LIST OF FINITE SIMPLE GROUPS

1. Background

This article assumes basic facts about K-algebras (such as tensor products, ideals, radical ideals), topological spaces (connectedness), and category theory.

Building on those foundations, the article gives a complete specification of all finite simple groups. The definition of a finite simple group of Lie type appears in Definition **??**. Unexplained notation from this section will be precisely defined later.

Theorem 1. *Every finite simple group is isomorphic to*

(1) *a cyclic group of prime order,*
(2) *an alternating group Alt_n on n letters for some $n \geq 5$,*
(3) *a finite simple group of Lie type, or*
(4) *one of the 26 sporadic groups.*

Every group these four families is a finite simple group.

Finite simple groups of Lie type are classified by certain data of the form (D_r, ρ, p, e) (written as ${}^{\rho}D_r(p^e)$), where D_r is a connected Dynkin diagram with r nodes, ρ is an arrow-forgetful isomorphism of the Dynkin diagram, p is a prime number, and $e \in \mathbb{Q}$ is an exponent. The explicit list of such tuples appears in Definition **??**.

Theorem 2. *If two finite simple groups on the list of Theorem* **??** *are isomorphic, then that isomorphism is one of the following duplicates.*

- $Alt_5 \simeq A_1(2^2) \simeq A_1(5)$.
- $Alt_6 \simeq A_1(3^2)$.
- $Alt_8 \simeq A_3(2)$.
- $A_1(7) \simeq A_2(2)$.
- $B_3(3) \simeq {}^2A_3(2)$.
- $B_r(2^m) \simeq C_r(2^m)$.

- *Any two finite simple groups of Lie type with isomorphic classifying data* (D, ρ, p, e) *are isomorphic.*

See [**?**].

2. Affine varieties

The material on finite groups of Lie type follows Carter [**?**] and Humphreys [**?**].

If I is an ideal of a ring R, the radical $\sqrt{I}$ of I is the set of all $f \in R$ such that $f^e \in I$ for some $e \geq 1$. The radical of I is an ideal.

Let K be an algebraically closed field. Let A_K be the set of finitely generated K-algebras without nilpotent elements. This can be made into a category, where the morphisms are morphisms of K-algebras, but this category will not be directly needed. An affine variety X over K is uniquely determined by an element of A_K.

An algebra $R \in A_K$ determines a set (the spectrum of R)

$$\mathrm{spec}(R) = \mathrm{Hom}_{K-alg}(R, K)$$

of K-algebra homomorphisms from R to K. The spectrum carries a topology (the Zariski topology) uniquely determined by the condition that a set Y is closed iff there exists a a subset S of R such that $Y = Z(S)$, where $Z(S)$ is the set of homomorphisms that vanish on S. We have $Z(S) = Z(\sqrt{(S)})$, where (S) is the ideal generated by S.

Although the data giving an affine variety X and the algebra R are one and the same, we make a conceptual distinction, thinking of X as a geometric object, which has a spectrum (written $X(K)$) and a coordinate ring (written $K[X] = R$). We also call $X(K)$ the set of K-points of X.

If Z is a closed subset of an affine variety X, then the subset $I(Z)$ on which every homomorphism in Z vanishes is a radical ideal. The Hilbert Nullstellensatz asserts that there is a bijection between closed subsets of X and radical ideals of $K[X]$ given by

$$Z \mapsto I(Z), \quad I \mapsto Z(I).$$

If Z is a closed subset of an affine variety X, then $K[X]/I(Z)$ is an algebra in A_K, and Z can be canonically identified with the spectrum of $K[X]/I(Z)$ via the composition of K-algebra homomorphisms

$$K[X] \to K[X]/I(Z) \to K.$$

In this way, each closed subset Z of X is an affine variety with coordinate ring $K[Z] = K[X]/I(Z)$.

If $R, R' \in A_K$, then $R \otimes R' \in A_K$. We have a product on affine varieties given by

$$K[X \times Y] = K[X] \otimes K[Y].$$

This product satisfies the universal property of a product. We warn that Zariski topology on the product is not the usual product topology in the theory of topological spaces.

A morphism $f : X \to Y$ of affine varieties is defined to be a K-algebra homomorphism $f^* : K[Y] \to K[X]$ (called the pull-back of coordinate functions). A morphism determines a map

$$f_* : X(K) \to Y(K),$$

by composition

$$K[Y] \to K[X] \to K.$$

This map is continuous. The data giving f and f^* are one and the same, but f^* is contravariant, and we make a conceptual distinction between them.

A point 1 is an affine variety with $K[1] = K$. It is a terminal object; for each affine variety there is a unique morphism $f : X \to 1$. Specifically, $f^* : K \to K[X]$ is the structure map of the K-algebra $K[X]$.

3. Affine algebraic groups

Henceforth we refer to a group in the usual sense as abstract groups to distinguish them from *affine groups*, which are group objects in the category of affine categories, which are described in this section.

