CHAPTER V

Groups

5.1. Introduction.

Groups are the most investigated topic for superstructures with one operation. We develop some basic ideas in group theory, study normal subgroups, the three isomorphism theorems, composition series and introduce Sylow's theorems. The theory of zargonions leads us to ask what impact zargonions have on the theory of simple groups, where the claim has been made that a complete classification was achieved after monumental efforts finally in 2008. This is dealt with in chapter IX. The classification of Lie algebras using Dynkin diagrams, in [Ad15] chapter V, is revisited and expanded. This leads to the further classification of simple groups.

5.2. Basic ideas in group theory.

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*, written additively as $(-a)$, 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.

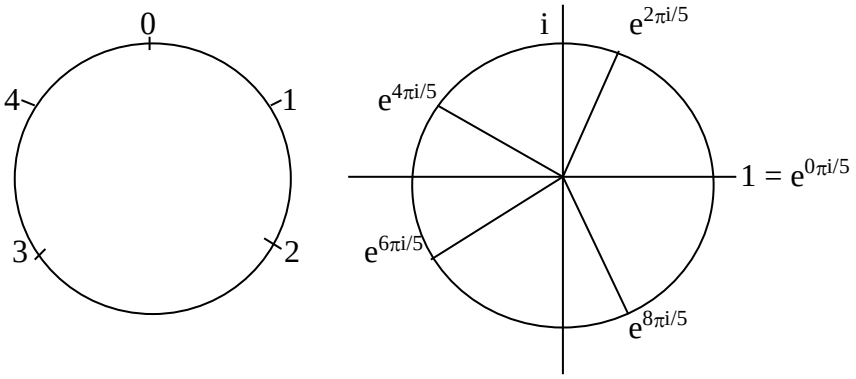
A *permutation* is a bijection of a finite set to itself. A permutation which interchanges cyclically m objects of a set {1, 2, ..., m} forms an abelian group called a cycle of degree m. This permutation is obtained from a power by specifying that a^{m-1} is the m^{th} element and the cyclic permutation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

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

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).

In what follows, though we represent |G| as the number of elements of G, we could change the text to represent |G| as the underlying set of G, forgetting its additive or multiplicative structure, because there is a bijection between the *number* of elements of a set and the *set* of its distinct elements.

We have represented a finite abelian group by cycles. Each cyclic group of order n may be thought of as additive in that

a (mod n) + b (mod n) = (a + b) (mod n).

The element 0 belongs to an additive group.

To represent an abelian group multiplicatively, suppose all elements are integers. Consider a multiplicative group within a subset of a cyclic additive group, so it contains 1. If 0 belongs to this group then we assume r0 = s0 for $r \neq s$, and since all elements of a group have multiplicative inverses, this includes 0, so r = s, a contradiction.

Theorem 5.2.1. *Let* G, + *be a cyclic additive abelian group of order* n *and the set* H ⊆ G. *Then if* H, × *is a multiplicative group* (mod n) *of maximal order, then* n *is prime*.

Proof. 0 does not belong to this subset, so the order of H is $n - 1 \geq 1$. For a finite multiplicative group, we can consider a negative number (–k) (mod n) as (n – k).

If n is not prime then there exist numbers t and $u \neq 0$ less than n with n = tu. Thus t and u belong to the maximal subset, but their product is 0 (mod n), a contradiction. □

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.

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

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

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 5.2.2. *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 5.2.3. 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 5.2.4. 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 5.2.5. 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 5.2.6. The *transposition* of elements a and b given by the composite ab is ba.

Theorem 5.2.7. *The complement* $C(Z)$ *of the overlaps* $a \in A$ *and* $b \in B$ *in a noncommutative transposition* $ab \rightarrow ba$ *of* Z *belongs to a permutation and is unchanged by the transposition, the remaining elements are changed.*

Proof. By lemma 5.2.2 [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 $ab = g \to h(g)$, such that

$$h(ab) = h(a)h(b).$$

An *automorphism* is a homomorphism $G \to G$.

Theorem 5.2.8. *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 $h: G \to G'$, if it satisfies

$$h(a)h(k) = h(a) = h(k)h(a),$$

in other words it is the identity of G′.

