers $x_0, x_1, \ldots, x_n$ with no common factor. When these integers are composed of primes from a fixed finite set, the consequence is that (1.3) has at most finitely many solutions satisfying

$$\sum_{i \in I} x_i \neq 0 \tag{D.4}$$

for all non-empty subsets I of $\{1, \ldots, n\}$. This (D.4) in our case (D.1) is hardly any restriction, and one finds at once that the solution set of (D.1) is at most finite. The general theory also provides an explicit estimate for the number of solutions. But the recent Theorem 1 (p.808) of the paper [ESS] of Evertse, Schlickewei and Schmidt gives only the upper bound $\exp(4.18^9) \approx 10^{344585380964}$, which is little use in actually finding the solutions. The same can be said even for the improvement $24^{1944} \approx 10^{2683}$ by Amoroso and Viada [AmVi]. And it is notorious that in general there are no effective estimates at all for the sizes of the solutions of (D.3). Here we will use a relatively simple method of congruences to show that the only solutions are in fact $a = b = c = 0$ and $a = b = c = 1$.

The equation (D.2) has been mentioned by Zannier [Z1] (pp.61,62) and [Z2] (p.1) and Corvaja and Zannier [CZ2] (p.296), [CZ3] (pp.168,169) (see also [Z3] (p.434), [CZ1] and [C] (p.130)) in the context of the Lang-Vojta Conjecture (see for example [HS] (p.486)). Here the term y^2 prevents the use of the Subspace Theorem as above. And indeed they remark that it is not even known whether the solution set is finite or not, unless one assumes such a conjecture. One can also assume a version for (D.3) which was formulated in elementary terms by Vojta [Voj] (p.7). Namely, for every $\lambda > 1$ there is a constant C and a non-zero homogeneous polynomial F, each depending only on n and λ, such that all solutions of (D.3) in coprime integers satisfy

$$\max\{|x_0|, |x_1|, \ldots, |x_n|\} \leq CP^\lambda \tag{D.5}$$

where P is the product of all the primes dividing the $x_0, x_1, \ldots, x_n$; however (D.4) now has to be replaced by

$$F(x_1, \ldots, x_n) \neq 0. \tag{D.6}$$

For $n = 2$ this is of course the intractable *abc*-conjecture.

With (D.2) we get at once $y^2 \leq C(6|y|)^\lambda$ in (D.5) and so it suffices to fix $\lambda < 2$. Now the failure of (D.6) is not so trivial; but (with $x_0 = y^2$) it would lead to a point $(x_1, x_2) = (3^a, 2^b)$ on one of a finite set of fixed curves. Now since 3 and 2 are multiplicatively independent a well-known result of Liardet (see for example Theorem 7.3 (p.207) of [L]) implies that there are at most finitely many such points unless x_1 or x_2 is constant on one of the curves. But when a or b is constant in (D.2) then it is easy to establish the finiteness, for example with $n = 2$ in Vojta's Conjecture.

Thus *a fortiori* there is no algorithm for the complete solution. Nevertheless we will use the same congruence method to show that the set is indeed finite and in fact that the only solutions are $y = \pm 2, a = 0, b = 1$ and $y = \pm 6, a = 1, b = 5$ and $y = \pm 6, a = b = 3$.

Because both equations do actually have solutions, it may seem impossible that we can use congruences to prove the finiteness. And indeed it would be impossible for equations that are polynomial in all the variables. Here we have exponential terms like 3^a. The values of this for example modulo 12 at $a = 0, 1, 2, 3, 4, \ldots$ are $1, 3, 9, 3, 9, \ldots$; of course eventually periodic but not at once. So if we can show that 3^a must be 1 modulo 12, then we deduce $a = 0$ and not just a congruence for a. It is this principle that we shall exploit, for various moduli the largest of which is 1820. In fact the various moduli could be taken together to show that we get no more solutions of (D.1) modulo 27927900 (and even 20475); however this kind of simplification seems not to be possible for (D.2).