We fix an algebraically closed field K. The objects from the categories of affine varieties and affine groups are all over this field K.

An affine group over K is defined as an affine variety G, together with morphisms $\mu : G \times G \to G$ (called multiplication) $i : G \to G$ (called inverse), and $e : 1 \to G$ (identity element) such that μ and i satisfy the usual axioms of a group. More precisely, we mean the axioms of a group in the category of affine algebraic groups.

For example, the right inverse property is that this diagram commutes: The other axioms are obtained by a similar translation of the group axioms into categorical language. The axioms are written explicitly in the Wiki article on group object [**?**]. (These axioms can also be expressed directly in A_K as the axioms of a Hopf algebra.)

If G is an affine group, then the corresponding operations on the spectrum

$$\mu_* : G(K) \times G(K) \to G(K), \quad e_*(1) \in G(K), \quad i_* : G(K) \to G(K)$$

make $G(K)$ into a group.

A morphism $f : G \to G'$ of affine algebraic groups is a morphism of affine varieties such that $f(xy) = f(x)f(y)$. That is, this diagram commutes: Unless stated otherwise, a morphism will mean a group homomorphism of affine algebraic groups.

The point 1 has the structure of an affine group.

If G and G' are affine groups, then $G \times G'$ also carries the structure of an affine group in a natural way.

A closed subgroup H of an affine group G is a closed subvariety that contains the neutral element and such that the inverse and multiplication on G restrict to H. Then H has the structure of an affine group. In what follows, being *closed* refers to the Zariski topology, but never to the algebraic sense in which a binary operation can be closed.

The kernel of a morphism $\psi : G \to H$ is the closed subset given by the preimage of $1 \in H$. The kernel of a morphism $\psi : G \to H$ is a closed subgroup of G. We define a normal subgroup of G to be any closed subgroup obtained as a kernel of a morphism.

An abelian group is an affine group such that

$$G \times G \to G \times G \to^{\mu} G$$

coincides with μ, where the first morphism swaps the factors.

A solvable group G is defined inductively as an affine group that is abelian, or as an affine group G that admits a morphism $\psi : G \to H$, where both H and the kernel of ψ are solvable.

An affine group G is connected, if it is connected as a topological space. A Borel subgroup of G is a maximal closed connected solvable subgroup of G.

Let G be an affine group. There exists an abelian affine group A (the abelianization of G) and morphism $G \to A$ with the following universal property: if A' is any affine abelian group, and morphism $\psi : G \to A'$, there exists a unique $A \to A'$ such that ψ is equal to $G \to A \to A'$. The kernel of $\phi : G \to A$ is the *closed derived* subgroup of G. The kernel does not depend on the choice of (A, ϕ).

Let G be an affine group and let H be a subgroup of G. A closed subgroup C of G *centralizes* H if the morphism of varieties

$$C \times H \to G, \quad (c, h) \to chc^{-1}$$

coincides with the inclusion $H \to G$. Among all closed subgroups C centralizing G, there exists a unique maximal element (under the ordering by inclusion of closed subsets of G). This is the centralizer $C_G(H)$ of H in G. The center $Z = Z_G$ of G is the centralizer in G of G:

$$Z = C_G(G).$$

We say that a closed subgroup N of G normalizes another closed subgroup H if the image of the morphism of varieties

$$N \times H \to G, \quad (n, h) \mapsto nhn^{-1}$$

lies in H. When N normalizes H, there is an action of N on H given by $(n, h) \mapsto nhn^{-1}$.

4. The general linear group

The most important example of an affine algebraic group for us is $GL(n)$ over K. Let $R = K[x_0, x_{ij} : i = 1, \ldots, n; j = 1, \ldots, n]$ be a polynomial ring in n^2+1 variables x_0 and x_{ij}. Let $\det(x_{ij}) \in R$ be the determinant in x_{ij}. Define $GL(n)$ as an affine variety by its coordinate ring: $K[GL(n)] = R/(x_0 \det(x_{ij}) - 1)$. We set $y_{ij} = x_{ij} \otimes 1$ and $z_{ij} = 1 \otimes x_{ij}$ in $K[GL(n) \times GL(n)]$. Then

$$K[GL(n)] \otimes K[GL(n)] \simeq K[y_0, y_{ij}, z_0, z_{ij}]/(y_0 \det(y_{ij}) - 1, z_0 \det(z_{ij}) - 1).$$

There exists a unique affine algebraic group $GL(n)$ with coordinate ring $K[GL(n)]$ and

$$\begin{aligned} e^*(x_{ij}) &= \delta_{ij} \text{ (Dirac delta function)}, & e^*(x_0) &= 1 \\ \mu^*(x_{ij}) &= \sum_{i=1}^{n} y_{ik} z_{kj}, & \mu^*(x_0) &= y_0 z_0 \\ i^* &= \text{adjugate formula for matrix inverse}, & i^*(x_0) &= \det(x_{ij}). \end{aligned}$$

The adjugate formula appears here [**?**].

