T. M. Groen

Suzuki groups and the other Zassenhaus groups

Bachelor thesis, 27th August 2012

Supervisor: Dr. B. de Smit

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

In 1934, the famous mathematician Hans Julius Zassenhaus classified the sharply triply transitive permutation groups in his dissertation. This would lead to an attempt to also classify a closely related class of doubly transitive permutation groups, these days known as Zassenhaus groups. Michio Suzuki, Walter Feit and Noburu Ito made the most important contributions to this endeavour. Eventually, Michio Suzuki would finish this classification in 1962.

In his pursuit for this classification, Suzuki discovered a new family of finite simple groups. Nowadays, these groups are known as the Suzuki groups and are often denoted as $\mathrm{Suz}(2^{2n+1})$. Suzuki defined his groups as a subgroup of the matrix group of invertibele 4×4 matrices over F, with F a well chosen field. He defined his groups by giving three generators. As these generators were matrices the calculations involved to prove that $\mathrm{Suz}(2^{2n+1})$ is a Zassenhaus group are not very insightfull. Another way to construct these groups is by means of Lie Algebras. This contruction however would require too much machinery for our purposes. In 2009, Robert Wilson published a new construction of the Suzuki groups which is rather elementary, and in his own words: "in time it will come to be regarded as the standard construction. "

In this bachelor thesis I will review the different Zassenhaus groups with a special emphasis on the Suzuki groups using Wilson's construction.

1 Zassenhaus groups

Definition 1.1. A group G that acts on a set X is said to be *k-transitive* if $\#X \geq k$ and the following condition is satisfied:
For all sequences $(x_1, ..., x_k)$ and $(x'_1, ..., x'_k)$ in X, each consisting of k distinct elements there is an element $\sigma \in G$ such that:

$$\sigma x_i = x'_i \quad \forall i \in \{1, ..., k\}$$

Definition 1.2. A group action of G on a set X is said to be *regular* if for all $\alpha, \beta \in X$ there is a unique $g \in G$ such that $g \cdot \alpha = \beta$.

Remark. A group action is regular if it is both free and transitive.

Definition 1.3. A permutation group G that acts on a finite set X is said to be a *Zassenhaus group* if the following conditions are satisfied:

1. G is 2-transitive.
2. Every non-trivial element in G fixes at most 2 points of X.
3. G has no regular normal subgroup.

Remark. If G is simple then G has no regular normal subgroup.

Another thing worth mentioning is the following: If G is a Zassenhaus group it acts faithfully on X. Hence the induced homomorfism $G \to \mathrm{Sym}(X)$ is injective. Because X is finite it follows that G is finite.

The third condition in the definition of a Zassenhaus group seems a bit artificial and needs some explanation. In order to do so we need these definitions.

Definition 1.4. Let G be a group acting on a finite set X. Then the degree of G is defined to be the number of elements of X.

Definition 1.5. A transitive permutation group G on a finite set is said to be a *Frobenius group* if it satisfies the following conditions:

1. Every non-trivial element in G fixes at most 1 point.
2. There exists a non-trivial element in G which fixes a point.

If we omit the third Zassenhaus condition the only extra groups we get are Frobenius groups or groups that are not of the Frobenius kind and have a normal regular subgroup. Feit proved the following theorem about the latter case:

Proposition 1.6. *Suppose that G is a permutation group of degree $n+1$ such that:*

1. *G is 2-transitive.*
2. *Every non-trivial element in G fixes at most 2 points.*
3. *G has regular normal subgroup.*
4. *G is not a Frobenius group.*

Then $n + 1 = 2^p$ for certain prime p and G is the group of all semilinear mappings $x \mapsto a \cdot \alpha(x) + b$ with $a, b \in \mathbb{F}_q$ ($q = 2^p$), $a \neq 0$ and α an automorfism of $\mathbb{F}_q$. In particular $\#G = 2^p(2^p - 1)p$ and G is solvable.

A proof can be found in [3], Chapter 11. To conclude, the third Zassenhaus condition is meant to eliminate the cases just mentioned.

1.1 Iwasawa's lemma

Definition 1.7. Let G act on a set X. Let $\{X_i\}_{i\in I}$ be a partition of X. This partition is said to be *G-stable* if G maps each X_i to X_j for some j.
That is:

$$\forall g \in G\, \forall i \in I\, \exists j \in I \text{ such that } g \cdot X_i = X_j$$

Definition 1.8. Let G act transitively on X with $\#X \geq 2$. The action of G on X is said to be primitive if there are precisely two G-stable partitions.

Remark. If G acts doubly transitively on X then its action is also primitive.

Proposition 1.9. *Let G act transitively on X with $\#X \geq 2$. Then the following are equivalent:*

1. *The action of G on X is primitive.*
2. *For all $x \in X$ holds: $Stab(x) \subset G$ is maximal.*

Proof. Let $x \in X$. Suppose $\{X_i\}_{i\in I}$ is a G-stable partition of X. Then G acts in the obvious way on $\{X_i\}_{i\in I}$ and there is a $j \in I$ such that $x \in X_j$. Thus we have that $\mathrm{Stab}(x) \subset \mathrm{Stab}(X_j)$. Hence we have the following map:

$$\{G\text{-stable partitions of } X\} \to \{K \subset G : \mathrm{Stab}(x) \subset K \subset G\}$$

$$\{X_i\}_{i\in I} \mapsto \mathrm{Stab}(X_j)$$

We will show that the map above is a bijection. In order to prove this, we will construct its inverse. Therefore let $K \subset G$ with $\mathrm{Stab}(x) \subset K \subset G$ and consider the set $Kx \subset X$. We will show that $\{gKx\}_{g\in G}$ is a partition of X.

By the transitivity of G it is clear that:

$$\bigcup_{g\in G} gKx = X$$

For $g \in G$ consider $gKx \cap Kx$. Suppose $a \in gKx \cap Kx$ then we have:

$$a = gk'x = kx \text{ for some } k, k' \in K$$

From this follows that $k^{-1}gk'x = x$ and thus $k^{-1}gk \in \mathrm{Stab}(x)$. Since $\mathrm{Stab}(x) \subset K$ we see $g \in K$. Hence for all $g \in G$ holds $gKx = Kx$ or $gKx \cap Kx = \emptyset$ (†).

Now let $g_1, g_2 \in G$ and consider $g_1Kx \cap g_2Kx$. Suppose $g_1Kx \cap g_2Kx \neq \emptyset$ and thus take $a \in g_1Kx \cap g_2Kx$. From this follows $g_2^{-1}a \in g_2^{-1}g_1Kx \cap Kx$. Using (†) we see that $g_2^{-1}g_1Kx = Kx$ and finally $g_1Kx = g_2Kx$. This means that elements of $\{gKx\}_{g\in G}$ are pairwise disjoint. Consequently $\{gKx\}_{g\in G}$ is a partition of X and by definition it is G-stable. Combining all this we get the following map:

$$\{K \subset G : \mathrm{Stab}(x) \subset K \subset G\} \to \{G\text{-stable partitions of } X\}$$

$$K \mapsto \{gKx\}_{g\in G}$$

It is clear that this map is the inverse of the map above. Hence the G-stable partitions of X are in one-to-one correspondence with the subgroups K between $\mathrm{Stab}(x)$ and G. This immediately gives the equivalence of 1. and 2. □

Definition 1.10. A group G is said to be perfect if $[G, G] = G$.

