CHAPTER V

Simple groups

5.1. Introduction.

Groups are the most investigated topic for superstructures with one operation. We develop some basic ideas in group theory, but the classification of Lie algebras is dealt with in [Ad15] chapter V, and is not repeated here.

The theory of zargonions leads us in a natural way to ask what impact zargonions have on the theory of groups, even the classification of simple groups, for which the claim has been made that a complete classification was achieved after monumental efforts finally in 2008. This subject is dealt with in chapter IX on zargonion lattices.

5.2. Basic ideas in group theory.

A *magma* is the most general structure combining sets and an operation. A magma is a set M with a single binary operation $M \times M \to M$, combining elements in pairs of the magma, with each pair forming another element belonging to the magma. No other properties are specified.

A *group* is a magma with the following structure. The operation on the magma can be written either additively or multiplicatively without brackets, the two choices being equivalent within the group. For an *abelian group* ($a + b = b + a$) the *identity*, e, for a group if written additively is the element 0, or 1 written multiplicatively, where $a + 0 = a = 0 + a$. Groups have *inverses* (-a) of a written additively, or a^{-1} written multiplicatively, with the additive rule

$$a + (-a) = 0,$$

alternatively if written multiplicatively

$$a\,(a^{-1}) = 1 = (a^{-1})a.$$

A group is *nonabelian* or *noncommutative*, usually written multiplicatively, if some $ab \neq ba$.

In any group the integral *power* of an element a can be defined as the element

$$a^m = a.a. \ldots a \text{ (m terms)}.$$

Negative powers can be defined by

$$a^m a^{-m} = 1.$$

A group G is called *cyclic* if it contains an element the powers of which exhaust G. Cyclic groups are abelian. It is often understood that cyclic groups are finite. When this is not so, we will explicitly state that they are infinite.

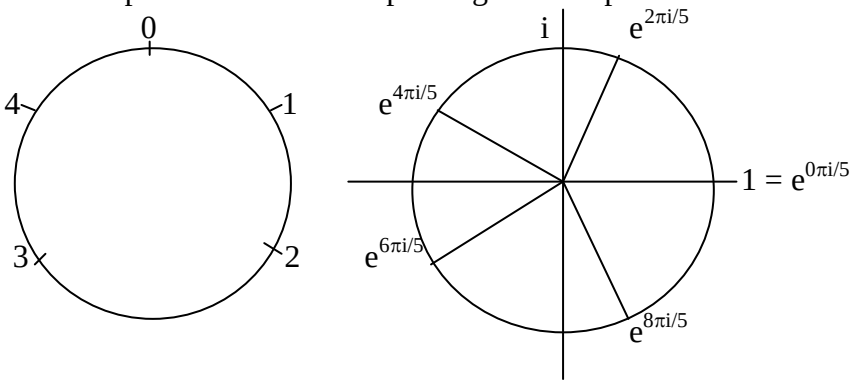
A *permutation* is a bijection of a finite set to itself. A permutation which interchanges cyclically m objects of a set {1, 2, ..., m} forms an abelian group called a cycle of degree m. This permutation is obtained from a power by specifying that a^{m-1} is the m^{th} element and the cyclic permutation consists of multiplying by a. It can be represented by

$$\begin{pmatrix} 1 & 2 & \cdots & m-1 & m \\ 2 & 3 & \cdots & m & 1 \end{pmatrix},$$

or in contracted notation by (1 2 ... m). Another picture of a cyclic group is given by the 'clock' diagram x (mod p) and the Argand complex circle diagram, where there is a bijection for fixed r

$$x \text{ (mod p)} \leftrightarrow e^{r + (2\pi i x/p)},$$

which can be pictured in the example diagrams for p = 5:



x (mod 5) complex (Argand) diagram with unit radius

A group derived from cyclic group generators which do not intersect, so the generators form a partition for the group, is also cyclic. For a finite cyclic group G its number of elements, or *order*, |G|, which is the number of times it takes a generator to return to the identity, is the least common multiple (l.c.m.) of the order of its cyclic components. An example of a cyclic permutation with the identity permutations present is

(1 2)(4 6 7)(3)(5)

which we can contract by removing the identity permutations to

(1 2)(4 6 7) = (4 6 7)(1 2).