If $a \in GL(n)(K) = GL(n, K) = \mathrm{Hom}_{K-alg}(K[GL(n)], K)$, we write a_{ij} for $a(x_{ij}) \in K$, and write it as an $n \times n$ matrix with coefficients in K. If $a_0 = a(x_0)$, then $a_0 \det(a_{ij}) = 1$, so that the determinant of the matrix is nonzero. In fact, the element x_0 appears exactly for the purpose of expressing the non-zero determinant condition as a polynomial equation.

4.1. **tori.** When $n = 1$, we also write $\mathbb{G}_m = GL(1)$. The coordinate ring is $K[t, u]/(tu - 1) \simeq K[t, t^{-1}]$. Also, $\mathbb{G}_m^r = \mathbb{G}_m \times \cdots \times \mathbb{G}_m$ for the r-fold product. The coordinate ring is

$$K[\mathbb{G}_m^r] = K[\mathbb{G}_m] \otimes \cdots \otimes K[\mathbb{G}_m] \simeq K[t_1, t_1^{-1}, \ldots, t_r, t_r^{-1}].$$

A closed subgroup T of G is a *maximal torus* if it is a subgroup isomorphic to $\mathbb{G}_m^r$, with $r \in \mathbb{N}$ maximal. We call r the rank of G. A maximal torus exists in every affine group.

Let T be a maximal torus of G. The character group of T is the set

$$X^*(T) = \mathrm{Hom}(T, \mathbb{G}_m).$$

It has the structure of (an abstract) abelian group as follows by multiplication in the target: if $\lambda_1, \lambda_2 \in X^*(T)$, then $(\lambda_1\lambda_2)(t) = \lambda_1(t)\lambda_2(t)$, for all $t \in T$. $X^*(T)$ is a free abelian group of rank r, when T is isomorphic to $\mathbb{G}_m^r$.

The cocharacter group of T is

$$X_*(T) = \mathrm{Hom}(\mathbb{G}_m, T),$$

It too has the structure of an abstract abelian group with multiplication in the target. $X_*(T)$ is a free abelian group of rank r.

There is a nondegenerate bilinear pairing

$$\langle \cdot, \cdot \rangle : X^*(T) \times X_*(T) \to \mathbb{Z},$$

given by the composition

$$\langle \lambda, \mu \rangle = \lambda \circ \mu \in \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}$$

4.2. **additive group.** The additive group $\mathbb{G}_a$ is the affine group whose coordinate ring is a polynomial ring in one variable $K[\mathbb{G}_a] = K[x]$. The group structure is uniquely determined by the conditions:

$$e^*(x) = 0, \quad i^*(x) = -x, \quad \mu^*(x) = x \otimes 1 + 1 \otimes x \in K[x] \otimes K[x].$$

The group $\mathbb{G}_m$ acts as automorphisms of $\mathbb{G}_a$ by the morphism

$$\mathbb{G}_m \times \mathbb{G}_a \to \mathbb{G}_a, \quad K[x] \to K[t, t^{-1}] \otimes K[x], \quad x \mapsto t \otimes x.$$

5. STRUCTURE THEORY FOR ALMOST SIMPLE GROUPS

An affine group is G is *almost simple* if it has no proper normal closed connected subgroup. An almost simple group is connected (because the connected component of the identity of any affine group is a normal closed connected subgroup).

We fix the context in the section. Let G be almost simple, let B be a Borel subgroup, let $U = B'$ be its closed derived subgroup, and let T be a maximal torus of G that is a subgroup of B.

5.1. **positive roots.** Let $f : X \to \mathbb{G}_a$ be an isomorphism from a closed subgroup X of U to $\mathbb{G}_a$. Assume that X is normalized by T. Then T acts on X by

$$T \times X \to X, \quad (t, x) \mapsto txt^{-1}.$$

Then there exists a unique element $\lambda \in X^*(T)$ such that T acts on X by

$$T \times X \to^{\lambda, f} \mathbb{G}_m \times \mathbb{G}_a \to \mathbb{G}_a \to^{f^{-1}} X,$$

using the action of $\mathbb{G}_m$ on $\mathbb{G}_a$ given above. The element $\lambda \in X^*(T)$ attached to X is called a positive root with respect to B and T, and $X = X_\lambda$ is called a positive root space. The set Φ^+ of positive roots is a finite subset of $X^*(T)$.

Let $\alpha \in \Phi^+$, let $T_\alpha \subset T$ be the kernel of $\alpha : T \to \mathbb{G}_m$, and let M_α be the centralizer of T_α with derived group M'_α. The affine group M'_α is almost simple with maximal torus $S \subset T \cap M'_\alpha$. There exists a unique cocharacter $\alpha^\vee \in X_*(T)$ factoring through S

$$\alpha^\vee : \mathbb{G}_m \to S \to T$$

and such that $\langle \alpha, \alpha^\vee \rangle = 2$. Running over $\alpha \in \Phi^+$, the set of all $\alpha^\vee$ so obtained is called the set of positive coroots $\Phi^{\vee+} \subset X_*(T)$.