Lemma 1.11. *Let G, G' be a groups and $f : G \to G'$ a homomorfism. Then $f([G, G]) \leq [G', G']$.*

Proof.

$$f\left(\prod_{i=1}^{n}[g_i, h_i]\right) = \prod_{i=1}^{n} f[g_i, h_i] = \prod_{i=1}^{n}[f(g_i), f(h_i)] \subset [G', G']$$

□

Lemma 1.12. *Let G be a group and N a normal subgroup. Then G is solvable if and only if N and G/N are solvable.*

A proof can be found in [2]. The following proposition is due to Iwasawa and will give us the instrument to prove simplicity of several groups.

Proposition 1.13. *Let G be a group that acts faithfully on a set X such that:*

- *The action of G on X is primitive.*
- *The group G is perfect.*
- *There is a point stabilizer $H \subset G$ which has a normal solvable subgroup A such that the conjugates of A in G, generate G.*

Then G is simple.

Proof. Suppose G is not simple. Then there exists a normal $K \subset G$ such that $\{1\} < K < G$. By assumption, the action of G on X is faithful. So if we take $k_1, k_2 \in K$ distinct then there is an $s \in X$ such that $k_1 s \neq k_2 s$. Hence K does not fix all the points.

Now suppose there is an $x \in X$ such that $K \subset \mathrm{Stab}(x)$. By transitivity of G there is a $g \in G$ such that $gx = s$. Hence follows:

$$\{gx\} = gKx = Kgx = Ks \neq \{gx\}$$

For the second equality we use the normality of K. This contradiction guarantees that K does not fix any point.

Let H be the given point stabilizer. We see $K \not\subseteq H$. Since G is primitive H is maximal by proposition 1.9 and thus $HK = G$. So if $g \in G$ we have $g = hk$ with $h \in H$ and $k \in K$. Consequently:

$$g^{-1}Ag = k^{-1}h^{-1}Ahk = k^{-1}Ak \subset AK$$

So every conjugate of A is contained in AK, hence $AK = G$. Thus we now have:

$$G/K = AK/K \cong A/(A \cap K)$$

By lemma 1.12 we see that $A/(A \cap K)$ is solvable. Thus G/K is solvable. However, this contradicts the perfectness of G by the following argument:

Define $f : G \to G/K$ to be the qoutient map. By the lemma above we have:

$$[G/K, G/K] \supset f([G, G]) = f(G) = G/K$$

And thus G/K is not solvable. □

1.2 Linear groups

Definition 1.14. Let F be a field and $n \in \mathbb{Z}_{>0}$. The group of invertible $n \times n$ matrices over F is called the *general linear group* of degree n over F; It is denoted $\mathrm{GL}(n, F)$.

Definition 1.15. Let F be a field and $n \in \mathbb{Z}_{>0}$. Let $\mathrm{Z}(n, F)$ denote the center of $\mathrm{GL}(n, F)$. The *projective general linear group* of degree n over F, denoted $\mathrm{PGL}(n, F)$, is defined to be:

$$\mathrm{PGL}(n, F) := \mathrm{GL}(n, F)/\mathrm{Z}(n, F)$$

Since $\mathrm{Z}(n, F)$ is normal in $\mathrm{GL}(n, F)$ the resulting $\mathrm{PGL}(n, F)$ is a group.

Definition 1.16. Let F be a field and $n \in \mathbb{Z}_{>0}$. The group of $n \times n$ matrices over F having determinant 1 is called the *special linear group* of degree n over F; It is denoted $\mathrm{SL}(n, F)$.

Definition 1.17. Let F be a field and $n \in \mathbb{Z}_{>0}$. Let $\mathrm{SZ}(n, F)$ denote the center of $\mathrm{SL}(n, F)$. The *projective special linear group* of degree n over F, denoted $\mathrm{PSL}(n, F)$, is defined to be:

$$\mathrm{PSL}(n, F) := \mathrm{SL}(n, F)/\mathrm{SZ}(n, F)$$

Let V be a vector space over a field F of dimension n and let $\mathrm{GL}(V)$ be the group of automorfisms of V. Then an element of $\mathrm{GL}(n, F)$ naturally corresponds to a linear isomorfism of V (with respect to a certain basis). Hence we have $\mathrm{GL}(V) \cong \mathrm{GL}(n, F)$. Let $\mathrm{SL}(V)$ be the group of automorfisms of V with determinant 1. Remark that the determinant of a matrix does not depend on the choice of basis, hence we also have $\mathrm{SL}(V) \cong \mathrm{SL}(n, F)$. In an analogous manner we also have $\mathrm{Z}(n, F) \cong \mathrm{Z}(V)$ and $\mathrm{SZ}(n, F) \cong \mathrm{SZ}(V)$. Hence also $\mathrm{PGL}(n, F) \cong \mathrm{PGL}(V)$ and $\mathrm{PSL}(n, F) \cong \mathrm{PSL}(V)$.

Definition 1.18. Let V be a vector space of dimension n over a field F . An element $f \in \mathrm{SL}(V)$ is said to be a transvection if it is not the identity but it fixes all elements of a certain hyperplane H of V.

Lemma 1.19. *The group $SL(V)$ is generated by transvections.*

A proof can be found in [1].

Proposition 1.20. *Suppose $z \in GL(V)$, then the following are equivalent:*

1. *The element z commutes with all transvections.*
2. *The element z fixes every one-dimensional subspace of V.*
3. *There exists a $\lambda \in F$ such that $z(v) = \lambda v$ for all $v \in V$.*
4. *The element z lies in the center of $GL(V)$.*

Proof. (1) $\Rightarrow$ (2) Let U be a one-dimensional subspace of V. There is a transvection t such that $(t-1)V = U$. Hence:

$$U = (t-1)V = (ztz^{-1} - 1)V = z(t-1)z^{-1}V = z((t-1)V) = z(U)$$

(2) $\Rightarrow$ (3), (3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (1) are evident. $\square$

Corollary 1.21. *$Z(V) = \{\lambda \cdot Id : \lambda \in F^*\}$ and $SZ(V) = SL(V) \cap Z(V)$.*

Consider the map $i : \mathrm{PSL}(V) \to \mathrm{PGL}(V)$ with $x \cdot \mathrm{SZ}(V) \mapsto x \cdot \mathrm{Z}(V)$. It is easy to see that this map is well-defined. Now suppose we have $x, y \in \mathrm{SL}(V)$ such that $x \cdot \mathrm{Z}(V) = y \cdot \mathrm{Z}(V)$. Then we have $y^{-1}x \in \mathrm{Z}(V)$ and obviously $y^{-1}x \in \mathrm{SL}(V)$. As a consequence we have that $y^{-1}x \in \mathrm{SZ}(V)$ and thus $x \cdot \mathrm{SZ}(V) = y \cdot \mathrm{SZ}(V)$. We conclude that i is injective. By means of this injection we can consider $\mathrm{PSL}(V)$ as a subgroup of $\mathrm{PGL}(V)$.
Define $(F^*)^n := \{x^n : x \in F^*\}$. Then we also have a map $\overline{\det} : \mathrm{PGL}(V) \to F^*/(F^*)^n$ with $\overline{x} \mapsto \overline{\det(x)}$. If $y \in \mathrm{Z}(V)$ then $y = \lambda \mathrm{Id}$ for a certain $\lambda \in F^*$ and thus $\det(y) = \lambda^n$. As a result this map is well-defined. Furthermore, this homomorfism is obviously surjective.