The set of all permutations of m objects forms a group called the *symmetric group*, denoted by S_m. The name is derived from its origins in describing polynomial equations.

We have represented permutations by two ordered rows of n elements. It can equally well be represented by n ordered columns of two elements. We will represent a *column* by [x, f(x)], where x and f(x) belong to the same set X of distinct elements.

Subsets $\{x_i\} \in X$ indexed by elements $i \in I$ form a *partition* of X whenever

$$\{x_i\} \cap \{x_j\} = \emptyset$$

for $i \neq j$, and

$$\cup_i \{x_i\} = X .$$

When only one value of i is selected, we will call $[x_i, f(x_i)]$ an *element* of the partition.

We have defined *composition of elements* of the partition by associating elements $[x_i, f(x_i)]$ and $[f(x_i), y_i]$ with the element $[x_i, y_i]$.

The element $[x_i, x_i]$ acts as an *identity* of the partition.

Lemma 5.2.1. *If* $[x_i, y_i]$ *and* $[z_i, x_i] \in X$ *are not identity elements, then* $[y_i, z_i]$ *does not belong to* X.

Proof. By definition $[z_i, y_i] \in X$, and if $[y_i, z_i] \in X$ then $[z_i, z_i] \in X$, but we have just stated that $[z_i, z_i] = [z_i, y_i]$ is not the identity. □

Definition 5.2.2. The *upper overlap* of $[x_i, f(x_i)] \in X$ and $[y_j, f(y_j)] \in Y$ is all those $[z_k, f(z_k)] \in Z$ with $x_i = y_i = z_k$.

Definition 5.2.3. The *lower overlap* of $[x_i, f(x_i)] \in X$ and $[y_j, f(y_j)] \in Y$ is all those $[z_k, f(z_k)] \in Z$ with $f(x_i) = f(y_i) = f(z_k)$.

It should be clear that the set Z does not belong to a permutation, unless it is the identity permutation.

Definition 5.2.4. The *overlap* of $[x_i, f(x_i)] \in X$ and $[y_j, f(y_j)] \in Y$ is the union of the upper and lower overlaps.

Definition 5.2.5. The *transposition* of elements a and b given by the composite ab is ba.

A noncommutative group must be generated by cycles which overlap somewhere, since it is not abelian and so cannot be represented by partitioned cycles. For example the transposition

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}3 & 4\\ 4 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix} \neq \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix} = \begin{pmatrix}3 & 4\\ 4 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}.$$

Theorem 5.2.6. *The complement* $C(Z)$ *of the overlaps* $a \in A$ *and* $b \in B$ *in a noncommutative transposition* $ab \to ba$ *of* Z *belongs to a permutation and is unchanged by the transposition, the remaining elements are changed*.

Proof. By lemma 5.2.1 [f(b), a] does not belong to AB and [f(a), b] does not belong to AB, but under a transposition [a, f(b)] does not belong to BA and [b, f(a)] does not belong to BA, and therefore the intersection of the upper or lower overlaps is empty, but their union is given by $Z = AB \cup BA$, forming a partition of Z.

Since all identity elements are excluded from Z, they may be included in C(Z), otherwise the combinations not involving ab or ba are in C(Z), which is unaffected by Z and thus belongs to a permutation.

But the upper overlap contains [b, f(a)], and the lower overlap contains [f(b), a], which do not intersect, AB contains [a, f(b)] and BA contains [f(a), b] which are distinct, since $a \neq f(a)$ and also AB contains $[f^{-1}(b), b]$ and BA $[f^{-1}(a), a]$, again distinct, which is all four possibilities. □

The symmetric group can be described by matrices. For example $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 1 & 3 & 5\end{pmatrix}$ can be represented by the matrix with one 1 in each row and column, and zeros elsewhere

$$\begin{bmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix},$$

in which, say, $2 \to 4$ is represented by a 1 in the second row and fourth column, with operations defined by matrix multiplication. As a further example, the cyclic group of order 4 is given by the matrices

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix} \text{ and } \begin{bmatrix}0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}.$$

All elements of S_4 can be obtained from the above by permuting rows or alternatively and equivalently by permuting columns.