From chapter III, section 12 on superstructure theory, we met the Yoneda lemma. In the special case where a category is a finite group, this implies Cayley's theorem, that any group can be uniquely represented by finite permutations under composition of permutations. We now prove this directly.

Proof. Let G be a multiplicative group of order m. The function $f_g: G \to G$ defined by $f_g(x) = gx$ is a permutation, because it has an inverse $f_{g^{-1}}$. Thus multiplication by g is a bijective mapping $G \to G$.

We need to prove that f_g is isomorphic to G. Denoting composition . of permutations written here as a function from right to left, the surjective function $T: G \to S_m$ defined for every $g \in G$ by $T(g) = f_g$ is a group homomorphism, since comparing the leftmost and rightmost expressions below

$$(f_g.f_h)(x) = f_g(f_h(x)) = f_g(hx) = g(hx) = (gh)x = f_{gh}(x).$$

This homomorphism is also injective, since if T(g) is the identity, then gx = g for all g ∈ G, and the kernel is trivial since if x is the identity e

g = ge = e. □

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 5.2.9. *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 5.2.10. (**Lagrange's subgroup theorem**). *The order of a finite subgroup* S ⊆ G *divides the order of a finite group containing it*. □

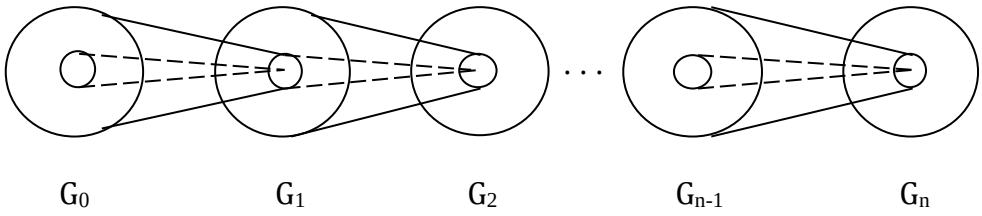
An idea using kernels occurs in homology theory, discussed in volume II. A sequence of groups G_0, ..., G_n and homomorphisms f_1, ..., f_n is called *exact* if the image (or the codomain) of each homomorphism is equal to the kernel of the next:

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \ldots \xrightarrow{f_n} G_n,$$

that is

$$\mathrm{im}(f_k) = \ker(f_{k+1}).$$

We will show this again in the diagram



where the larger circle is the group, the smaller circle is its kernel, and the kernel maps to the identity. □

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 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 $a \in B$ then $a^{-1} \in B$, so $ea^{-1} \in B$. Further, if the element $b \in B$, 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, $A \cap B$ is a subgroup of G. □

Remark 5.4.3. The probability P(A) and P(B) of two events A and B respectively, satisfies

$$P(A \cap B) = P(A)P(B) \quad (1)$$

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 ℕ. But now lemma 5.4.2 demonstrates a mapping between groups and sets, which in the categorical language of chapter III, section 12, 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. □

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

$$f(h) = h = hnN \text{ (because } n \in N)$$
$$= gN,$$

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 5.4.10. (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 → 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 ∈ 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, 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 × n invertible matrices, meaning they have a multiplicative inverse, together with the operation of ordinary matrix multiplication. GL(n, 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

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

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, ℂ), one takes a homomorphism into the projective general linear group PGL(n, ℂ). In other words, a projective representation is a representation modulo the center.

5.6. The standard classification of simple groups.

Finite simple groups have currently two classifications, the first 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.

Otherwise they were thought as one of 26 *exceptions*. The number of elements of the 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, the set of permutations of elements of 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

$$|G| = |G(x)|.|G_x|. \quad \square$$

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

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

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. □

5.9. Composition series.

A *subnormal series* of a group G is a sequence of subgroups, each a normal subgroup of the next. We write this as

$$1 = E_0 \lhd E_1 \lhd ... \lhd E_n = G.$$

It is not necessarily the case that E_k is a normal subgroup of G, only that it is a normal subgroup of E_{k+1}.

The quotient groups E_{k+1}/E_k are called *factor groups* of the series.

When $E_k \neq E_{k+1}$ we say the series is *without repetition*, so that each E_k is a proper subgroup of E_{k+1}.