Proposition 1.22. *Let V be an n-dimensional vector space over F. Then we have the following exact sequence:*

$$0 \longrightarrow PSL(V) \xrightarrow{i} PGL(V) \xrightarrow{\overline{\det}} F^*/(F^*)^n \longrightarrow 0$$

Proof. Remark that every element in the image of i is contained in the kernel of $\overline{\det}$. Let $\overline{x} \in \ker(\overline{\det})$, then we have that $\det(x) \in (F^*)^n$. We have $\det(x) = \lambda^n$ for a certain $\lambda \in F^*$. Hence follows that $\det(\lambda^{-1} \cdot \mathrm{Id} \cdot x) = 1$ and thus $\lambda^{-1} \cdot \mathrm{Id} \cdot x \in \mathrm{SL}(V)$. Now remark that $\lambda^{-1} \cdot \mathrm{Id} \cdot x \cdot \mathrm{Z}(V) = x \cdot \mathrm{Z}(V)$. We see that $\overline{x} \in \mathrm{Im}(i)$ and as a result $\mathrm{Im}(i) = \ker(\overline{\det})$. □

Suppose $F = \mathbb{F}_q$ with q a prime power and $n = 2$. Since F is a finite field F^* is cyclic and thus $F^* = \langle c \rangle$ for a certain $c \in F^*$. Remark that c has order $q - 1$. If q is a power of 2 we have that $q - 1$ and 2 are coprime. Hence follows that $(F^*)^2 = F^*$. If q is a power of an odd prime we have that $q - 1$ is divisible by 2. Then $(F^*)^2$ has index 2 in F^*. By the exact sequence above it follows that $\mathrm{PGL}(2, \mathbb{F}_q)$ contains $\mathrm{PSL}(2, \mathbb{F}_q)$ with index 1 or 2.

Proposition 1.23. *Let F be a field and $n \in \mathbb{Z}_{\geq 2}$. Then $PSL(n, F)$ acts doubly transitively on $\mathbb{P}^{n-1}(F)$.*

Proof. Since all the elements in $\mathrm{SZ}(n, F)$ are of the form $\lambda \cdot \mathrm{Id}$ the canonical action of $\mathrm{PSL}(n, F)$ on $\mathbb{P}(F^n)$ is well-defined. Let P_1 and P_2 be two different points in $\mathbb{P}(F^n)$. Then $P_i = \langle v_i \rangle$ with $v_i \in F^n \setminus \{0\}$. Hence v_1 and v_2 are linearly independent. Let Q_1, Q_2 be two different points in $\mathbb{P}(F^n)$ induced by linearly independent vectors w_1 and w_2. For all $\lambda \in F^*$ there is a $\sigma \in \mathrm{GL}(n, F)$ such that $\sigma(v_1) = w_1$ and $\sigma(v_2) = \lambda w_2$. Now choose λ such that $\det(\sigma) = 1$. Then $\sigma \in \mathrm{SL}(n, F)$. Note that this σ does not need be unique. We conclude that $\mathrm{PSL}(n, F)$ is 2-transitive. □

Corollary 1.24. *Let F be a field and $n \in \mathbb{Z}_{>1}$. Then $PGL(n, F)$ acts doubly transitively on the points of $\mathbb{P}^{n-1}(F)$.*

We introduce the following notation. For $\mathrm{PGL}(n, \mathbb{F}_q)$ and $\mathrm{PSL}(n, \mathbb{F}_q)$ we write $\mathrm{PGL}(n, q)$ and $\mathrm{PSL}(n, q)$, respectively.

Proposition 1.25. *$PSL(2, q)$ is simple for $q > 3$.*

Proof. By proposition 1.23 we have that the action of $\mathrm{PSL}(2,q)$ on $\mathbb{P}^1(\mathbb{F}_q)$ is doubly transitive and thus primitive. Define $H := \mathrm{Stab}_{(1:0)}$. One easily sees that $A \subset H$ with A as follows:

$$A := \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in F \right\}$$

Remark that A is abelian and thus solvable. The non-trivial elements from A are induced by transvections and these matrices encode elementary row operations. Since all elements in $\mathrm{PSL}(2,q)$ have determinant 1 they are the product of these row operations. Thus the conjugates of A generate the entire group.

Since the polynomial $X^2 - 1$ can have at most 2 distinct roots in $\mathbb{F}_q$ and $q > 3$ there is a non zero element $x \in F$ such that $x^2 \neq 1$. Now remark that:

$$\left[\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} \right] = \begin{pmatrix} 1 & (x^2-1)y \\ 0 & 1 \end{pmatrix}$$

We conclude that all the transvections are contained in the commutator of $\mathrm{PSL}(2,q)$ and thus $\mathrm{PSL}(2,q)$ is simple by Iwasawa's Lemma (Proposition 1.13). □

Proposition 1.26. *$PGL(2,q)$ acting on $\mathbb{P}^1(\mathbb{F}_q)$ is a Zassenhaus group for $q > 3$.*

Proof. We already showed that $\mathrm{PGL}(2,q)$ acts doubly transitively.
Since $\mathrm{PGL}(2,q)$ contains $\mathrm{PSL}(2,q)$ with index 1 or 2 and $\mathrm{PSL}(2,q)$ is simple it follows that $\mathrm{PSL}(2,q)$ is the only non trivial normal subgroup within $\mathrm{PGL}(2,\mathbb{F}_q)$. As a consequence $\mathrm{PGL}(2,q)$ does not contain a regular normal subgroup.

Now suppose an element $f \in \mathrm{PGL}(2,q)$ fixes three different points in $\mathbb{P}^1(\mathbb{F}_q)$. These points lie in general position and as a consequence $f = \mathrm{Id}$. Therefore $\mathrm{PGL}(2,q)$ is a Zassenhaus group. □

$\mathrm{PGL}(2,2)$ and $\mathrm{PGL}(2,3)$ are not Zassenhaus groups. This can be seen in the following way:

$$\mathrm{PGL}(2,2) \cong \mathrm{GL}(2,\mathbb{F}_2) \cong S_3 \text{ and } \mathbb{P}^1(\mathbb{F}_2) = \{(1:0),(1:1),(0:1)\}$$

Since the subgroup isomorfic to A_3 within $\mathrm{PGL}(2,2)$ does act regularly on $\mathbb{P}^1(\mathbb{F}_2)$ it follows that $\mathrm{PGL}(2,\mathbb{F}_2)$ is not a Zassenhaus group.

Furthermore we see that:

$$\mathrm{PGL}(2,3) \cong S_4 \text{ and } \mathbb{P}^1(\mathbb{F}_3) = \{(1:0),(0:1),(1:1),(1:2)\}$$

Within S_4 we have a normal subgroup isomorfic to V_4 given by the following set:

$$\{(1),(12)(34),(13)(24),(14)(23)\}$$

This subgroup acts regularly on $\{1,2,3,4\}$. As a consequence the corresponding subgroup within $\mathrm{PGL}(2,3)$ acts regularly on $\mathbb{P}^1(\mathbb{F}_3)$. Hence $\mathrm{PGL}(2,3)$ does contain a regular normal subgroup and is not a Zassenhaus group.

Suppose $q > 3$ such that q is a power of 2. Then $\mathrm{PSL}(2,q) = \mathrm{PGL}(2,q)$ by proposition 1.22. We now prove that $\mathrm{PSL}(2,q)$ is a Zassenhaus group if $q > 3$ and not a power of 2.

Proposition 1.27. *If $p > 2$ and $q = p^k > 3$ then $PSL(2, q)$ acting on $\mathbb{P}^1(\mathbb{F}_q)$ is a Zassenhaus group.*

Proof. We already showed that $\mathrm{PSL}(2, q)$ is simple and that it is 2-transitive. In the proof of the previous proposition we showed that every non trivial element in $\mathrm{PGL}(2, q)$ fixes at most 2 points. Since $\mathrm{PSL}(2, q)$ can be regarded as a subgroup of $\mathrm{PGL}(2, q)$ the non trivial elements in $\mathrm{PSL}(2, q)$ fix at most 2 points of $\mathbb{P}^1(\mathbb{F}_q)$. We conclude that $\mathrm{PSL}(2, q)$ is a Zassenhaus group for $q > 3$. □

1.3 Semilinear groups

In order to construct another Zassenhaus group it is not enough to look at projective special/general linear groups. In the following we will construct the (projective) semilinear group.