5.2. **simple roots and the Dynkin diagram.** There exists a unique subset $\Delta \subset \Phi^+$ such that every positive root is a linear combination of Δ with nonnegative coefficients. That is, every positive root is in the cone spaned by the simple positive roots. The set Δ is called the set of simple roots. (The set Δ depends on the choices $T \subset B \subset G$.)

6. CLASSIFICATION DATA

In this subsection, we drop the earlier context. Let Δ be any finite set.

Define the *Cartan matrix* to be a matrix $A : \Delta \times \Delta \to \mathbb{Z}$ that has the following properties.

- $A(\alpha, \beta) \in \{2, 0, -1, -2, -3\}$.
- $A(\alpha, \alpha) = 2$.
- $A(\alpha, \beta) \leq 0$ for all $i \neq j$.
- $A(\alpha, \beta) = 0$ iff $A(\beta, \alpha) = 0$.
- If $A(\alpha, \beta) < -1$, then $A(\beta, \alpha) = -1$.

The Dynkin diagram of (Δ, A) is a graph (with no loops and no multiple joins) with r nodes, indexed by Δ, which we now describe. Edges of the graph are optionally decorated with an integer 2 or 3 and an ordering of the endpoints (an arrow from node α to node β). Two distinct nodes are connected by an edge iff $A(\alpha, \beta) \neq 0$. The edge is not decorated if $A(\alpha, \beta) = A(\beta, \alpha) = -1$. But if $A(\beta, \alpha) \neq -1, 0$, then the edge is decorated with the integer $-A(\beta, \alpha)$ and an arrow from α to β. The integer 2 or 3 is often depicted as a double or triple bond in the graph.

An isomorphism of Dynkin diagrams is a bijection $f : \Delta \to \Delta$ that preserves edges and the labeling of on edges.

An arrow-forgetful automorphism ρ of a Dynkin diagram is defined to be a graph isomorphism of the underlying graph of the Dynkin diagram except that it might not respect the optional arrows that label some edges. ρ is required to respect all the optional natural number labels.

A classification datum consists of a tuple

$$(D, \rho, p, e)$$

where D is a Dynkin diagram, ρ is an arrow-forgetful automorphism of the diagram p is a prime number, and e is a rational number. Not all such tuples appear in the classification theorem. See definition .

In particular, D must be only of the connected Dynkin diagrams that appear in the Cartan classification of Lie algebras over $\mathbb{C}$. By that classification, there are diagrams

$$D = A_r,\ B_r,\ C_r,\ D_r,\ E_6,\ E_7,\ E_8,\ G_2,\ F_4.$$

as shown in Figure `(insert)`.

The automorphism ρ of the Dynkin diagram is determined by its order, and the symbol for the Dynkin diagram is decorated with a prepended superscript indicating the order. If $\rho = 1$ the superscript is omitted. The tuple (D, ρ, p, e) is thus written ${}^{\rho}D(q)$ or $D(q)$, where $q = p^e$. Here is the classification. p is any prime. $e \in \mathbb{N}$, with $e \geq 1$. The excluded values come from [**?**].

Definition 1. *A tuple (D, ρ, p, e) has simple type if it consists of one of the following cases.*

- $A_r(p^e)$, *where* $r \geq 1$. *If* $r = 1$, *then* $p^e > 3$.
- $B_r(p^e)$, *where* $r \geq 2$. *If* $r = 2$, *then* $p^e > 2$.
- $C_r(p^e)$, *where* $r \geq 3$.
- $D_r(p^e)$, *where* $r \geq 4$
- ${}^2A_r(p^e)$, *where* $r \geq 2$. *If* $r = 2$, *then* $p^e > 2$.
- ${}^2D_r(p^e)$, *where* $r \geq 4$.
- ${}^3D_4(p^e)$.
- $G_2(p^e)$, *where* $p^e > 2$.
- $F_4(p^e)$.
- $E_6(p^e)$.
- ${}^2E_6(p^e)$.
- $E_7(p^e)$.
- $E_8(p^e)$.

- ${}^2B_2(2^{f+1/2})$, *where* $f \in \mathbb{N}$.
- ${}^2G_2(3^{f+1/2})$, *where* $f \in \mathbb{N}$.
- ${}^2F_4(2^{f+1/2})$, *where* $f \in \mathbb{N}$.

The last three cases are noteworthy. If the automorphism ρ of D is nontrivial, and if some edge of D carries a label $a = 2, 3$, then $p = a$.

7. Frobenius

Let K, G, B, T be given as in the previous section. We assume in this section that K is an algebraically closed field of positive characteristic p.