A *subgroup* S of a group G is a group included in G. If $S \neq G$, S is a *proper subgroup*. The number of elements in the subgroup is called the order of the subgroup. The complement of S in G cannot form a subgroup, since 1 does not belong to it.

A *homomorphism* h of a group G to a group G′ is a surjective map ab = g → h(g), such that
h(ab) = h(a)h(b).
An *automorphism* is a homomorphism G → G.

Theorem 5.2.7. *Under a homomorphism the identity* e *of* G *maps to the identity* h(e) *of* G′, *and maps inverses* a^{-1} *to* $h(a)^{-1} = h(a^{-1})$.

Proof. The identity satisfies ee = e, so h(ee) = h(e) = h(e)h(e). The inverse satisfies $(a)(a^{-1}) = e$, so $h(a)h(a^{-1}) = h(e) = h(a)h(a)^{-1}$, and multiplying on the left by $h(a)^{-1}$ gives $h(a^{-1}) = h(a)^{-1}$. □

The set {k} is the *kernel*, K, of a group homomorphism h: G → G′, if it satisfies
h(a)h(k) = h(a) = h(k)h(a),
in other words it is the identity of G′.

A *right coset or right residue class* of a subgroup S of G is the set of elements Sa, with s ∈ S and a ∈ G. A *left coset* is the set aS, and when both coincide the set can be called a *coset*.

The *quotient group* G/S *of* G mod S for G a group, S a subgroup, is the family of left cosets.

Lemma 5.2.8. *If* S *is finite, each right* (*or left*) *coset has as many elements as* S. *Two right* (*or left*) *cosets are either identical or have no common elements*.

Proof. The map a → sa is a bijection, since each sa is the image of one and only one a, and if a → sb, with b ≠ a then $1 = a(a^{-1})$ maps to $sb(a^{-1}) = s(ba^{-1}) = s$, so b = a. Further, if there were any intersection, then sb = sa, which we have shown is impossible unless b = a. □

If G is finite, it can be partitioned into a finite number of right or left cosets where each coset contains the same number of elements, and the conclusion is
Theorem 5.2.9. (**Lagrange's subgroup theorem**). *The order of a finite subgroup* S ⊆ G *divides the order of a finite group containing it*. □

5.3. Normal subgroups.

A *conjugate* of an element x in a group G is an element $a^{-1}xa$.

Theorem 5.3.1. *For an element* a *of* G, *conjugation* T_a: x → a^{-1}xa *is an automorphism of* G.

Proof. $(a^{-1}xa)(a^{-1}ya) = a^{-1}(xy)a$. □

An automorphism of the form a^{-1} xa is called an *inner automorphism*, otherwise it is called an *outer automorphism*. It follows from what we have said that inner automorphisms form a subgroup of all the automorphisms of a group G. □

A subgroup S of G is *normal* in G if and only if it is invariant under all inner automorphisms of G. For example, consider the symmetric group S_3 of all permutations of the set {1, 2, 3}. Then {(1, (1 2 3), (1 3 2)} is a normal subgroup of S_3, because we can verify the following statements.

(1 2){(1, (1 2 3), (1 3 2)} = {(1 2), (1 3), (2 3)} = {(1, (1 2 3), (1 3 2)}(1 2)
(1 3){(1, (1 2 3), (1 3 2)} = {(1 3), (2 3), (1 2)} = {(1, (1 2 3), (1 3 2)}(1 3)
(2 3){(1, (1 2 3), (1 3 2)} = {(2 3), (1 2), (1 3)} = {(1, (1 2 3), (1 3 2)}(2 3).

Theorem 5.3.2. *A subgroup* S *is normal if and only if all of its right cosets are left cosets*.

Proof. Let S be normal. Then $aSa^{-1} = (a^{-1})^{-1}S(a^{-1}) = S$. Thus Sa = aS. Conversely, applying lemma 5.3.2, if two cosets are equal so that Sa = bS, then a = b and S is normal. □

It should be carefully noted that the equation Sa = aS does not claim that every element of S commutes with a, only that the cosets Sa and aS are the same.

The *commutator* of two group elements a and b is
$$[a, b] = aba^{-1}b^{-1}.$$
The commutator [a, b] is equal to the identity element e if and only if ab = ba.