Of course our method is far too special to be considered as a contribution to the theory of either the S-unit equation or the Vojta Conjecture. See also the remark in the footnote of [Z1] (p.57). But its success with the fairly natural equations (D.1) and (D.2) perhaps gives hope that it can be applied to other interesting equations of the same sort. This is certainly true of $y^2 = 10^a + 6^b + 1$ also mentioned in [Z1] (p.60), for example; and already there the same is noted for the two-variable equation $y^2 = 5^a + 2^a + 7$.

D.1 The equation $3^a + 5^b - 7^c = 1$

In this section we prove the following result.

Theorem 5. *Let a, b, c in $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ satisfy (D.1); then either $a = b = c = 0$ or $a = b = c = 1$.*

Proof. We need one simple observation.

Lemma 22. *Let a, b, c be in $\mathbb{N}_0$ with (D.1) and $abc = 0$; then $a = b = c = 0$.*

Proof. At first let $a = 0$. Then (D.1) appears as $5^b = 7^c$ which forces $b = c = 0$. Similarly if we start with $b = 0$. Finally, $c = 0$ leads to $3^a + 5^b = 2$ and so again $a = b = c = 0$, which completes the proof of the present lemma. □

Lemma 22 shows that either $a = b = c = 0$ or $a, b, c \in \mathbb{N}$ and hence in the following we may assume $a, b, c \in \mathbb{N}$.

Let us consider the following table, where we calculate values of $3^n, 5^n, 7^n$

modulo 1820

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$3^n \pmod{1820}$	3	9	27	81	243	729	367	1101	1483	809	607	1	3
$5^n \pmod{1820}$	5	25	125	625	1305	1065	1685	1145	265	1325	1165	365	5
$7^n \pmod{1820}$	7	49	343	581	427	1169	903	861	567	329	483	1561	7

Here we get the same values for $n = 1$ and $n = 13$, hence we see a period of length 12 when we calculate the table above for all n in $\mathbb{N}$.

Now, for m, k in $\mathbb{N}_0$ we define $\{m\}_k = m + k\mathbb{N}_0$. Then the values of n for which the triple $(3^n, 5^n, 7^n)$ lies in various congruence classes modulo 1820 form subsets $\{1\}_{12}, \dots, \{11\}_{12}$ of $\mathbb{N}$.

Perhaps with the help of a computer we now look for (a, b, c) with $1 \leq a, b, c \leq 12$ such that

$$3^a + 5^b - 7^c \equiv 1 \pmod{1820}$$

In fact we find that $(a, b, c) = (1, 1, 1)$ is the only triple as required and this proves that a, b, c lie in the set $\{1\}_{12}$, which means that

$$a \equiv b \equiv c \equiv 1 \pmod{12} \tag{D.7}$$

However, we rerun the procedure above modulo 341. Due to (D.7) we just consider values with $n \equiv 1 \pmod{12}$ and get the table

n	1	13	25	37	49	61
$3^n \pmod{341}$	3	148	254	141	136	3
$5^n \pmod{341}$	5	191	67	36	284	5
$7^n \pmod{341}$	7	112	87	28	107	7

Here we see a period of length 60 and, as before, we find that $(1, 1, 1)$ is the only solution of (D.1) modulo 341 from the table above. This implies that

$$a \equiv b \equiv c \equiv 1 \pmod{60}$$

Let us continue with the following table modulo 50

n	1	61	121
$3^n \pmod{50}$	3	3	3
$5^n \pmod{50}$	5	25	25
$7^n \pmod{50}$	7	7	7

Here we have only the two classes $\{1\}_0 = \{1\}$ and $\{61\}_{60}$, in which the first class is finite because the sequence $5^n \pmod{50}$ is not periodic but only eventually so. Now looking for solutions of (D.1) modulo 50 forces $b = 1$.

Thus with (D.1) we get the new equation

$$7^c - 3^a = 4. \tag{D.8}$$

And here

n	1	61	121
$7^n \pmod{9}$	7	7	7
$3^n \pmod{9}$	3	0	0

which forces in a similar way $a = 1$. Now (D.8) implies that $c = 1$ and this completes the proof of Theorem 5. □

D.2 The equation $y^2 = 3^a + 2^b + 1$

In this section we prove the following result.