Definition 1.28. Let V, W be vector spaces over a field K. Let θ be an automorfism of K. A function $f : V \to W$ is said to be θ-semilinear, or simply semilinear, if for all $x, y \in V$ and $\lambda \in K$ the following holds:

1. $f(x + y) = f(x) + f(y)$
2. $f(\lambda x) = \theta(\lambda) f(x)$

Lemma 1.29. *Let V and W be K vector spaces. Suppose that $f : V \to W$ is θ-semilinear. Then θ fixes the prime subfield k of K, i.e. $\theta \in Aut_k(K)$.*

Proof. For all non-negative integers n and $x \in V$ we have:

$$\theta(n) f(x) = f(nx) = nf(x)$$

It follows that θ fixes the prime subfield of K. □

Definition 1.30. Suppose V is a K vector space. The set of all invertible semilinear maps of V is defined to be the *general semilinear group*, denoted $\Gamma\mathrm{L}(V)$.

Definition 1.31. Let V be vector space over a field K. The *projective semilinear group* of V, denoted $\mathrm{P\Gamma L}(V)$, is defined to be:

$$\mathrm{P\Gamma L}(V) := \Gamma\mathrm{L}(V)/\mathrm{Z}(V)$$

Proposition 1.32. *Suppose V is a vector space over a field K. Let k be the prime subfield of K. Then $\Gamma L(V)$ decomposes as the following semidirect product:*

$$\Gamma L(V) = GL(V) \rtimes Aut_k(K)$$

Proof. Let B be a basis of V. We identify an element $\theta \in \mathrm{Aut}_k(K)$ with the map $\sum_{b \in B} \lambda_b b \mapsto \sum_{b \in B} \theta(\lambda_b) b$.

Let $f \in \Gamma\mathrm{L}(V)$ be θ-semilinear. Define $g : V \to V$ by:

$$g\left(\sum_{b \in B} \lambda_b b\right) := \sum_{b \in B} \lambda_b f(b)$$

Remark that the image of B under f is again a basis of V. As a consequence g is linear and invertible, i.e. $g \in \mathrm{GL}(V)$. Let $h := fg^{-1}$. For $v = \sum_{b\in B} \lambda_b b \in V$ we see that:

$$fg^{-1}v = \sum_{b\in B} \theta(\lambda_b)b$$

In other words: $fg^{-1} \in \mathrm{Aut}_k(K)$.

Since $\mathrm{GL}(V)$ is normalized by $\mathrm{Aut}_k(K)$ it follows that $\Gamma\mathrm{L}(V)$ decomposes as the given semidirect product. □

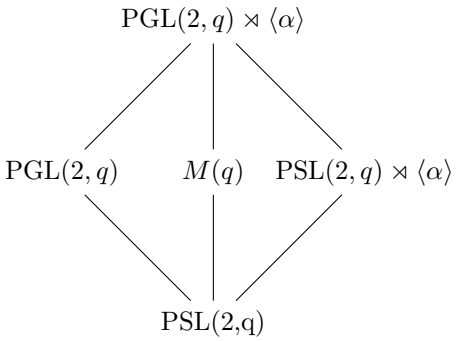
Corollary 1.33. *Suppose V is a vector space over a field K. Let k be the prime subfield of K.Then $P\Gamma L(V)$ decomposes as the follwing semidirect product:*

$$P\Gamma L(V) = PGL(V) \rtimes Aut_k(K)$$

Remark that elements from $\Gamma\mathrm{L}(V)$ map 1-dimensional subspaces (of V) to 1-dimensional subspaces. As a consequence $\mathrm{P\Gamma L}(V)$ acts on $\mathbb{P}(V)$.

We introduce the following notation. If V is an n-dimensional vector space over $\mathbb{F}_q$, then we write $\mathrm{P\Gamma L}(n, q)$ and $\Gamma\mathrm{L}(n, q)$ for $\mathrm{P\Gamma L}(V)$ and $\Gamma\mathrm{L}(V)$, respectively.

We will now construct another Zassenhaus group. Let p be a prime such that $p > 2$ and $m \in \mathbb{Z}_{\geq 1}$. Now consider the field $\mathbb{F}_q$ with $q = p^{2m}$. This field has an automorfism of order 2. That is: $\alpha : \mathbb{F}_q \to \mathbb{F}_q$ with $\alpha(x) = x^{p^m}$. Let $H := \mathrm{PGL}(2, q) \rtimes \langle\alpha\rangle$. This group H can be viewed as a subgroup of $\mathrm{P\Gamma L}(2, q)$ via the previous corollary. Since $p > 2$ we have that $[\mathrm{PGL}(2, q) : \mathrm{PSL}(2, q)] = 2$ by proposition 1.22. Thus within H we already have two subgroups of index 2, namely $\mathrm{PSL}(2, q) \rtimes \langle\alpha\rangle$ and $\mathrm{PGL}(2, q)$. Remark that $H/\mathrm{PSL}(2, q)$ has 4 elements. Combining this with the fact that H has at least two different subgroups of index 2, we must have that $H/\mathrm{PSL}(2, q) \cong V_4$. From this follows that H must have another subgroup of index 2, different from $\mathrm{PSL}(2, q) \rtimes \langle\alpha\rangle$ and $\mathrm{PGL}(2, q)$. We call this subgroup $M(q)$. This gives the following diagram:



Proposition 1.34. *$M(q)$ with $q = p^{2m}$, $p > 2$ and $m \in \mathbb{Z}_{\geq 1}$ acting on $\mathbb{P}^1(\mathbb{F}_q)$is a Zassenhaus group.*

Proof. Since $\mathrm{PSL}(2, q) < M(q)$ it follows that $M(q)$ is doubly transitive. Because $\mathrm{PSL}(2, q)$ is simple, $M(q)$ does not contain a regular normal subgroup.
In order to prove the third Zassenhaus property we need to comprehend $M(q)$

a little bit better. Remark that every element in $M(q)$ is of the form: $h \cdot \beta$ with $\beta \in \{1, \alpha\}$ and $h \in \mathrm{PGL}(2,q)$.

We already noted that $(\mathrm{PGL}(2,q) \rtimes \langle\alpha\rangle)/\mathrm{PSL}(2,q) \cong V_4$. Let $f \in \mathrm{PGL}(2,q) \setminus \mathrm{PSL}(2,q)$ then $\overline{f}$ is the non trivial element in $\mathrm{PGL}(2,q)/\mathrm{PSL}(2,q)$. We see that $\overline{\alpha}$ is the non trivial element in $(\mathrm{PSL}(2,q) \rtimes \langle\alpha\rangle)/\mathrm{PSL}(2,q)$. As a consequence, the non trivial element in $M(q)/\mathrm{PSL}(2,q)$ is $\overline{f \cdot \alpha}$. Hence:

$$M(q) = \mathrm{PSL}(2,q) \cup \mathrm{PSL}(2,q) \cdot f \cdot \alpha$$

Using propositin 1.22 we thus find that for every $h \cdot \beta \in M(q)$ we have $\det(h) \in \mathbb{F}_q^2$ and $\beta = 1$ or $\det(h) \notin \mathbb{F}_q^2$ and $\beta = \alpha$. (†)

Now we will consider the stabilizer of the points $(1:0)$ and $(0:1)$ within $M(q)$. Remark that α leaves these points fixed. Suppose an element $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}(2,q)$ fixes $(1:0)$ and $(0:1)$ then $b = c = 0$. Furthermore, we may assume that $d = 1$ by definition of PGL. As a consequence this stabilizer consists of all maps of the form $h \cdot \beta$ with $h = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ and $\beta \in \{1, \alpha\}$.