The *length*, n, of the series is the number of strict inclusions $E_k \subset E_{k+1}$.

A subnormal series $1 = F_0 \lhd F_1 \lhd ... \lhd F_n = G$ in subgroups F_k is a *refinement* of a subnormal series in E_j given by $1 = E_0 \lhd E_1 \lhd ... \lhd E_n = G$, with $j \leq k$ if $\{E_j\} \subseteq \{F_k\}$.

A *composition series* of a group G is a subnormal series of finite length

$$1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G,$$

with strict inclusions, where each H_k is a maximal strict normal subgroup of H_{k+1}. A proper normal subgroup M is called a maximal normal subgroup of G if $M \lhd H \lhd G$ implies $H = G$ or $H = M$. An alternative way of saying this is that each factor group H_{k+1}/H_k is simple. The factor groups are called composition factors.

A subnormal series is a composition series if and only if it is of maximal length. If a group G has a composition series, then any subnormal series can be refined to a composition series, informally, by inserting subgroups into the series up to maximality.

Theorem 5.9.1. Every finite group G has a composition series.

Proof. We use induction on |G|. If |G| = 1 then the composition series is just $G = H_0 = 1$. Assume that |G| > 1 and the result is true for all groups of order less than |G|. Since G is finite, it has at least one maximal normal subgroup N. Then |N| < |G|, so by induction N has a composition series $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_{n-1} = N$ with $H_k \lhd H_{k+1}$ and H_{k+1} simple for $k = 0, \ldots, n-2$. Putting $H_n = G$ gives the composition series $1 = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$ for G, since $H_{n-1} \lhd H_n$ and $H_n/H_{n-1} = G / N$, which is simple. □

A group may have more than one composition series. However, the Jordan-Hölder theorem states that any two composition series of a given group are equivalent. That is, they have the same composition length and they have the same composition factors up to permutation and isomorphism.

The Zassenhaus lemma is useful to prove the Schreier refinement theorem – that any two equivalent subnormal series have equivalent refinements.

Theorem 5.9.2. (Zassenhaus, or butterfly lemma). Given subgroups $A \lhd B$ and $C \lhd D$ of a group G, then

(i) $A(B \cap C) \lhd A(B \cap D)$,
(ii) $C(D \cap A) \lhd C(D \cap B)$,
(iii) $(A \cap D)(B \cap C) \lhd (B \cap D)$,

and there is an isomorphism

(iv) $\frac{A(B \cap D)}{A(B \cap C)} \leftrightarrow \frac{C(D \cap B)}{C(D \cap A)}$.

Proof. If $p \in (A \cap D)$ and $q \in (B \cap D)$ then $qpq^{-1} \in (A \cap D)$. Now $qpq^{-1} \in A$, since $p \in A$ and $A \lhd D$, but also $qpq^{-1} \in D$, since $p, q \in D$. Hence we have $A(B \cap C) \lhd A(B \cap D)$, and similarly $C(D \cap A) \lhd C(D \lhd B)$.

Thus the subset N, defined by

$N = (A \cap D)(B \cap C)$

is a normal subgroup of $(B \cap D)$, because it is generated by two normal subgroups.

Using the symmetry, it is sufficient to show that there is an isomorphism

$\frac{A(B \cap D)}{A(B \cap C)} \leftrightarrow \frac{(B \cap D)}{N}$.

Define $\theta: A(B \cap D) \to (B \cap D)/N$ by $\theta: aq \to qN$, where $a \in A$ and $q \in (B \cap D)$. Now θ is well-defined: if $aq = a'q'$ where $a' \in A$ and $q' \in (B \cap D)$, then

$(a')^{-1}a = q'q^{-1} \in A \cap (B \cap D) = (A \cap D) \subseteq N$.

Also θ is a homomorphism: $aqa'q' = a''qq'$, where $a'' = a(qa'q^{-1}) \in A$ (since $A \lhd B$), and so

$\theta(aqa'q') = \theta(a''qq) = qq'N = \theta(aq)\theta(a'q')$.

It is routine to check that θ is surjective, since $(B \cap D) \subseteq A(B \cap D)$.