Let $q = p^k$ for some $k \geq 1$.

There is a *Frobenius* morphism $F_q : GL(n) \to GL(n)$ given on coordinate rings by

$$F_q^*(x_{ij}) = x_{ij}^q, \quad F_q^*(x_0) = x_0^q.$$

Let G be a linear algebraic group over K. *Standard Frobenius* data for G consists of data (F, n, ϕ, k), where $F : G \to G$ is a morphism, $\phi : G \to GL(n)$ is an isomorphism of G onto a closed subgroup of $GL(n)$ that intertwines:

$$\phi \circ F = F_q \circ \phi$$

where $q = p^k$. *Frobenius data* (F, n, ϕ, k, j) consists of a morphism $F : G \to G$, where (F^j, n, ϕ, k) is a standard Frobenius. Here $F^j = F \circ F \cdots$ (j times).

Let G be a reductive group with Frobenius data (F, n, ϕ, k, j). Then $e = k/j \in \mathbb{Q}$ is the *Frobenius exponent.*

Assume further that F has the property that $F(T) = T$ and $F(B) = B$. The Frobenius F then permutes the set of root spaces X_α, of simple roots $\alpha \in \Delta$ and there is a unique permutation $\rho : \Delta \to \Delta$ such that $F(X_\alpha) = X_{\rho\alpha}$. This uniquely determines an automorphism (again called ρ) of the Dynkin diagram that respects the integer labels on edges, but that does not always respect the direction of the arrows on edges.

If F if a Frobenius map on G, then the set of fixed points

$$G(K)^F = \{g \in G(K) \mid F(g) = g\}$$

is a finite group. In fact,

$$G(K)^F \subset^{\phi} GL(n,K)^{F^j} = GL(n,\mathbb{F}_q),$$

where $\mathbb{F}_q = K^{Fr_q}$ is a finite field with $q = p^k$ elements.

We have a map Q from the set of pairs (G,F) to the set of finite groups given by

$$Q(G,F) = (G(K)^F/Z_G(K)^F)'$$

Here the derived group (indicated by $'$) is the derived group as an abstract group rather than the closed derived subgroup introduced earlier.

8. Almost Simple simply-connected groups

We say that an almost simple group G is *simply connected* if the set of positive coroots spans the cocharacter lattice: $\mathbb{Z}\Phi^{\vee+} = X_*(T)$. (This condition does not depend on the choice of B and $T \subset B$.)

The structure theory of almost simple groups leads to a collection of data $(p,K,G,B,T,\ldots)$ that we call the Lie *theater*. This is the data introduced in the first pages of an enormous number of research articles on Lie theory. Here we consider the data as restricted to the context of interest for the classification of finite simple groups.

Definition 2. *A Lie theater (for almost-simple simply connected groups) consists of the following data*

$$\Theta = (p,K,G,B,T,A,D,F,n,\phi,k,j,e,\rho)$$

subject to the type constraints and propositions given below.

- $p \geq 2$ is a prime number.
- K is an algebraically closed field of characteristic p.
- G is an almost simple group.
- B is a Borel subgroup of G.
- T is a maximal torus of G that is also a subgroup of B. The maximal torus has character $X^*(T)$ and cocharacter groups $X_*(T)$.
- Let $\Phi^+ \subset X^*(T)$ be the set of positive roots in $X^*(T)$ with respect to B and T.
- Let $\Delta \subset \Phi^+$ be the set of simple roots.
- $A : \Delta \times \Delta \to \mathbb{Z}$ is the Cartan matrix $A(\alpha,\beta) = \langle \alpha, \beta^\vee \rangle$ with node set $\Delta \ni \alpha, \beta$.

- D is the Dynkin diagram attached to Δ, A.
- (F, n, ϕ, k, j) is Frobenius data for G such that $F(G) = G$, $F(B) = B$ and $F(T) = T$.
- $e = k/j \in \mathbb{Q}$ is the Frobenius exponent.
- $\rho : D \to D$ is the arrow-forgetful automorphism of the Dynkin diagram induced by the Frobenius data (as described above).

The data is subject to the following additional conditions.

- (simply-connected) $\mathbb{Z}\Phi^{\vee+} = X_*(T)$.
- (D, ρ, p, e) has simple type. (See definition **??**.)

Given a theater $\Theta = (p, K, G, \ldots, F, \ldots)$ there is a finite group $Q(\Theta) = Q(G, F)$, introduced above.

Theorem 3. *If Θ is a Lie theater, then $Q(\Theta)$ is a finite simple group.*

Definition 3. *A finite simple group isomorphic to $Q(\Theta)$ for some Lie theater Θ is a finite simple group of Lie type.*

We define a relation between tuples of simple type and finite simple groups Q of Lie type:

$$(D, \rho, p, e) \sim H$$

if there exists a theater Θ mapping to (D, ρ, p, e) such that $Q = Q(\Theta)$.