Suppose we have another point $(x:1)$ with $x \neq 0$. Let $h \cdot \beta$ be in the stabilizer of $\{(1:0), (0:1), (x:1)\}$. As a consequence we need to have $x = a \cdot \beta(x)$. If $\beta = 1$ then $a = 1$. This implies that $h \cdot \beta = 1$. If $\beta = \alpha$ we have the following:

$$a = x \cdot \alpha(x)^{-1} = x^{1-p^m}$$

Since $p > 2$ we see that $1 - p^m$ is divisible by 2. This means that $a = x^{1-p^m} \in \mathbb{F}_q^2$. This however contradicts (†) and as a result this three point stabilizer is trivial. By the 2-transitivity all the 2-point stabilizers are conjugate. This fact combined with our discussion above gives that every three-point stabilizer is trivial. □

Theorem 1. *Every Zassenhaus group is either one of the groups mentioned in Propositions 1.26 , 1.27 , 1.34 or one of the Suzuki groups.*

The proof of this theorem is beyond the scope of this bachelor thesis and can be found in [3], Chapter 11.

As stated in the introduction, the proof of this classification contained work from Feit, Ito and Suzuki. The proof contained three essential steps. Firstly, Feit showed that the degree of a Zassenhaus group is always of the form $q + 1$, with q a prime power. Next, Ito showed that for q odd the Zassenhaus group in question has to contain a normal subgroup isomorfic to $\mathrm{PSL}(2,q)$ with index 1 or 2. To conclude, Suzuki dealt with the case where q is even.

2 Wilson's approach to Suzuki groups

2.1 Definition of the group and action

Definition 2.1. Let V be a vector space over a field F. A bilinear form $f : V \times V \to F$ is said to be a *symplectic form* if it is:

1. Alternating: $f(v, v) = 0$ for all $v \in V$.
2. Nondegenerate: $f(u, v) = 0$ for all $v \in V$ implies $u = 0$.

Definition 2.2. Let V be a vector space over F with a symplectic form f. The *symplectic group* of (V, f) is defined to be:

$$\mathrm{Sp}(V, f) := \{g \in \mathrm{End}(V) : \forall v, w \in V \quad f(g(v), g(w)) = f(v, w)\}$$

Lemma 2.3. *If* $\dim(V) < \infty$ *then the symplectic group of* (V, f) *is a group under composition and thus a subgroup of Aut(V).*

Proof. Suppose $g \in \mathrm{Sp}(V, f)$ and $v \in \ker(g)$. For all $u \in V$ we have:

$$f(u, v) = f(g(u), g(v)) = f(g(u), 0) = 0$$

Since g is nondegenerate we have $v = 0$. Because V is of finite dimension g must be an automorphism. The remainder of the claim is trivial to prove. □

Definition 2.4. Let V be a vector space over a field F. Let $\bullet$ be a product defined on V, that is a map $\bullet : V \times V \to V$. Write $v \bullet w$ for $\bullet(v, w)$. This product is called a bi-semilinear commutative product if the following conditions are satisfied:

1. $v \bullet w = w \bullet v$ for all $v, w \in V$.
2. $(v + w) \bullet z = v \bullet z + w \bullet z$ for all $v, w, z \in V$.
3. There is a $\sigma \in \mathrm{Aut}(F)$ such that $(\lambda v) \bullet w = \sigma(\lambda)(v \bullet w)$ for all $\lambda \in F$ and $v, w \in V$.

If $v \in V \setminus \{0\}$, denote the linear subspace generated by v by $\langle v \rangle$.

Definition 2.5. Let V be a vector space over a field F of finite dimension. Furthermore, let f be a symplectic form on V and $\bullet$ a bi-semilinear commutative product on V. Define:

$$G(V, f, \bullet) := \left\{ g \in \mathrm{End}(V) : \begin{array}{l} \forall v, w \in V \quad f(g(v), g(w)) = f(v, w) \\ \text{and } f(v, w) = 0 \Rightarrow g(v) \bullet g(w) = g(v \bullet w) \end{array} \right\}$$

$$X(V, f, \bullet) := \{\langle v \rangle : v \in V \setminus \{0\} \text{ and } \exists w \in V \text{ with } v = v \bullet w \text{ and } f(v, w) = 0\}$$

Remark. We see that $G(V, f, \bullet)$ is a subgroup of the symplectic group of (V, f) and that it acts on $X(V, f, \bullet)$.

For $n \in \mathbb{Z}_{\geq 0}$ take $F = \mathbb{F}_q$ with $q = 2^{2n+1}$. For this particular field there is a $\sigma \in \mathrm{Aut}(F)$ such that $\sigma^2(x) = x^2$. This is $\sigma : F \to F$ with $\sigma(x) = x^{2^{n+1}}$. We see that $\sigma^2(x) = x^{2^{2n+2}} = \left(x^{2^{2n+1}}\right)^2 = x^2$. One could say that σ is a square root of the Frobenius map on F. Now let τ be the inverse of σ. If $n \geq 1$ then τ is the following map $\tau : F \to F$ with $\tau(x) = x^{2^n}$. From now we will write x^σ for $\sigma(x)$ and x^τ for $\tau(x)$.

Define V to be the 4-dimensional vector space over F with basis $\{e_{-2}, e_{-1}, e_1, e_2\}$.

Now we define a bilinear form $f : V \times V \to F$ such that $f(e_{-i}, e_i) = 1$ and $f(e_i, e_j) = 0$ otherwise. Remark that this f is a symplectic form since $\mathrm{char}(F) = 2$.

Futhermore, let θ be the order preserving bijection from $\{-3, -1, 1, 3\}$ to $\{-2, -1, 1, 2\}$. Now define a commutative product: $\bullet : V \times V \to V$ in the following way;
First on the basis:

$$e_i \bullet e_j = \begin{cases} 0 & \text{if } i = \pm j \\ e_{\theta(i+j)} & \text{otherwise} \end{cases}$$

Extend this by the following rule:

$$\left(\sum_i \lambda_i e_i\right) \bullet \left(\sum_j \mu_j e_j\right) = \sum_{i,j} \sigma^{-1}(\lambda_i \mu_j)\,(e_i \bullet e_j)$$

We see that this product is bi-semilinear and commutative.

Definition 2.6. For $n \in \mathbb{Z}_{\geq 0}$ define $F = \mathbb{F}_q$ with $q = 2^{2n+1}$ as above. Furthermore, let V, f and $\bullet$ be as above. Then we define the Suzuki group (for this n), denoted as $\mathrm{Suz}(2^{2n+1})$, in the following way:

$$\mathrm{Suz}(2^{2n+1}) := G(V, f, \bullet)$$

The Suzuki groups will act on $\mathrm{Ov}(2^{2n+1}) := X(V, f, \bullet)$.

In the remainder of this chapter V, F, f and $\bullet$ will keep this definition and $q = 2^{2n+1}$ for a certain $n \in \mathbb{Z}_{\geq 0}$.

We will show for all $n \in \mathbb{Z}_{\geq 1}$ that $\mathrm{Suz}(2^{2n+1})$ is a Zassenhaus group.

2.2 The elements of $\mathbf{Suz}(q)$

Lemma 2.7. *Let $g \in Aut(V)$. Suppose g satisfies the following conditions:*

1. *g preserves our form f with respect to the given basis of V. That is:*

$$f(g(e_i), g(e_j)) = f(e_i, e_j) \quad \forall i, j \in \{-2, -1, 1, 2\}$$

2. *g preserves our product $\bullet$ with respect to all perpendicular basisvectors. That is:*

$$f(e_i, e_j) = 0 \quad \Rightarrow \quad g(e_i) \bullet g(e_j) = g(e_i \bullet e_j)$$

Then $g \in Suz(q)$.