To prove $\ker \theta = A(B \cap C)$, suppose that aq is in the kernel of θ. This has the consequence that $q \in N = (A \cap D)(B \cap C)$. Thus we can write $q = a'q'$ where $a' \in (A \cap D) \subset A$ and $q' \in (B \cap C)$. It follows that $aq = aa'q' \in A(B \cap C)$.

The first isomorphism theorem completes the proof. □

Definition 5.9.3. Two subnormal series $(K_i)_{i=0}^n$, $(L_i)_{i=0}^n$ of the same group G are isomorphic if there is a bijection $\mathcal{h}\{K_{i+1}/K_i, 0 \le i \le n-1\} \leftrightarrow \{L_{i+1}/L_i, 0 \le i \le n-1\}$ for $i = 0, \ldots, n-1$.

Theorem 5.9.3. (Schreier) Any two subnormal series of a group have equivalent refinements.

Proof. Consider two subnormal series

$1 = K_0 \lhd K_1 \lhd \ldots \lhd K_n = G$,
$1 = L_0 \lhd L_1 \lhd \ldots \lhd L_n = G$.

For each $0 \le i \le n-1$ define a chain of groups $K_{i\,j}$ for $0 \le j \le m$ given by

$K_{i\,0} = K_i$ for $0 \le i < n$.

It follows that

$$1 = K_{0\,0} \lhd K_{0\,1} \lhd \ldots \lhd K_{0\,m-1} \lhd K_{1\,0}$$
$$\lhd K_{1\,1} \lhd \ldots \lhd K_{1\,m-1} \lhd K_{2\,0}$$
$$\ldots$$
$$\lhd K_{n-1\,1} \lhd \ldots \lhd K_{n-1\,m-1} \lhd K_{n-1\,m}$$

is a subnormal series by part (i) of the Zassenhaus lemma, which refines the original series of $K_{i\,j}$'s.

Observe that $L_{j\,0} = L_j$ for $0 \leq j \leq m$

$$1 = L_{0\,0} \lhd L_{0\,1} \lhd \ldots \lhd L_{0\,n-1} \lhd L_{1\,0}$$
$$\lhd L_{1\,1} \lhd \ldots \lhd L_{1\,n-1} \lhd L_{2\,1}$$
$$\ldots$$
$$\lhd L_{m-1\,1} \lhd \ldots \lhd L_{m-1\,n-1} \lhd L_{m-1\,n}$$

by part (ii) of the lemma.

By part (iv)

$$\frac{K_{i\,j+1}}{K_{i\,j}} = \frac{K_i(K_{i+1} \cap L_{j+1})}{K_i(K_{i+1} \cap L_j)} \leftrightarrow \frac{L_j(K_{i+1} \cap L_{j+1})}{L_j(K_{i+1} \cap L_{j+1})} = \frac{L_{j\,i+1}}{L_{j\,i}}.$$

This shows the two refinements are isomorphic. The desired isomorphism is given by $(K_{i\,j}) = L_{j\,i}$.

The proof is concluded by deleting repeated groups in the chain. □

Since a subnormal series is a composition series if and only if it is of maximal length, the refinements given by the Schreier theorem must be those of the composition series themselves, and the Jordan-Hölder theorem for composition series is proved. □

A finite group is called solvable if it has a composition series whose composition factors are all abelian, and hence isomorphic to $\mathbb{Z}_p$ for primes p.

The term solvable group arose from the claimed use of the symmetric group in describing the absence of solutions of certain polynomial equations by radicals. As will be proved in the next chapter, this solvability model is false, and indeed all polynomial equations are solvable by radicals. A possible reason why the contamination has not spread as far as might be expected is that such mathematics has no correct applications.

The theory needed to describe the new mathematics to replace this is not one of symmetries under transformations of one operator, but a theory of the comparison of states utilising the features of many operators. For instance, to solve a polynomial equation requires its splitting into bijective multiple states, where each state is transformed under multiple operations (in the case of polynomials + and ×) so that the solution of one set of states by known methods can be compared with the solution of the remaining states to be computed from them. The structure of these comparisons is more complex than any that can be achieved with one operator, and generally cannot be reduced to the one operator case.