Theorem 4 (classification of finite groups of Lie type)**.** *This relation $(\simeq)$ induces a well-defined surjective map from isomorphism classes of tuples of simple type to isomorphism classes of finite groups of Lie type. If two non-isomorphic tuples of simple type map to isomorphic finite groups of Lie type, then it is one of the duplicates enumerated in Theorem* **??**.

That is, each tuple of simple type is isomorphic to one in the image of a Lie theater Θ. Then $Q(\Theta)$ is a finite simple group of Lie type.

8.1. **Notes on Lie type.** Wiki's list [**?**] notes that the order of a finite simple group uniquely determines it up to isomorphism, with the following exceptions.

- $|\mathrm{Alt}_8| = |A_2(4)|$ and both have order 20160,
- $|B_n(q)| = |C_n(q)|$, when $n > 2$ and q odd.

There is a special situation that occurs for the smallest of the the series ${}^2B_2(2^{1/2})$. It is not simple, but its derived group is simple. This is the Tits group, which is sometimes considered as a sporadic groups. It is for the sole purpose of including the Tits group that the map Q was defined using the derived subgroup.

9. Comments about Notation

The rest of the article deals with the sporadic groups. We depart from conventions used in the earlier sections, where G was an affine group. Now G is an abstract group; that is, a group in the conventional sense. Notation will be adapted to this new setting, so that now $Z(G)$ and G' denote the center and derived subgroup of G, respectively.

Alt_n is the alternating group on n letters, (reserving A_n for the Dynkin diagram that appeared earlier).

"$A \times B$ denotes a direct product, with normal subgroups A and B; also $A : B$ denotes a semidirect product (or split extension), with a normal subgroup A and subgroup B; and $A \cdot B$ denotes a non-split extension, with a normal subgroup A and quotient B, but no subgroup B; finally $A.B$ or just AB denotes an unspecified extension" [**?**, p.9]. (For sequences of dots, what is the operator precedence and associativity of this notation?)

If p is prime, p^n denotes a direct product of n cyclic groups of order p. That is, p^n is elementary abelian group of order p^n. [**?**, p.9]

Let p be a prime. An extraspecial p-group is a finite p-group P such that $P' = Z(P)$ and P' has order p. Then P has order p^{1+2n}, for some positive n. For each p, n, there are two extraspecial p-groups of a given order up to isomorphism, denoted $p_{\pm}^{1+2n}$. The signs are determined by the following rules. If p is odd, the sign is $+$ iff P has exponent p (that is, every non-identity element has order p). If $p = 2$, the function x to x^2 on P induces a map P/P' to $Z(P)$, which turns out to be a quadratic form on the vector space P/P'. The notation $+$ means that the quadratic form has an isotropic vector, and $-$ otherwise (for an anisotropic form) [**?**, p.19], [**?**, pp.59,83].

The term *almost simple* is used in the sense of Lie theory (that is, having a simple Lie algebra, or equivalently noncommutative and having no proper closed connected normal subgroups) and not in the sense used by [**?**, p.22].

S_n is the symmetric group on n letters, and Alt_n is the alternating subgroup of index two in S_n.

$O_p(G)$ denotes the p-core of the finite group G. It is the largest normal p-subgroup of G. It is the intersection of Sylow p-subgroups.

10. Sporadic Groups

The lists above specify all but the last 26 finite simple groups, called the sporadic groups. The 26 sporadic groups are classified into three happy families $(5 + 7 + 8)$ and the six pariahs. A useful reference is the atlas of sporadic groups [**?**].

10.1. **First Happy Family (Mathieu groups).**

The first happy family (of 5) are the Mathieu groups. These are quite elementary to specify in terms of automorphism groups of Steiner systems and their subgroups.

- A Steiner system $S(t, k, v)$, where $t < k < v$ are positive integers is a finite set X of cardinality v, a collection of k element subsets of X (called blocks), such that each t element subset of X is contained in a unique block.
- The Steiner system $S(5, 8, 24)$ exists and is unique up to isomorphism. The automorphism group of this Steiner system is M_{24} (which by construction is a subgroup of S_{24}). The stabilizer of a point x (in the 24 element set X) is M_{23}, and the stablizer of two distinct points is M_{22}.
- The Steiner system $S(5, 6, 12)$ exists and is unique up to isomorphism. The automorphism group of this Steiner system is M_{12}. The stabilizer of a point is M_{11}.
- The isomorphism class of the finite simple groups M_{24}, M_{23}, M_{22}, M_{12}, and M_{11} does not depend on any of the choices in this construction.

10.2. **Second Happy Family and the Leech lattice.**

The second happy family (of 7) are those related to the Leech lattice.