The *commutator subgroup* [G, G] (also called the *derived subgroup* of G and denoted $G^{(1)}$) is the subgroup generated by all the commutators.

Theorem 5.3.3. *the quotient group* G/[G, G] *is abelian*.

Proof. If a, b ∈ G, then by definition $aba^{-1}b^{-1} = c \in [G, G]$, which is normal,
$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}.$$
A general element of [G, G] may not be a commutator, but is a product of commutators
$$g(c_1,c_2, \ldots c_n)g^{-1} = (gc_1g^{-1})(gc_2g^{-1})\ldots(gc_ng^{-1}).$$
Thus $[G, G]aba^{-1}b^{-1} = [G, G]$, implying [G, G]ab = [G, G]ba. □

A group G is called *simple* if its only normal subgroups are the identity and G itself.

5.4. The isomorphism theorems.

Our objectives now are to prove three isomorphism theorems [Ar88]. We will relate groups to probability logic, which includes a theorem on direct sums, and connect these ideas with the factor-commutator group, giving the relationship of these to eigenvalues in chapter VIII, section 5. Firstly we prove two lemmas

Lemma 5.4.1. *A nonempty subset* B *of a group* G *is a subgroup of* G *if and only if* $ab^{-1} \in B$ *whenever* a ∈ B *and* b ∈ B.

Proof. If B is a subgroup, then since b^{-1} belongs to B, so does the product ab^{-1}. Conversely, if $B \neq \emptyset$ and $ab^{-1} \in B$, then $aa^{-1} = e \in B$, and whenever a ∈ B then $a^{-1} \in B$, so $ea^{-1} \in B$. Further, if the element b ∈ B, so $b^{-1} \in B$, then $ab = a(b^{-1})^{-1} \in B$. Thus, B is a subgroup of G. □

Lemma 5.4.2. *The intersection of two subgroups of a group is itself a subgroup*.
Proof. Let A and B be two subgroups of a group G, then the identity lies in both of them, and thus $A \cap B \neq \emptyset$. Further, if a ∈ A and b ∈ B, then they are both elements of A and B, and thus the product ab^{-1} belongs to both A and B. So on applying lemma 5.4.1, A ∩ B is a subgroup of G. □

Remark 5.4.3. The probability P(A) and P(B) of two events A and B respectively, satisfies
$$P(A \cap B) = P(A)P(B) \qquad (1)$$
so, given by the equivalence demonstrated in *Superexponential algebra* [Ad15], chapter XIV, of set theory to arithmetic, there is a bijective mapping between sets and probabilities, say,

represented by fractions in the interval [0, 1], which is bijective to $\mathbb{N}$. But now lemma 5.4.2 demonstrates a mapping between groups and sets, which in the categorical language of chapter III, section 8, is a forgetful functor. This shows that there is a forgetful functor between groups and the logic of fractional probabilities, which is abelian. If the group is finite this means the fractional probability arithmetic is a finite, or congruence, arithmetic.

In the case we have considered, namely that impossible is 0 and certain is 1, the probability of the complement of A is

$$P(C(A)) = 1 - P(A). \tag{2}$$

We can extend these ideas further to consider, as has been proved in [Ad15], chapter XIII,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \tag{3}$$

where $A \cup B$ the union of A and B satisfies

$$A \cup B = C(C(A) \cap C(B)) \tag{4}$$

and note that

$$P(A \cup B) - P(A \cap B)$$

is the probability of A OR B but not both, which in the case $P(A \cap B) = 0$ is the disjoint sum of P(A) and P(B), but in general we can use (1) to define multiplication and (3) to define addition in these logics, so if we wished we could define superexponential operations as an extension of this idea. □

Theorem 5.4.4. (First isomorphism theorem). *For* $a \in G$ *the kernel* K *of a homomorphism* $h: G \to G'$ *is a normal subgroup of* G, *and there is an isomorphism* $aK \to h(a)$ *of the quotient group* G/K *to the codomain of* h.

Proof. Firstly, let $a, b \in K$. Then $h(ab^{-1}) = h(a)h(b)^{-1} = e$, so $ab^{-1} \in K$. Since $e \in K$, $K \neq \emptyset$, so that by lemma 5.3.7, K is a subgroup of G. Now if $a \in K$ and $g \in G$, then

$$h(gag^{-1}) = h(g)h(a)h(g)^{-1} = h(g)h(g)^{-1} = e,$$

and thus $gag^{-1} \in K$, which is the same as saying that K is normal in G.