5.10. Normal subgroups not forming a modular lattice.

Despite the conventional wisdom, normal subgroups do not always form a modular lattice.

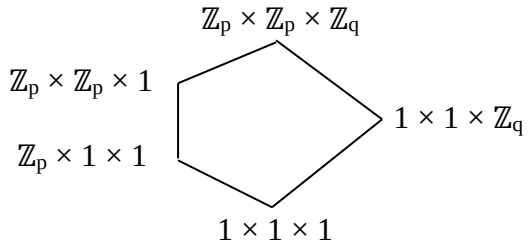
The Jordan-Hölder theorem splits groups into simple groups. Like a prime factorisation, the number of simple groups in a Jordan-Hölder composition series is unique up to order of factors

of the simple groups, so the number of factors is unique too. When the groups are abelian, the analogy of normal subgroups of a group to prime numbers in a product is a direct one.

The particular lattice that is useful to compare with groups is derived from multiplication. Whole numbers form a lattice under meet, $\wedge$, as their greatest common factor (so this is small) and join, $\vee$, as their least common multiple (which is large).

We saw in chapter II, section 5, that a Hasse diagram for a nondistributive lattice must contain at least a diamond lattice M_3 or a pentagon lattice N_5. It is well known that there exist lattices for groups containing M_3 diagrams, so these are not distributive lattices. If a lattice is modular it contains no diagram of type N_5. We will construct a lattice of normal subgroups of N_5 type.

This is obtained from the Hasse diagram for a pentagon diagram of type N_5 in the section referred to. Let p and q be distinct primes and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$ be a group viewed as a maximum join. Then on one leg of the N_5 pentagon it contains normal subgroups $\mathbb{Z}_p \times \mathbb{Z}_p \times 1$, $\mathbb{Z}_p \times 1 \times 1$ and the meet $1 \times 1 \times 1$, and on the other the normal subgroups $1 \times 1 \times \mathbb{Z}_q$ and $1 \times 1 \times 1$, shown in the Hasse diagram



5.11. Continuous groups.

The half-finished, half-unfinished interval [1, 0[of positive real numbers r where $1 \geq r > 0$ generates by multiplication a group for such numbers r_1 and r_2 to give a positive real number r_3 with

$$r_1 r_2 = r_3,$$

where the inverses belong to the interval defined by $r \geq 1$.

The punctured interval [–1, 1] with 0 excluded also generates a multiplicative group of real numbers s.

For a finite group with elements g, we can form a continuous set with elements of type rg or sg, forming in an obvious way a continuous group.

Likewise the punctured complex disk with unit norm, and the punctured quaternion 4-disk also form groups in a similar way, and these may be applied to elements of finite groups, in the case of quaternions, by left or right multiplication, or by both, so that for quaternions q, r, s and t and elements of a group g_1 and g_2, we could specify

$$(qg_1r)(sg_2t) = qsg_1g_2rt.$$

Note that we are always at liberty, if we wish, on being provided with a representation of group elements which operate as if, say, they were +g or –g, to ignore this representation and treat the group elements purely formally from their group multiplication tables. This is the dual of the Grothendieck construction of chapter III, section 12. In this circumstance, the allocation of the continuous set of elements, when they include negative numbers, provides a structure for the continuous group, which differs from its structure when the negative elements of g are not distinguished in the codomain of this mapping from the continuous set of elements applied to them. □

5.12. Dynkin diagrams.

The best introduction to the theory of Lie algebras and root systems is probably Roger Carter's in *Lectures on Lie groups and Lie algebras* [CSM95]. Our purpose in following closely the development there is so that it is embedded in this work, but we do not take its development as far as discussing groups of Lie type. To generalise $sl_n(\mathbb{C})$ to $gl_n(\mathbb{C})$ see [1Ca72], [1Ca05] and for Lie groups [1Ca93].

A *Lie algebra* is a vector space g over a field $\mathbb{F}$ in which is defined a multiplication

$$g \times g \to g,$$
$$x, y \to [x, y],$$

where [x, y] is called the *Lie bracket*, satisfying the axioms

(i) [x, y] is linear in x and y.
(ii) [x, x] = 0 for all $x \in g$.
(iii) The *Jacobi identity* [x, [y, z]] + [y, [z, x]] + [z, [x, y]] holds.