- The Leech lattice $L = L24$ can be characterized as the unique even unimodular lattice in dimension 24 that does not have any vectors of norm 2. Norm means the length squared here.
- $Co_1 = Aut_0(L)/\{\pm 1\}$, where $A = Aut_0(L) \subset O(24)$ is the subgroup of the automorphism group of L fixing the origin.

- $Co_2 \subseteq A$ is the stabilizer of any vector of norm 4 (that is, any nonzero vector of shortest length).
- $Co_3 \subseteq A$ is the stabilizer of any vector of norm 6.
- $McL \subseteq Co_3$ is the stabilizer of any pair of vectors $v, w \in L$ such that v has norm 6, w has norm 4, and with inner product $(w, v) = -3$. Equivalently McL is the stabilizer of any pair of vectors v, w of norm 4, such that $(w, v) = -1$.
- $HS \subseteq Co_3$ is the stabilizer of any pair of vectors v, w in L such that v has norm 6 and w is a vector of norm 4, such that $(w, v) = -2$. Equivalently, HS is a rank 3 permutation group on 100 points in which a point stabilizer is isomorphic to M_{22}. [?, p.116]. (Rank 3 permutation group is defined below in the pariah section.)
- J_2. Co_1 has a subgroup of order 3 whose normalizer is isomorphic to $\mathrm{Alt}_9 \times S_3$. The Alt_9 factor has subgroup Alt_5, and the centralizer of Alt_5 in Co_1 is J_2 [?, p.218].
- Suz. In continuation of the construction of the subgroups $\mathrm{Alt}_9 \times S_3$ and Alt_5 in Co_1, the group Alt_5 has a subgroup Alt_3. The centralizer of Alt_3 in Co_1 is $3 \cdot Suz$, a 3-fold central cover of Suz. [?, p.218].
- The isomorphism class of the finite simple groups Co_1, Co_2, Co_3, McL, HS, J_2, Suz do not depend on any of the choices in the construction.

10.3. **monster.** The third happy family (of 8) are those related to the Fischer-Griess monster group M. A construction of the monster is needed.

- Here is a construction of the monster (up to a factor of 2) as the quotient of an infinite Coxeter group by one additional relation [?]. This gives a quick construction. (Compare [?, sec.5.8.5].)
- The monster can also be described up to isomorphism as the finite simple group that contains a pair of involutions z, t, such that the centralizer of z is isomorphic to $2_+^{1+24}Co_1$ and the centralizer of t is isomorphic to the baby monster B. [?, p.148]. This approach requires us to have a prior construction of B.
- A third possible route to the monster is the construction of the Griess algebra, which has the monster as its automorphism group. (See the sketches in [?, p.146] and [?, p.251].) A fourth construction is through the monster vertex algebra [?].

The monster group has an elementary presentation in terms of a quotient of an infinite Coxeter group [?] [?].

We define a Coxeter group Y_{443}. The Coxeter graph is associated with a Coxter graph with 12 vertices:

$$v_{ij}, \quad i = 0, 1, 2, \quad j = 0, .., 3.$$

We construct an undirected graph with 9 edges $\{v_{ij}, v_{i,j+1}\}$, for $j < 3$, and with two additional edges that connect the graph:

$$\{v_{00}, v_{10}\}, \{v_{00}, v_{20}\}.$$

Write E for this set of 11 edges.

Note: the graph is in the shape of a Y with three arms v_{ij}, for $i = 0, 1, 2$.

The associated Coxeter group Y_{433} is the group given by 12 generators and the following relations.

Generators:

$$x_{ij}, \quad i = 0, 1, 2, \quad j = 0, .., 3.$$

Relations:

$$\forall ij, \quad (x_{ij} x_{i'j'})^{m(i,j,i',j')} = 1,$$

where

$$m(i, j, i', j') = \begin{cases} 1, & \text{if } (i, j) = (i', j'); \\ 3, & \text{if } \{v_{ij}, v_{i'j'}\} \in E; \\ 2, & \text{otherwise} \end{cases}$$

This defines Y_{433}. We define G to be the quotient of Y_{433} by the additional relation (called the spider relation):

$$(x_{00} x_{20} x_{21} x_{00} x_{10} x_{11} x_{00} x_{01} x_{02})^{10} = 1.$$

This quotient is $2 \times M$.

10.4. **Third Happy Family and the Monster.**

- M. The monster is characterized above and has an atlas page with further useful information [**?**].
- B. $2 \cdot B$ is a centralizer of an involution in $2A$ in M [**?**, p.256]. ($2A$ is specified below.)

- Fi'_{24}. $3 \cdot Fi'_{24}$ is a centralizer of an element x in the conjugacy class $3A$ of order 3 in M [**?**, p.256-257]. Moreover, $3 \cdot Fi_{24}$ is the normalizer of the subgroup $\langle x \rangle$.
- Fi_{23}. This is a subgroup of Fi'_{24} described below.
- Fi_{22}. This is a subgroup of Fi'_{24} described below.
- Th. Let x be an element of order three in the conjugacy class $3C$, then $Th = C_M(\langle x \rangle)/\langle x \rangle$.
- HN. Let x be an element of conjugacy class $5A$ in M. Then $HN \simeq C_M(x)/\langle x \rangle$ [**?**, p.262].
- He. Let x be an element in conjugacy class $7A$ in M. Then $He \simeq C_M(x)/\langle x \rangle$. [**?**, p.263].