Secondly, if two cosets aK and bK are equal, then $b^{-1}a \in K$. This implies that the identity $e = h(b^{-1}a) = h(b)^{-1}h(a)$, and thus $h(a) = h(b)$, so that we have a function $j: G/K \to G'$ satisfying $j(aK) = h(a)$. Conversely, if $h(a) = h(b)$, then $aK = bK$, so that j is an injection. Moreover, for any two cosets $aK, bK \in G/K$, j is a homomorphism with

$$j(aKbK) = j(abK) = h(ab) = h(a)h(b) = j(aK)j(bK).$$

Since the codomain of j is identical to that of of h, we have proved j is an isomorphism from G/K to the codomain of h. □

Corollary 5.4.7. *If the codomain of* h *is all of* G', *then* G/K *is isomorphic to* G'.

Corollary 5.4.8. *Let the codomain of* h *be all of* G'. *Then* h *is an isomorphism if and only if* K *is precisely the identity element of* G.

Theorem 5.4.9. (Second isomorphism theorem). *Let* H *and* N *be subgroups of* G *with* N *normal in* G *Then* HN *is a subgroup of* G, $H \cap N$ *is a normal subgroup of* H, *and the groups* HN/N *and* $H / H \cap N$ *are isomorphic.*

Proof. Suppose $g_1, g_2 \in HN$ and write $g_1 = h_1n_1$, $g_2 = h_2n_2$, where $h_1, h_2 \in H$, $n_1, n_2 \in N$. Then

$$g_1g_2^{-1} = h_1n_1n_2^{-1}h_2^{-1} = (h_1h_2^{-1})(h_2n_1n_2^{-1}h_2^{-1}) \in HN,$$

and by lemma 5.3.7, HN is a subgroup of G.

The normality of $H \cap N$ follows from the fact that the function $f: H \to HN/N$ is a surjective homomorphism, because if $f = hn \in HN$, then

$f(h) = hN$
$= hnN$ (because $n \in N$)
$= gN$,

so that the element $h \in H$ belongs to the kernel of f exactly when $hN \in N$. Thus, the kernel of f is $H \cap N$, and the result follows from the first isomorphism theorem, 5.2.10. □

Theorem 5.4.8. (Third isomorphism theorem). *If* M, N *are normal subgroups of* G *and* M *is included in* N, N/M *is a normal subgroup of* G/M *and the quotient group* $(G/M)/(N/M)$ *is isomorphic to* G/N.

Proof. The function $h: G/M \to G/N$ defined by $h(aM) = aN$ is a surjective homomorphism. Now a coset aM belongs to the kernel of h precisely when $aN = N$, that is, when $a \in N$. Thus, the kernel of h is N/M, so the theorem follows from theorem 5.4.4, the first isomorphism theorem. □

5.5. The Schur multiplier.

The *center* of a group G, denoted Z(G), is the set of elements that commute with every element of G.

The *general linear group* GL of degree n is the set of $n \times n$ invertible matrices, meaning they have a multiplicative inverse, together with the operation of ordinary matrix multiplication. $GL(n, \mathbb{C})$ are invertible matrices with complex number elements.

The *projective linear group* PGL is the induced action of the general linear group of a vector space **V** on the associated projective space P(**V**). Explicitly, the projective linear group is the quotient group

$PGL(\mathbf{V}) = GL(\mathbf{V})/Z(\mathbf{V})$

where GL(**V**) is the general linear group of **V** and Z(**V**) is the subgroup of all nonzero scalar transformations of **V**. These are quotiented out because they act trivially on the projective space and they form the kernel of the action. The notation "Z" is used because the scalar transformations form the center of the general linear group.

A group homomorphism from D to G is said to be a *Schur cover* of the finite group G if the kernel is contained both in the center and the commutator subgroup of D, and amongst all such homomorphisms, this D has maximal size.

The *Schur multiplier* of G is the kernel of any Schur cover. When the homomorphism is understood, the group D is often called the Schur cover.