Proof. Since f is bilinear 1. clearly implies that $f(g(v), g(w)) = f(v, w)$ for all $v, w \in V$. Remark that $\bullet$ induces a map $\pi : V \wedge V \to V$ with $\pi(u \wedge w) = u \bullet w$ and extending linearly. In order to show that g leaves π invariant it suffices to check this on a basis of $V \wedge V$. Hence 2. implies that $g(u \bullet v) = g(u) \bullet g(v)$ for all perpendicular vectors. □

In order to understand Suz(q) we need to have some key elements in Suz(q).

- Consider the map that extends the following basis permutation in a linear way: $e_i \mapsto e_{-i}$. Remark that the construction of Suz(q) is symmetric in e_i, e_{-i} and thus this map is certainly contained in Suz(q). We will denote this map by W and with respect to the basis $\{e_{-2}, e_{-1}, e_1, e_2\}$ it can be written in the following way:

$$W := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

- Now we will look for maps in Suz(q) which can be identified with diagonal matrices. These are maps of the following form:

$$\sum_i \alpha_i e_i \mapsto \sum_i \lambda_i \alpha_i e_i$$

  In order to preserve f we need to have that $\lambda_{-i} = \lambda_i^{-1}$. We also need to preserve the dotproduct so there has to hold that: $(\lambda_1 e_1) \bullet (\lambda_2 e_2) = \lambda_2 e_2$, or equivalently $(\lambda_1 \lambda_2)^\tau = \lambda_2$. From this follows that $\lambda_1 = \lambda_2^{\sigma-1}$. So if we fix one λ_i the entire map is fixed by the following rules.

$$\lambda_{-i} = \lambda_i^{-1} \quad \text{and} \quad \lambda_1 = \lambda_2^{\sigma-1}$$

  One now easily checks that the rest of the dotproducts on the basis are also preserved. So for every $\lambda \in F^*$ there is a diagonal element in Suz(q), therefore there are $q - 1$ diagonal elements in Suz(q). Remark that this subgroup of Suz(q) is cyclic because F^* is cyclic. These diagonal maps $h(\lambda)$ can be written in matrix form:

$$h(\lambda) = \begin{pmatrix} \lambda^{-1} & 0 & 0 & 0 \\ 0 & \lambda^{-\sigma+1} & 0 & 0 \\ 0 & 0 & \lambda^{\sigma-1} & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

- The following element is a bit of a surprise:

$$\begin{aligned} e_{-2} &\mapsto e_{-2} \\ e_{-1} &\mapsto e_{-1} + e_{-2} \\ e_1 &\mapsto e_1 + e_{-1} \\ e_2 &\mapsto e_2 + e_1 + e_{-1} + e_{-2} \end{aligned}$$

We shall call this map x. By lemma 2.7 It suffices to check on the basis that this map preserves f and the dotproduct (for perpendicular basisvectors). This is a straightforward check. This map has the following matrix representation:

$$x = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad x^2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

For our future endeavours it is convenient to calculate the following conjugates of x and x^2:

$$h(\lambda)^{-1}x^2h(\lambda) = \begin{pmatrix} 1 & 0 & \lambda^\sigma & \lambda^2 \\ 0 & 1 & 0 & \lambda^\sigma \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$h(\lambda)^{-1}xh(\lambda) = \begin{pmatrix} 1 & ... & ... & ... \\ 0 & 1 & ... & ... \\ 0 & 0 & 1 & \lambda^{2-\sigma} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

For our purposes it is sufficient to have the matrix $h(\lambda)^{-1}xh(\lambda)$ partially. We do not need the dotted entries.

Let ω be a generator for F^* then $\langle h(\omega)\rangle$ contains all diagonal matrices within $\mathrm{Suz}(q)$. Thus we have:

$$\langle W, h(\omega), x\rangle \subset \mathrm{Suz}(q)$$

2.3 The elements of $\mathbf{Ov}(q)$

Definition 2.8. Let $v \in V \setminus \{0\}$ with $v = \sum_i \lambda_i e_i$ then:

$$\deg(v) := \max\{i : \lambda_i \neq 0\} \text{ and } \deg\langle v\rangle := \deg(v)$$

Remark. We see that $\deg\langle v\rangle$ is well defined.

Proposition 2.9. *If $\langle v\rangle \in Ov(q)$ then $\deg\langle v\rangle = \pm 2$.*

Proof. Because $\langle v\rangle \in \mathrm{Ov}(q)$ there exists $w \in V$ with $f(v,w) = 0$ and $v \bullet w = v$. Hence we have $\deg(v \bullet w) = \deg(v)$ and $w \neq 0$. We would like to show that $\deg(v \bullet w) = \theta(\deg(v) + \deg(w))$. Considering the definition of the $\bullet$ and the fact that θ is order preserving it is clear that this equality holds unless $\deg(v) = \pm\deg(w)$. We now show that we may assume that $\deg(v) \neq \pm\deg(w)$.

If $\deg(w) = \deg(v)$ take $\lambda \in F$ such that $\deg(w') < \deg(v)$ with $w' := w + \lambda v$. Remark that $f(v,v) = 0$ and $v \bullet v = 0$. As a consequence:

$$f(v,w') = f(v, w + \lambda v) = f(v,w) + \lambda f(v,v) = 0$$

$$v \bullet w' = v \bullet (w + \lambda v) = v \bullet w + \lambda^\tau (v \bullet v) = v \bullet w = v$$

Hence $f(v, w') = 0$ and $v \bullet w' = v$. Thus without loss of generality we may assume $\deg(w) \neq \deg(v)$.

Now suppose that $\deg(v) = -\deg(w)$. Then it follows that $f(v, w) \neq 0$. This can be seen by just working out the different cases. Hence we may assume, without loss of generality, that $\deg(v) \neq \pm \deg(w)$.

Thus we have:

$$\theta(\deg(v) + \deg(w)) = \deg(v \bullet w) = \deg(v)$$

Assume $\deg\langle v\rangle = \pm 1$, then we would have that $\deg(v) + \deg(w) = \deg(v)$ since θ is the identity on $\{-1, 1\}$. As a result we must have that $\deg(w) = 0$. This contradicts the fact that w is non zero. □

If $\deg\langle v\rangle = -2$ we have that $\langle v\rangle = \langle e_{-2}\rangle$. Therefore it is more interesting to look at the case of: $\deg\langle v\rangle = 2$. We characterise the points of degree 2 with the following proposition.

Proposition 2.10. *(i) For all $\alpha, \beta \in F$ there is a unique $\gamma \in F$ such that:*

$$\langle e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}\rangle \in Ov(q).$$

(ii) The group Suz(q) acts transitively on Ov(q).

Proof. Suppose $\langle v\rangle \in \mathrm{Ov}(q)$ with $\deg\langle v\rangle = 2$. Thus we can write $v = e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}$ with $\alpha, \beta, \gamma \in F$.
We claim that $2 - \sigma$ is a bijection from F to F. To see this, remark that: $2 - \sigma = \sigma(\sigma - 1)$. Furthermore $(\sigma - 1)$ is an automorfism because $(\sigma + 1)$ is it's inverse. Hence $2 - \sigma$ is, as composition of two bijections, a bijection.