Theorem 6. *Let y in $\mathbb{Z}$ and a, b in $\mathbb{N}_0$ satisfy (D.2); then either $y = \pm 2$ and $a = 0, b = 1$ or $y = \pm 6$ and $a = 1, b = 5$ or $a = b = 3$.*

At first we note that $y \neq 0$ and hence we may assume $y \in \mathbb{N}$ without loss of generality.

Lemma 23. *Let y in $\mathbb{N}$ and a, b in $\mathbb{N}_0$ with $ab = 0$ satisfy (D.2); then $y = 2$ and $a = 0, b = 1$.*

Proof. At first let $a = 0$. Then $b \neq 0$ because 3 is not a square. Further $b = 1$ leads to $y^2 = 4$ and so $y = 2$. If now $b \geq 2$ then $4 \mid 2^b$ and so

$$y^2 \equiv 2 \pmod 4,$$

impossible because $y^2 \equiv 0, 1 \pmod 4$.

Otherwise we have a in $\mathbb{N}$ and $b = 0$ which leads to

$$y^2 \equiv 2 \pmod 3,$$

impossible because $y^2 \equiv 0, 1 \pmod 3$. This completes the proof. □

Therefore we may assume that a, b are in $\mathbb{N}$.

Lemma 24. *Let y, a, b in $\mathbb{N}$ satisfy (D.2); then 6 divides y.*

Proof. We calculate (D.2) modulo 2. Then

$$y^2 \equiv 3^a + 2^b + 1 \equiv 1 + 0 + 1 \equiv 0 \pmod 2,$$

hence y^2 is even and so is y.

Similarly we consider (D.2) modulo 3. Here

$$(y + 1)(y - 1) \equiv y^2 - 1 \equiv 3^a + 2^b \equiv 2^b \not\equiv 0 \pmod 3.$$

So neither $y+1$ nor $y-1$ is divisible by 3 and hence 3 divides y, which completes the proof of the present lemma. □

Lemma 24 shows that $y = 6x$ for some x in $\mathbb{N}$ and thus (D.2) appears as

$$36x^2 = 3^a + 2^b + 1. \tag{D.9}$$

Lemma 25. *Let x, a, b in $\mathbb{N}$ satisfy (D.9). Then exactly one of the following holds:*

1. *$x = 1$ and either $a = 1, b = 5$ or $a = b = 3$,*

2. *x is odd, $a \equiv 1 \pmod 8$, and $b \equiv 3 \pmod 6$ with $a \neq 1$, $b \neq 3$.*

Proof. Considering (D.9) modulo 36 we get

$$0 \equiv 3^a + 2^b + 1 \pmod{36}. \tag{D.10}$$

Further we calculate in the table below 3^n and 2^n modulo 36 for $1 \leq n \leq 8$.

n	1	2	3	4	5	6	7	8
$3^n \pmod{36}$	3	9	27	9	27	9	27	9
$2^n \pmod{36}$	2	4	8	16	32	28	20	4

Here we note that we get the same values for $n = 2$ and $n = 8$. Hence we see a period of length 6 when we calculate the table above for all n in $\mathbb{N}$ or rather we get a partition of $\mathbb{N}$ with the classes

$$\{1\}_0 = \{1\},\ \{2\}_6 = 2 + 6\mathbb{N}_0, \ldots,\ \{7\}_6 = 7 + 6\mathbb{N}_0. \tag{D.11}$$

We now look for all (a, b) with $1 \leq a, b \leq 7$ satisfying (D.10) and with the table above we find

$$(a, b) = (1, 5), (3, 3), (5, 3), (7, 3).$$

Together with (D.11) this implies that for $a, b \in \mathbb{N}$ we have either $a = 1$ and $b \in \{5\}_6$ or a is in one of the sets $\{3\}_6, \{5\}_6, \{7\}_6$ and $b \in \{3\}_6$.