Schur's motivation for studying the multiplier was to classify projective representations of a group. A projective representation is much like a group representation except that instead of a homomorphism into the general linear group $GL(n, \mathbb{C})$, one takes a homomorphism into the projective general linear group $PGL(n, \mathbb{C})$. In other words, a projective representation is a representation modulo the center.

5.6. The standard classification of simple groups.

Finite simple groups are classified as lying in one of 18 *families*:

- Z_p – a cyclic group of prime order,
- A_n – an alternating group for $n \geq 5$;
  The alternating groups may be thought of as groups of Lie type over the field with one element, which unites this family with the next, so all families of nonabelian finite simple groups may be considered to be of Lie type,
- One of 16 families of Lie type groups;
  The Tits group is usually considered of this form, although strictly speaking it is not of Lie type, but rather of index 2 in a Lie type group,

or otherwise as one of 26 *exceptions*. The number of elements of these 26 sporadic simple groups, together with their Schur multipliers is listed below.

Simple group (p = pariah)	**Order**	**Order of Schur multiplier**
Monster *M*	$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$	1
Baby monster *B*	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$	2
Thompson group *Th*	$2^{11}.3^{10}.5^3.7^2.13.19.31$	1
Lyons group *Ly* (p)	$2^8.3^7.5^6.7.11.31.37.67$	1
Harada-Norton group *HN*	$2^{14}\cdot3^6\cdot5^6\cdot7\cdot11\cdot19$	1
O'Nan group *O'N* (p)	$2^9\cdot3^4\cdot5\cdot7^3\cdot11\cdot19\cdot31$	3
Suzuki sporadic group *Suz*	$2^{13}\cdot3^7\cdot5^2\cdot7\cdot11\cdot13$	6
Rudvalis group *Ru* (p)	$2^{14}\cdot3^3\cdot5^3\cdot7\cdot13\cdot29$	2
Held group *He*	$2^{10}\cdot3^3\cdot5^2\cdot7^3\cdot17$	1
McLaughlin group *MCL*	$2^7\cdot3^6\cdot5^3\cdot7\cdot11$	3
Higman-Sims group *HS*	$2^9\cdot3^2\cdot5^3\cdot7\cdot11$	2
Fischer group Fi_{22}	$2^{17}\cdot3^9\cdot5^2\cdot7\cdot11\cdot13$	6
Fischer group Fi_{23}	$2^{18}\cdot3^{13}\cdot5^2\cdot7\cdot11\cdot13\cdot17\cdot23$	1
Fischer group Fi_{24}	$2^{21}\cdot3^{16}\cdot5^2\cdot7^3\cdot11\cdot13\cdot17\cdot23\cdot29$	3
Conway group Co_1	$2^{21}\cdot3^9\cdot5^4\cdot7^2\cdot11\cdot13\cdot23$	2
Conway group Co_2	$2^{18}\cdot3^6\cdot5^3\cdot7\cdot11\cdot23$	1
Conway group Co_3	$2^{10}\cdot3^7\cdot5^3\cdot7\cdot11\cdot23$	1
Janko group J_1 (p)	$2^3\cdot3\cdot5\cdot7\cdot11\cdot19$	1
Janko group J_2	$2^7\cdot3^3\cdot5^2\cdot7$	2
Janko group J_3 (p)	$2^7\cdot3^5\cdot5\cdot17\cdot19$	3
Janko group J_4 (p)	$2^{21}\cdot3^3\cdot5\cdot7\cdot11^3\cdot23\cdot29\cdot31\cdot37\cdot43$	1
Mathieu group M_{11}	$2^4\cdot3^2\cdot5\cdot11$	1
Mathieu group M_{12}	$2^6\cdot3^3\cdot5\cdot11$	2
Mathieu group M_{22}	$2^7\cdot3^2\cdot5\cdot7\cdot11$	12
Mathieu group M_{23}	$2^7\cdot3^2\cdot5\cdot7\cdot11\cdot23$	1
Mathieu group M_{24}	$2^{10}\cdot3^3\cdot5\cdot7\cdot11\cdot23$	1

The 20 sporadic groups which are subquotients of the monster are called the *happy family*. The remaining 6 are referred to as *pariahs*. 37 does not divide the order of the monster but divides *Ly* and J_4, which are therefore pariahs. Four other groups can be shown to be pariahs.