These constructions mention conjugacy classes $2A$, $3A$, $3C$, $5A$, $6A$, $7A$ in M. Classes are labeled NX, where $N = 1, 2, 3, 4, 5, 6$ is the order of an element in the conjugacy class, and $X = A, B, \ldots$ are letters to differentiate the conjugacy classes of a given order, A is the class of smallest cardinality of that order, B is the second smallest, etc. In general there can be classes of the same order and cardinality, but that does not happen with any of the orders in M we discuss. In particular, $2A$ is the smallest conjugacy class of order 2, and $3A$ is the smallest conjugacy class of order 3. The product of two elements of $2A$ can land in any of nine different conjugacy classes: $1A$, $2A$, $2B$, $3A$, $3C$, $4A$, $4B$, $5A$, $6A$. See [**?**, p.7] and [**?**, p256].

A 3-transposition group is a "finite group G generated by a conjugacy class D of involutions, such that any two elements of D have a product of order at most 3, and ... such that $G' = G''$ and any normal 2- or 3-subgroup of G is central" [**?**, p235]. We call the elements of D transpositions. There is a classification of 3-transposition groups. There is a 3-transposition group such that its quotient by its center is Fi_n, for $n = 22, 23, 24$.

- Fi_{23}. The stabilizer of one transposition in Fi'_{24} is Fi_{23}.
- Fi_{22}. The stabilizer of two commuting transpositions in Fi'_{24} is $2 \cdot Fi_{22} : 2$. [**?**, p.250]

10.5. **The Pariahs.** It is not clear what the best route to the six pariahs will be. Expert opinion is needed. At the very least we might specify them as the unique simple group of a given order, even if that is not a very useful description. "The behavior of these six groups is so bizarre that any attempt to describe them ends up looking like a disconnected sequence of related facts." [**?**, p.184]. [**?**, pp.150-153] gives a brief description of each pariah.

- J_1. "It is the unique simple group which has abelian Sylow 2-groups and contains an involution with centralizer isomorphic to" $2 \times \mathrm{Alt}_5$. [**?**, p.150]
- J_3. This group appears in a centralizer involution problem. $2_-^{1+4} : \mathrm{Alt}_5$, split extension (therefore not the standard holomorph, which embeds in $GL(4, C)$)" [**?**, p.151]. There are two finite simple groups with this involution centralizer. The other is J_2, which appears in the second happy family. J_3 has order $2^7\, 3^5\, 5.17.19$."
- Ly. This group is uniquely characterized up to isomorphism as a finite simple group that contains an involution whose centralizer is isomorphic to $2 \cdot \mathrm{Alt}_{11}$, the covering group of the alternating group of degree 11. Moreover, the group has a single class of involutions and has order $2^8 * 3^5 * 5 * 7 * 11 * 37 * 61 * 67$. [**?**, p.151]
- $O'N$. This is the unique simple group G up to isomorphism with the following properties [**?**, p.152]:
  - For every elementary subgroup E of G, we have $N_G(E)/C_G(E) \simeq GL(E)$.
  - G contains a subgroup $E \simeq 2^3$ such that $N_G(E) \simeq 4^3 \cdot GL(3, 2)$
  - G contains an involution whose centralizer has the form $4.PSL(3, 2).2$.
- J_4. This is characterized as a finite simple group that contains an involution with centralizer isomorphic to $2_-^{1+12} \cdot 3 \cdot M_{22} : 2$. "The centralizer is nonsplit over the [2-core] O_2 and contains a perfect group $6 \cdot M_{22}$." Moreover, the simple group has order $2^{21}3^3 5.7.11^3.23.29.31.37.43$ [**?**, p.152].
- Ru. A permutation group is defined to have rank r if it is transitive and a point stabilizer has r orbits. This group is characterized as a rank 3 finite simple group whose point stabilizer is $H = {}^2F_4(2)$, the Ree group over the field with 2 elements. (As described above, the derived group of H is the Tits group.) [**?**, p.151]

11. Checking the Answer

If proofs are not included in the statement of the theorem, what sanity checks are there to make sure that the specification is correct? One possibility that has been discussed is the following. There is currently a bridge between Mathematica and Lean, constructed by Rob Lewis and Minchao Wu [**?**]. Lean is also now available as a package in CoCalc (which also provides access to GAP). We can hope that further development will provide a bridge (at some indefinite day in the future) that would allow for some sanity checks by running some GAP calculations based on the Lean specification and comparing to known answers. We can discuss what might be done here.

Other references [?], [?].