Consider first $a = 1$. Then (D.9) appears as

$$36x^2 = 2^b + 4$$

and hence

$$(6x + 2)(6x - 2) = 2^b.$$

Thus $6x + 2$ and $6x - 2$ are powers of 2 and $(6x + 2) - (6x - 2) = 4$ yields $6x + 2 = 8$ and $6x - 2 = 4$ respectively; so $x = 1$ and $b = 5$.

Otherwise $a \neq 1$ is odd and $b \equiv 3 \pmod 6$. Now $b = 3$ in (D.9) leads to

$$36x^2 = 3^a + 9$$

and similar to above we see that $6x+3$ and $6x-3$ are powers of 3 with $(6x+3)$ $-(6x - 3) = 6$; hence $x = 1$ and $a = 3$, which completes the first part of the lemma.

Let now $b \neq 3$. Since a is odd (D.9) yields

$$36x^2 \equiv 3 + 0 + 1 \equiv 4 \pmod 8$$

and thus x is odd. So $x = 2z + 1$ and now

$$36x^2 = 288\frac{z(z + 1)}{2} + 36 \equiv 4 \pmod{32}$$

Therefore (D.9) leads to

$$3 \equiv 3^a \pmod{32}.$$

For the values of $3^n \pmod{32}$ we consider the following table

n	1	3	5	7	9
$3^n \pmod{32}$	3	27	19	11	3

Here we see a period of length 8 and hence that $a \equiv 1 \pmod 8$. Therefore the present lemma is proved. □

Lemma 26. *There are no x, a, b in $\mathbb{N}$ with (D.9) which satisfy the conditions of the second part of Lemma 25.*

Proof. Suppose that we have such x, a, b in $\mathbb{N}$. We then consider (D.9) modulo 120. Therefore we use the table

n	3	5	7
$3^n \pmod{120}$	27	3	27
$2^n \pmod{120}$	8	32	8

Similar to above we see a period of length 4 and $a \equiv 1 \pmod 8$ with $a \neq 1$ implies that a is in the set $\{5\}_4 = 5 + 4\mathbb{N}_0$. Further we note that

$$36x^2 \equiv \begin{cases} 36 \pmod{120}, & x \equiv \pm 1 \pmod{10}, \\ 84 \pmod{120}, & x \equiv \pm 3 \pmod{10}, \\ 60 \pmod{120}, & x \equiv 5 \pmod{10}. \end{cases}$$

Therefore we find that $b \in \{5\}_4$ as well because $36x^2 \not\equiv 12 \pmod{120}$. So the left side of (D.9) is $36 \pmod{120}$ and hence we have $x = \pm 1 \pmod{10}$. Further $b \in \{5\}_4$ implies that $b \equiv 9 \pmod{12}$ because $b \equiv 3 \pmod 6$.

Next we consider (D.9) modulo 560. Therefore we use the following table

n	5	9	13	17
$3^n \pmod{560}$	243	83	3	243
$2^n \pmod{560}$	32	512	352	32

Thus we see a period of length 12. Now $a \equiv 1 \pmod 8$ with $a \neq 1$ means that a is in one of the sets $\{5\}_{12}, \{9\}_{12}, \{13\}_{12}$ and $b \equiv 9 \pmod{12}$ shows $b \in \{9\}_{12}$. Further, $x \equiv \pm 1 \pmod{10}$ and we get

$$36x^2 \equiv \begin{cases} 36 \pmod{560}, & x \equiv \pm 1, \pm 29 \pmod{70}, \\ 116 \pmod{560}, & x \equiv \pm 9, \pm 19 \pmod{70}, \\ 436 \pmod{560}, & x \equiv \pm 11, \pm 31 \pmod{70}, \\ 196 \pmod{560}, & x \equiv \pm 21 \pmod{70}; \end{cases}$$

and thus we see that a is not in the set $\{13\}_{12}$.