The set of n × n matrices, A, B, ... with entries in a field $\mathbb{F}$ can be made into a Lie algebra with Lie bracket [A, B] by setting

$$[A, B] = AB - BA,$$

and this is denoted by $gl_n(\mathbb{F})$, the general linear Lie algebra over the field $\mathbb{F}$.

It follows for these matrices that

$$[A + A', B + B'] = [A, B] + [A, B'] + [A', B] + [A', B']$$
$$[A, A] = 0$$
$$[A, B] = -[B, A],$$

and the Jacobi identity holds

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0, \tag{1}$$

since this is

$$\begin{aligned} &ABC - BAC - CAB + CBA \\ &+ BCA - CBA - ABC + ACB \\ &+ CAB - ACB - BCA + BAC \\ &\quad = 0, \end{aligned}$$

but the Lie bracket is not generally associative

$$[[A, B], C] \neq [A, [B, C]].$$

Let $sl_n(\mathbb{C})$ be the set of n × n matrices with complex entries, a zero sum of diagonal entries, so the trace tr is zero, and with Lie brackets.

Example 5.12.1. The Lie algebra of a 2 × 2 intricate matrix has a $sl_2(\mathbb{C})$ basis of i, α, ϕ, since

$$[i, \alpha] = -2\phi,\ [i, \phi] = 2\alpha \text{ and } [\alpha, \phi] = 2i,$$

and all of i, α, ϕ are matrices with zero trace.
The trace tr, of the matrix Lie bracket is zero. For instance, since

$$tr(AB) = \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij}B_{ji} = \sum_{j=1}^{n} \sum_{i=1}^{n} B_{ji}A_{ij} = tr(BA),$$

if A and $B \in gl_n(\mathbb{C})$ then

$$tr[A, B] = tr(AB - BA) = tr(AB) - tr(BA) = 0, \tag{2}$$

for any two n × n matrices. As we have seen in chapter II, the diagonal trace of an intricate actual number α and the hyperintricate traces involving αs are all zero, so for $2^n \times 2^n$ matrices, equation (2) reduces to the case where the real hyperintricate trace is zero,

$$tr1[A, B] = tr1(AB - BA) = tr1(AB) - tr1(BA) = 0, \tag{3}$$

where 1 is interpreted as a hyperintricate diagonal 1.

Thus $gl_n(\mathbb{C})$ contains $sl_n(\mathbb{C})$, which is a nontrivial proper subspace when $n > 1$. By a subspace we mean the set of all [A, B].

If h is the set of diagonal matrices of $sl_n(\mathbb{C})$ where tr is zero, this is a subalgebra of rank $n - 1$. Further, $[h, h] = 0$, so h is commutative.

For finitely many summands, direct sums are the same as direct products, where for sets this is the Cartesian product. For infinite subspaces, for direct sums all but a finite number of coordinates must be zero, whilst for direct products all but a finite number of multiples must be 1. Let E_{ij} be an elementary matrix, the unit diagonal matrix with just rows i and j swapped. Then

$$sl_n(\mathbb{C}) = h \oplus \sum_{i \neq j} \mathbb{C}E_{ij}, \tag{4}$$

where $\oplus$ is a direct sum of subspaces. This is because row $i = 1$ can be written as a linear combination of $j - 1$ terms in E_{ij} where $i < j$, down to row $n - 1$ as a linear combination with 1 term, and similarly for $j < i$, which supplies sufficient degrees of freedom to write complex elements of (4) uniquely.

Given a vector space **V** over a field $\mathbb{F}$, the span of a set **S** of vectors (not necessarily finite) is defined as the intersection **W** of all subspaces of **V** that contain **S**. **W** is referred to as the subspace spanned by **S** or by the vectors in **S**. Conversely we say **S** spans **W**.