The famous theorem of Feit and Thompson states that every group of odd order is solvable. This means every finite simple group has even order unless it is cyclic of prime order.

5.7. The orbit-stabiliser theorem.

For a set X, let S_X be the symmetric group of X, that is, the set of permutations of elements of the set X.

Definition 5.7.1. An *action* of a group G on a set X is a homomorphism h from G to S_X.

For $g \in G$ and $x \in X$ we will use the notation g(x) for h(g(x)), that is, the image of the point x under the permutation corresponding to g.

Definition 5.7.2. The *orbit* of x, written G(x) is the set of all images of g(x) as g varies over G.

Thus $G(x) \subseteq X$.

Definition 5.7.3. For $x \in X$, the elements of G which leave x fixed are known as the *stabiliser*, G_X, of G.

Theorem 5.7.4. *Points in the same orbit have conjugate stabilisers.*

Proof. Let x and y belong to the same orbit with g(x) = y. We need to show

$$gG_xg^{-1} = G_y.$$

Suppose $h \in G_x$. Then

$$\begin{aligned} ghg^{-1}(y) &= ghg^{-1}(g(x)) \\ &= gh(x) \\ &= g(x) \\ &= y. \end{aligned}$$

Thus $gG_xg^{-1} \subseteq G_y$. But the same argument applies with x and y reversed, giving $g^{-1}G_yg \subseteq G_x$, or $G_y \subseteq gG_xg^{-1}$. Therefore $gG_xg^{-1} = G_y$. □

Theorem 5.7.5. (**Orbit-stabiliser theorem**). *Let* $x \in X$. *The mapping* $g(x) \to gG_x$ *is bijective between* G(x) *and the left cosets of* G_x *in* G.

Proof. The mapping is surjective, since G_x is a subset of G. It is also injective, since if $gG_x = hG_x$ then g = hj for some element j of G_x, and thus (hj)(x) = h(j(x)) = h(x). □

Corollary 5.7.6. *If* G *is finite, the cardinality, or size, of each orbit is a multiplicative factor in the order of* G.

Proof. The orbit-stabiliser theorem states that the size of the orbit is the index of the stabiliser of x in G, $|G|/|G_x|$, in other words that

$$|G| = |G(x)|.|G_x|.$$ □

Theorem 5.7.7. (**Counting theorem**). *Let* X^g *be the subset of* X *of points left fixed by the element* $g \in G$. *The number of distinct orbits is the average number of points left fixed by an element of* G, *that is*

$$\frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Proof. The number of ordered pairs (g, x) of $G \times X$ with g(x) = x is

$$\sum_{g\in G}|X^g|, \qquad (1)$$

which is the same as

$$\sum_{x\in X}|G_x|. \qquad (2)$$

If the number of distinct orbits is X_1, X_2, ..., X_n, then this is just

$$\sum_{k=1}^{n} \sum_{x \in X_k} |G_x|.$$

Since points in the same orbit have conjugate stabilisers, if we choose a point y of X_k then

$$\sum_{x \in X_k} |G_x| = |X_k|.|G_y| = |G(y)|.|G_y|,$$

which by the orbit stabiliser theorem 5.7.5 is precisely |G|. Therefore the theorem follows on identifying (1) and (2). □

Theorem 5.7.8. *Conjugate group elements fix the same number of points.*

Proof. Let g and h be conjugate in G under $jgj^{-1} = h$. When g fixes x, this implies that h fixes j(x), since

$$h(j(x)) = jgj^{-1}(j(x)) = jg(x) = j(x),$$

and thus j maps injectively the set X^g to X^h. Then on swapping round g and h, j^{-1} is surjective from X^h to X^g. Thus there is a bijection between these sets, and the number of fixed points in each is the same. □

5.8. Sylow's theorems.

Lemma 5.8.1. *Let* p *be a prime number, and suppose* k *is not divisible by* p. *If* $0 \leq y \leq p^n - 1$, *then* $(kp^n - y)/(p^n - y)$ *is not divisible by* p.