Finally, let us consider (D.9) modulo 208. Here we have a table

n	5	9	13	17
$3^n \pmod{208}$	35	131	3	35
$2^n \pmod{208}$	32	96	80	32

Again we see a period of length 12 and as above it follows that a is in one of the sets $\{5\}_{12}, \{9\}_{12}, \{13\}_{12}$ and $b \in \{9\}_{12}$. And $x \in \mathbb{N}$ is odd so we find

$$36x^2 \equiv \begin{cases} 36 \pmod{208}, & x \equiv \pm 1 \pmod{26}, \\ 116 \pmod{208}, & x \equiv \pm 3 \pmod{26}, \\ 68 \pmod{208}, & x \equiv \pm 5 \pmod{26}, \\ 100 \pmod{208}, & x \equiv \pm 7 \pmod{26}, \\ 4 \pmod{208}, & x \equiv \pm 9 \pmod{26}, \\ 196 \pmod{208}, & x \equiv \pm 11 \pmod{26}, \\ 52 \pmod{208}, & x \equiv 13 \pmod{26}. \end{cases}$$

But this forces $a \in \{13\}_{12}$, which is a contradiction to above; and this completes the proof of the present lemma. $\square$

Now the proof of Theorem 6 follows directly from the lemmas above.

References

[ABB] L. Arenas-Carmona, D. Berend and V. Bergelson, *Ledrappier's system is almost mixing of all orders*, Ergodic Theory and Dynamical Systems **28** (2008), 339-365.

[AbVo] D. Abramovich and F. Voloch, *Towards a proof of the Mordell-Lang conjecture in characteristic p*, International Math. Research Notices **5** (1992), 103-115.

[AmVi] F. Amoroso and E. Viada, *Small points on subvarieties of a torus*, Duke Math. J. **150** (2009), 407-442.

[BMZ] E. Bombieri, D. Masser and U. Zannier, *On unlikely intersections of complex varieties with tori*, Acta Arithmetica **133** (2008), 309-323.

[BHMZ] E. Bombieri, P. Habegger, D. Masser and U. Zannier, *A note on Maurin's Theorem*, Rend. Lincei Mat. Appl. **21** (2010), 251-260.

[C] P. Corvaja, *Problems and results on integral points on rational surfaces*, in Diophantine geometry (ed. U. Zannier), Edizioni della Normale 2007, 123-141.

[CZ1] P. Corvaja and U. Zannier, *On the diophantine equation* $f(a^m, y) = b^n$, Acta Arithmetica **94** (2000), 25-40.

[CZ2] P. Corvaja and U. Zannier, *Some cases of Vojta's conjecture on integral points over function fields*, J. Algebraic Geometry **17** (2008), 295-333.

[CZ3] P. Corvaja and U. Zannier, *Applications of the subspace theorem to certain diophantine problems*, in Diophantine approximation, Developments in Mathematics **18** (eds H.P. Schlickewei, K. Schmidt, R.F. Tichy), Springer 2008, 161-174.

[DM] H. Derksen and D. Masser, *Linear equations over multiplicative groups, recurrences, and mixing I*, Proc. London Math. Soc. **104** (2012), 1045-1083.

[E] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Mathematica **53** (1984), 225-244.

[ESS] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals of Mathematics **155** (2002), 807-836.

[G] D. M. Goldschmidt, *Algebraic functions and projective curves*, Springer Verlag 2003.

[GM] D. Ghioca and R. Moosa, *Division points on subvarieties of isotrivial semi-abelian varieties*, International Math. Research Notices, Article ID 65437 (2006), 23 pages.

[GV] A. Garcia and J.F. Voloch, *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math. **59** (1987), 457-469.

[H] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J. American Math. Soc. **9** (1996), 667-690.

[HP] E. Hrushovski and A. Pillay, *Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties*, American J. Math. **122** (2000), 439-450.

[HS] M. Hindry and J. H. Silverman, *Diophantine Geometry*, Springer 2000.

[La1] S. Lang, *Introduction to algebraic geometry*, Addison-Wesley 1972.

[La2] S. Lang, *Fundamentals of diophantine geometry*, Springer Verlag 1983.

[La3] S. Lang, *Algebra*, Springer Verlag 2002.