If $\alpha \neq 0$, take $\lambda \in F$ such that $\lambda^{2-\sigma} = \alpha$. Hence follows:

$$h(\lambda)^{-1} x h(\lambda) \cdot v = e_2 + \beta' e_{-1} + \gamma' e_{-2} := v'$$

If $\beta' \neq 0$, take $\kappa \in F$ such that $\kappa^\sigma = \beta'$. Then we see:

$$h(\kappa)^{-1} x^2 h(\kappa) \cdot v' = e_2 + \gamma'' e_{-2} := v''$$

Consequently we see that the vector v'' is of the form $e_2 + \mu e_{-2}$ and $\langle v''\rangle \in \mathrm{Ov}(q)$. This means that there exists $w \in V$ with $f(v'', w) = 0$ and $v'' \bullet w = v''$. As we saw in the proof of the previous proposition, w can be chosen such that $\deg(w) \neq \deg(v)$ and thus w has no term in e_2. So w is of the following form: $w = e_1 + \delta e_{-1} + \xi e_{-2}$. We have that $0 = f(v'', w) = \xi$. Thus $w = e_1 + \delta e_{-1}$. As a consequence we see:

$$v'' \bullet w = e_2 + \delta^{2^n} e_1 + \mu^{2^n} e_{-1} + (\mu\delta)^{2^n} e_{-2}$$

We conclude that $\mu = 0$ and thus $\langle v''\rangle = \langle e_2\rangle$. Remark that $\langle e_2\rangle$ goes to $\langle e_{-2}\rangle$ under the element W of $\mathrm{Suz}(q)$. Hence all elements of $\mathrm{Ov}(q)$ are in the orbit of $\langle e_2\rangle$ and thus $\mathrm{Suz}(q)$ works transitively on $\mathrm{Ov}(q)$. We also see that, given α and β there is at most one $\gamma \in F$ such that $\langle e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}\rangle \in \mathrm{Ov}(q)$.

Let α, β be given and consider $e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}$. By the process above there is a $k \in \langle h(\omega), x \rangle$, independent of the choice of γ, such that k maps $e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}$ to $e_2 + \mu e_{-2}$ for some $\mu \in F$. Since k is an automorphism we have that the following restriction of k is a bijection:

$$k' : \{e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2} : \gamma \in F\} \to \{e_2 + \mu e_{-2} : \mu \in F\}$$

$$v \mapsto k(v)$$

Hence there is a $\gamma \in F$ such that $e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}$ is mapped to e_2 by k and it follows that $\langle e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2} \rangle \in \mathrm{Ov}(q)$. This proves that for all $\alpha, \beta \in F$ there is a unique $\gamma \in F$ such that:

$$\langle e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2} \rangle \in \mathrm{Ov}(q)$$

□

Corollary 2.11. *For all $\alpha, \beta \in F$ there is a unique $\gamma \in F$ such that there exists an element in $\langle h(\omega), x \rangle$ that sends e_2 to $e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}$.*

We conclude that there are q^2 points of degree 2 and one point of degree -2 if $F = \mathbb{F}_q$ and thus $\mathrm{Ov}(q)$ consists of $q^2 + 1$ elements.

2.4 2-transitivity

There is a well known theorem about 2-transitivity which immediately gives that $\mathrm{Suz}(q)$ works 2-transitively on $\mathrm{Ov}(q)$.

Lemma 2.12. *Let G act on X with $\#X \geq 2$. Fix $x_0 \in X$. The action is 2-transitive if and only if it is transitive and $Stab_{x_0}$ acts transitively on $X \setminus \{x_0\}$.*

Proof. Suppose the action is 2-transitive. Then is clear that Stab_{x_0} acts transitively on $X \setminus \{x_0\}$ and the action is obviously transitive. This proves the first implication.

Now suppose that the action is transitive and Stab_{x_0} acts transitively on $X \setminus \{x_0\}$. If $\#X = 2$ then every non-trivial action of G is doubly transitive. Since transitive actions are non-trivial, the action is doubly transitive if $\#X = 2$. Hence we may and do assume that $\#X \geq 3$. Firstly, we will show that for every $y \in X$ the action of Stab_y acts transitively on $X \setminus \{y\}$. The 2-transitivity will follow from this.

Therefore, let $y \in X$. By the transitivity there is a $g \in G$ such that $gx_0 = y$. As a consequence we have that $\mathrm{Stab}_y = g\,\mathrm{Stab}_{x_0}\, g^{-1}$. Let $a, b \in X \setminus \{y\}$ then the elements $g^{-1}a$ and $g^{-1}b$ are distinct from $g^{-1}y = x_0$. By assumption there is an element $h \in \mathrm{Stab}_{x_0}$ such that $hg^{-1}a = g^{-1}b$. From this follows that $ghg^{-1}a = b$. Now remark that $ghg^{-1} \in g\,\mathrm{Stab}_{x_0}\, g^{-1} = \mathrm{Stab}_y$. This shows that Stab_y acts transitively on $X \setminus \{y\}$.

Let $(x_1, x_2), (y_1, y_2) \in X \times X$ such that $x_1 \neq x_2$ and $y_1 \neq y_2$. If $y_2 \neq x_1$ there is an element in Stab_{x_1} which maps (x_1, x_2) to (x_1, y_2). Now there is an element in Stab_{y_2} which maps (x_1, y_2) to (y_1, y_2). Thus we can map (x_1, x_2) to (y_1, y_2). If $x_1 = y_2$, then we choose $z \in X$ such that z is not equal to x_1 or y_1. Here we use that $\#X \geq 3$. Now use elements from Stab_z, Stab_{x_1} and Stab_{y_1} to obtain:

$$(x_1, x_2) \mapsto (x_1, z) \mapsto (y_1, z) \mapsto (y_1, y_2)$$

We conclude that the action is doubly transitive. □

Theorem 2. *Suz(q) acts doubly transitively on Ov(q).*

Proof. We already saw that $\mathrm{Suz}(q)$ acts transitively on $\mathrm{Ov}(q)$. Fix $\langle e_{-2}\rangle \in \mathrm{Ov}(q)$ and remark that $\langle h(\omega), x\rangle \subset \mathrm{Stab}_{\langle e_{-2}\rangle}$. We also saw that every element of degree 2 can be mapped to $\langle e_2\rangle$ by an element from $\langle h(\omega), x\rangle$ and thus $\mathrm{Stab}_{\langle e_{-2}\rangle}$ acts transitively on $\mathrm{Ov}(q) \setminus \{\langle e_{-2}\rangle\}$. By the previous lemma, $\mathrm{Suz}(q)$ acts doubly transitively on $\mathrm{Ov}(q)$. □

Proposition 2.13. *Suppose we have $g \in Suz(q)$ such that g is contained in the stabilizer of $\langle e_2\rangle$ and $\langle e_{-2}\rangle$ then $g \in \langle h(\omega)\rangle$.*

Proof. Let g be in the stabilizer of the points $\langle e_2\rangle$ and $\langle e_{-2}\rangle$. At first remark that $\langle e_2\rangle^\perp = \{v \in V : f(v, e_2) = 0\}$ is linear subspace of V. Since g fixes $\langle e_2\rangle$ we have that $g(e_2) = \lambda e_2$ for a certain $\lambda \in F$. If $v \in \langle e_2\rangle^\perp$ we have that:

$$0 = f(v, e_2) = f(g(v), g(e_2)) = f(g(v), \lambda e_2) = \lambda \cdot f(g(v), e_2)$$

And thus $g(v) \in \langle e_2\rangle^\perp$. Hence we see that $\langle e_2\rangle^\perp = \langle e_1, e_{-1}, e_2\rangle$ is fixed by g.