Proof. Because p is prime, it follows that if y is not divisible by p^m for $0 < m < n$, then neither $(kp^n - y)$ nor $(p^n - y)$ are divisible by p, but if y is divisible by p^m, then the factor p^m cancels in the numerator and denominator of $(kp^n - y)/(p^n - y)$, and then the same situation applies as before but with new variables. □

Consider a finite group G with order divisible by the prime p. Let p^n be the highest power of p which is a factor of |G|, and let $k = |G|/p^n$.

Theorem 5.8.2. G *contains at least one subgroup of order* p^n.

Proof. Suppose X is the set of all subsets of G with p^n elements, and let G act on X by *left translation*, meaning that $g \in G$ sends the subset $W \in X$ to gW. By lemma 5.8.1 the size of X is not divisible by p, so there is an orbit G(W) which is also not divisible by p. By the orbit-stabiliser theorem, $|G| = |G(W)|.|G_W|$, so that $|G_W|$ has no factor p^n. The fact that G_W is the stabiliser of W means that if $w \in W$ and $g \in G_W$, then $gw \in W$. Thus whenever $w \in W$ the right coset $G_W w$ is contained in W. But $|G_W|$ cannot be greater than p^n. Thus G_W is a subgroup of G with order p^n. □

Lemma 5.8.3. *Let* H_1, H_2, ..., H_m *denote subgroups of* G *with order* p^n. *Let* H_1 *act on the set* $\{H_1, H_2, ..., H_m\}$ *by conjugation, meaning* $h \in H_1$ *sends* H_i *to* hH_ih^{-1}. *If* K_i *is the stabiliser of* H_i, *then* $K_i = H_1 \cap H_i$.

Proof. By definition $K_i \subseteq H_1$ and $H_1 \cap H_i \subseteq K_i$. We need to show that $K_i \subseteq H_i$. But K_i, which is the set $\{h \in H_1: hH_jh^{-1} = H_j\}$, satisfies $K_iH_i = H_iK_i$, since if k, $k^{-1} \in K_i$ and h, $h^{-1} \in H_i$, then kh, $(kh)^{-1} = h^{-1}k^{-1}$, $k^{-1}h^{-1}$ and $(k^{-1}h^{-1})^{-1} = hk \in K_iH_i$ and also H_iK_i. So K_iH_i is a subgroup of G. So H_i is a normal subgroup of K_iH_i, and by the second isomorphism theorem 5.4.9

$$K_iH_i/H_i = K_i/(K_i \cap H_i).$$

Thus the order of K_iH_i, $|H_i|.|K_i/(K_i \cap H_i)|$, is a power of p. Since the largest power of p is $p^n = |H_i|$, this shows that $K_i \subseteq H_i$ as we needed to prove. □

Theorem 5.8.4. *Any two subgroups of* G *of order* p^n *are conjugate. Moreover, the number of subgroups of* G *of order* p^n *is congruent to* 1 (mod p) *and is a factor* of $k = |G|/p^n$.

Proof. We have $K_1 = H_1$, so by the orbit-stabiliser theorem the only element of H_1 is H_1 itself. If $i \neq 1$, then the order of K_i is a smaller power of p than p^n, so that by the same theorem, every other orbit has a size that is a multiple of p. But summation of the orbits using the counting theorem 5.7.7 shows that m is congruent to 1 (mod p).

Suppose the whole group G acts on $\{H_1, H_2, ..., H_m\}$ by conjugation. We now prove that any two subgroups of G of order p^n are conjugate. Every G-orbit consists of H_1-orbits. Now H_1 is contained in the G-orbit of H_1, so its orbit size is congruent to 1 (mod p). Let H_j be outside the G-orbit of H_1. We prove the following contradiction. If H_j operates on $\{H_1, H_2, ..., H_m\}$ by conjugation, then the G-orbit of H_1 is partitioned into H_j orbits, and because the orbit $\{H_j\}$ is absent, the size of each of these is a multiple of p. Thus $|G(H_1)|$ is congruent to 0 (mod p), in violation of the conclusion of the previous paragraph, so this implies that the G-orbit of H_1 consists of all of $\{H_1, H_2, ..., H_m\}$, which we set out to prove.

Finally, by the orbit-stabiliser theorem the size of the orbit is always a factor of the order of the group G, so that m divides kp^n. But p does not divide m, which means that m is a factor of k. □