[Le1] D. Leitner, *Two exponential diophantine equations*, Journal de théorie des nombres de Bordeaux **23** (2011), 479-487.

[Le2] D. Leitner, *Linear equations over multiplicative groups in positive characteristic*, Acta Arithmetica **153** (2012), 325-347.

[Le3] D. Leitner, *Linear equations over multiplicative groups in positive characteristic II*, submitted.

[Mas1] D. Masser, *Mixing and linear equations over groups in positive characteristic*, Israel J. Math. **142** (2004), 189-204.

[Mas2] D. Masser, *Unlikely intersections for multiplicative groups over positive characteristic*, in preparation.

[Mau] G. Maurin, Courbes algébriques et équations multiplicatives, Math. Annalen **341** (2008), 789-824.

[MS1] R. Moosa and T. Scanlon, *The Mordell-Lang conjecture in positive characteristic revisited*, Model theory and applications, Quaderni di matematica **11** (eds. L. Belair, Z. Chatzidakis, P. D'Aquino, D. Marker, M. Otero, F. Point, and A. Wilkie), Dipartimento di Matematica Seconda Università di Napoli (2002), 273-296.

[MS2] R. Moosa and T. Scanlon, *F-structures and integral points on semiabelian varieties over finite fields*, American J. Math. **126** (2004), 473-522.

[P] R. Pink, *A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang*, manuscript dated 17th April 2005 (13 pages).

[PS] A.J. van der Poorten and H. P. Schlickewei, *Additive relations in fields*, J. Australian Math. Soc. **A 51** (1991), 154-170.

[Sc] T. Scanlon, *A positive characteristic Manin-Mumford theorem*, Compositio Mathematica **141** (2005), 1351-1364.

[St] H. Stichtenoth, *Algebraic function fields and codes*, Springer Verlag 2009.

[Voj] P. Vojta, *A more general abc conjecture*, International Math. Research Notices **21** (1998), 1103-1116.

[Vol1] J.F. Voloch, *On the conjectures of Mordell and Lang in positive characteristic*, Inventiones Math. **104** (1991), 643-646.

[Vol2] J.F. Voloch, *The equation $ax + by = 1$ in characteristic p*, J. Number Theory **73** (1998), 195-200.

[W] R. Walker, *Algebraic curves*, Princeton University Press 1955.

[Z1] U. Zannier, *Some applications of diophantine approximation to diophantine equations*, Forum Editrice Universitaria Udinese S.r.l. (2003).

[Z2] U. Zannier, *Polynomial squares of the form $aX^m+b(1-X)^n+c$*, Rendiconti del Seminario Matematico della Universit di Padova **112** (2004), 1-9.

[Z3] U. Zannier, *Diophantine equations with linear recurrences. An overview of some recent progress*, Journal de Thorie des Nombres de Bordeaux **17** (2005), 432-435.

[Za] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Math. Studies **181**, Princeton 2012.

[Zi] B. Zilber, *Exponential sums equations and the Schanuel conjecture*, J. London Math. Soc. **65** (2002), 27-44.

Curriculum Vitae

I was born on October 17th 1981 in Basel. I am citizen of Basel. My parents are Oswald and Doris Leitner.

Education

April 2009	-	March 2013	PhD in Mathematics at the University of Basel, Switzerland. Adviser: Prof. Dr. David Masser.
October 2012	-	November 2012	Research visit at the Mathematical Institute of Oxford, United Kingdom.
October 2005	-	February 2009	Master studies in Mathematics at the University of Basel. Degree: Master of Science in Mathematics.
October 2002	-	November 2005	Bachelor studies in Mathematics at the University of Basel. Degree: Bachelor of Science in Mathematics.
August 1995	-	June 2001	Humanistisches Gymnasium, Basel. Degree: Matura Typus A.

I have visited lectures and seminars of Prof. M. Grote, Prof. H.-C. Im Hof, Prof. H. Kraft, Dr. C. Luchsinger, Prof. D. Masser, Prof. W. Reichel, Prof. C. Schönenberger, Prof. B. Schweizer, PD Dr. P. Weidemaier.