Consider the following set:

$$e_2 \bullet V = \{e_2 \bullet v : v \in V \text{ and } f(e_2, v) = 0\} = \langle e_1, e_2\rangle$$

Hence follows:

$$g(e_2 \bullet V) = \{e_2 \bullet g(v) : v \in V \text{ and } f(e_2, g(v)) = 0\} = \langle e_1, e_2\rangle$$

Therefore, $\langle e_1, e_2\rangle$ is also fixed by g. Now g must also fix the intersection of the sets $\langle e_1, e_2\rangle$ and $\langle e_1, e_{-1}, e_{-2}\rangle$. We conclude that $\langle e_1\rangle$ is fixed by the two-point stabilizer. With an analogous argument, one sees that $\langle e_{-1}\rangle$ is fixed by g. Hence the elements in this two-point stabilizer are precisely the diagonal elements in $\mathrm{Suz}(q)$. □

Corollary 2.14. *Suz(q) consists of $(q-1)q^2(q^2+1)$ elements if $F = \mathbb{F}_q$.*

Proof. This follows from the previous proposition together with the 2-transitivity. □

Corollary 2.15. *Suz(q) = $\langle W, h(\omega), x\rangle$*

Proof. Let $g \in \mathrm{Stab}_{\langle e_{-2}\rangle}$. There is an element $d \in \langle h(\omega), x\rangle$ such that gd stabilizes $\langle e_2\rangle$. By proposition 2.13 gd must lie in $\langle h(\omega)\rangle$. Hence $g \in \langle h(\omega), x\rangle$. Consequently we have $\langle h(\omega), x\rangle = \mathrm{Stab}_{\langle e_{-2}\rangle}$. By proposition 1.9 $\mathrm{Stab}_{\langle e_{-2}\rangle}$ is maximal. Since $W \notin \mathrm{Stab}_{\langle e_{-2}\rangle}$ we conclude that:

$$\mathrm{Suz}(q) = \langle W, h(\omega), x\rangle$$

□

2.5 Three-point stabilizers

Theorem 3. *Non-trivial elements in Suz(q) fix at most 2 points of Ov(q).*

Proof. By the 2-transitivity all 2-point stabilizers within $\mathrm{Suz}(q)$ are conjugate. Consider the stabilizer of $(\langle e_2\rangle, \langle e_{-2}\rangle)$. We already saw that this stabilizer is precisely the group of diagonal elements in $\mathrm{Suz}(q)$. Let $z \in \mathrm{Ov}(q)$ be a point different from $\langle e_2\rangle$ and $\langle e_{-2}\rangle$. We will now show that the 3-point stabilizer of $(\langle e_2\rangle, \langle e_{-2}\rangle, z)$ is trivial. This implies that every three-point stabilizer is trivial because all 2-point stabilizers are conjugate.

Since z is a different point we must have that $z = \langle e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}\rangle$ with α or β non zero. An element in this three-point stabilizer must be diagonal, thus suppose that $h(\lambda)$ stabilizes these three points. As we know $h(\lambda)$ acts in the following way on the points $e_2, e_{-2}, e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}$:

$$e_2 \mapsto \lambda e_2 \tag{1}$$

$$e_{-2} \mapsto \lambda^{-1} e_{-2} \tag{2}$$

$$e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2} \mapsto \lambda e_2 + \lambda^{\sigma-1}\alpha e_1 + \lambda^{1-\sigma}\beta e_{-1} + \lambda^{-1}\gamma e_{-2} \tag{3}$$

Suppose α is non zero. Because $\langle e_2 + \alpha e_1 + \beta e_{-1} + \gamma e_{-2}\rangle$ is also fixed by $h(\lambda)$ we need to have that:

$$\lambda = \lambda^{\sigma-1}$$

From this follows that $1 = \lambda^{\sigma-2}$. In section 2.3 we saw that $\sigma - 2$ is an automorfism of F and thus $\lambda = 1$. With an analogous argument the same can be proven if β is non zero.

Consequently, the only element contained in this 3-point stabilizer is the trivial element of $\mathrm{Suz}(q)$. Therefore, non trivial points in $\mathrm{Suz}(q)$ fix at most 2 points of $\mathrm{Ov}(q)$. □

Corollary 2.16. *Suz(q) acts faithfully on Ov(q).*

2.6 Simplicity of Suz(q)

Theorem 4. *Suz(q) is simple for $q > 2$.*

Proof. We will show that $\mathrm{Suz}(q)$ satisfies the conditions in Proposition 1.13.

- $\mathrm{Suz}(q)$ acts faithfully on $\mathrm{Ov}(q)$ by corollary 2.16.
- Since $\mathrm{Suz}(q)$ acts doubly transitively on $\mathrm{Ov}(q)$ it follows that the action of $\mathrm{Suz}(q)$ on $\mathrm{Ov}(q)$ is primitive.
- Since $q > 2$ we see that $\langle h(\omega)\rangle$ is not just the trivial element. Hence follows:

  $$W^{-1}h(\lambda)^{-1}Wh(\lambda) = Wh(\lambda)^{-1}Wh(\lambda) = h(\lambda^2)$$

  As a consequence $\langle h(\omega)\rangle$ is contained in $[\mathrm{Suz}(q), \mathrm{Suz}(q)]$. As we already saw, the point stabilizer of $\langle e_{-2}\rangle$ is generated by conjugates from $\langle h(\omega)\rangle$. Hence this point stabilizer is contained in $[\mathrm{Suz}(q), \mathrm{Suz}(q)]$. Now we need to make a commutator which lies outside $\langle h(\omega), x\rangle$. Remark that all matrices

contained in$\langle h(\omega), x\rangle$ are upper traingular. When we calculate $[W, x]$ we see that this matrix is not upper traingular and thus not contained in $\langle h(\omega), x\rangle$. Since $\mathrm{Stab}_{\langle e_{-2}\rangle} = \langle h(\omega), x\rangle$ is maximal it follows that $[\mathrm{Suz}(q), \mathrm{Suz}(q)] = \mathrm{Suz}(q)$.

- Consider the point stabilizer $H := \mathrm{Stab}_{\langle e_{-2}\rangle}$. As we saw, the elements in H are upper traingular matrices. Hence H is solvable. Remark that $W^{-1}x^2W \notin H$. By the maximality of H we conclude that the conjugates of H generate $\mathrm{Suz}(q)$.

We conclude that $\mathrm{Suz}(q)$ is simple for $q > 2$. □

Combining theorems 2, 3 and 4 we find:

Theorem 5. *Suz(q) is a Zassenhaus group for $q > 2$.*

If $q = 2$ there is only one diagonal element contained in $\mathrm{Suz}(q)$ and thus $\langle h(\omega)\rangle = \{1\}$. As a consequence $\mathrm{Stab}_{\langle e_{-2}\rangle} = \langle x\rangle \cong C_4$. From this follows that $\mathrm{Suz}(2) = C_5 \rtimes C_4$ and thus contains $\mathrm{Suz}(2)$ a regular normal subgroup.

One should remark that definition 2.6 of the Suzuki group does not require that the field, F, over which we work is finite. Assume that F is a field such that:

- The characteristic of F is 2.
- The Frobenius map $\lambda \mapsto \lambda^2$ is an automorfism.
- F has an automofism σ which is a square root of the Frobenius automorfism.

Then we can define a Suzuki group for this F and this σ according to definition 2.6. The resulting group $\mathrm{Suz}(F)$ would still act doubly transitively on $\mathrm{Ov}(F)$ such that every non-trivial element fixes at most 2 points. Iwasawa's lemma is still applicable if the group in question is infinite and as a result $\mathrm{Suz}(F)$ is still simple.

References

[1] M. Suzuki, *Group Theory I.* Springer-Verlag, 1982.

[2] S. Lang, *Algebra.* Springer, revised third edition, 2002.

[3] B. Huppert, N. Blackburn, *Finite Groups III (Grundlehren Der Mathematischen Wissenschaften)* , Springer-Verlag, 1982.