By a dual space of a linear vector space **V**, if we interpret **V** as the space of *columns* of n real (Eudoxus) numbers, $\mathbb{U}$, or complex numbers, $\mathbb{C}$, its dual space $\mathbf{V}^*$ is typically written as the space of *rows* of n Eudoxus or complex numbers. If **V** consists of the linearly independent space of geometrical Eudoxus vectors in the plane, then the level curves of an element of $\mathbf{V}^*$ form a family of parallel lines in **V**. So an element of $\mathbf{V}^*$ can be intuitively thought of as a particular family of parallel lines covering the plane. For a linearly independent space **V** of dimension n, the elements of **V*** are parallel hyperplanes of dimension n. In the finite case the space **V*** has the same dimension as **V** and the dual of the dual is isomorphic to the original space: $\mathbf{V}^{**} = \mathbf{V}$. If the vectors of **V** are linearly dependent, so the rank r is less than the dimension n of **V**, then the rank of **V*** is r, being the number of linearly independent basis elements of **V***.

Now choose a representative x of h

$$x = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ & & \ddots \\ 0 & & \lambda_n \end{bmatrix},$$

with $\lambda_1 + ... + \lambda_n = 0$, so these are linearly dependent of rank $n - 1$, then let

$$[xE_{ij}] = (\lambda_i - \lambda_j)E_{ij},$$

so we have a mapping

$$x \to (\lambda_i - \lambda_j).$$

Note that we have $n(n - 1)$ 1-dimensional representations of h arising in this way, being the number of combinations of $(\lambda_i - \lambda_j)$ with $i \neq j$. These are called the *roots* of $sl_n(\mathbb{C})$ with respect to h. Let Φ be this set of roots. We will show how it lies in the dual space h*.

If $\beta \in \Phi$ then $-\beta \in \Phi$ also, since the map $x \to (\lambda_j - \lambda_i)$ is the negative of the map $x \to (\lambda_i - \lambda_j)$. Thus the roots are not independent. The roots do however span h*. For define $\beta_i \in \Phi$ by

$$\beta_i(x) = \lambda_i - \lambda_{i+1}.$$

Then $\beta_1, \beta_2, \ldots \beta_{n-1}$ are linearly independent and form a basis of h*. Let $\Pi = \{\beta_1, \beta_2, \ldots \beta_{n-1}\}$. Π is called the set of fundamental roots, or simple roots. We consider the way the roots are expressed as linear combinations of the fundamental roots. The root $x \to (\lambda_i - \lambda_j)$ is equal to

$\beta_1 + \beta_2 + \ldots + \beta_{n-1}$ if $i < j$

$-(\beta_1 + \beta_2 + \ldots + \beta_{n-1})$ if $j < i$.

Thus each root in Φ is a linear combination of fundamental roots with coefficients in $\mathbb{Z}$, and these integers can all be partitioned into nonnegative combinations Φ^+ of Π and nonpositive combinations Φ^- so that

$\Phi = \Phi^+ \cup \Phi^-$ and $\Phi^+ = -\Phi^-$.

Given an element x of a Lie algebra g, we define the *adjoint* action of x on g as the map

$ad_x: g \to g$

where for all z in g

$ad_x(z) = [x, z]$.

Let g be a Lie algebra over a field $\mathbb{F}$. Then the linear mapping $x \to ad_x$ is a representation of the Lie algebra and is called the adjoint representation of the algebra. The Lie bracket is, by definition, obtained from two operators:

$[ad_x, ad_y] = ad_x \circ ad_y - ad_y \circ ad_x$

where $\circ$ denotes composition of linear maps. By the Jacobi identity we have

$ad_x \circ ad_y(z) - ad_y \circ ad_x(z) = [x, [y, z]] - [y, [x, z]] = [[x, y], z]$

$= ad_{[x, y]}(z)$.

Now, supposing g is of finite dimension, the trace of the composition of two such maps defines a bilinear form

$\langle x, y \rangle = tr(ad_x \circ ad_y)$,

where $\langle x, y \rangle$ is the *Killing form* on g. The name Killing form first appeared in a paper of Armand Borel in 1951. Since tr(AB) = tr(BA), the Killing form is symmetric

$\langle x, y \rangle = \langle y, x \rangle$.

The Killing form is an invariant form, in the sense that it is associative

$\langle [x, y], z \rangle = \langle x, [y, z] \rangle$,

since

$\langle [x, y], z \rangle = tr([x, y]z) = tr(xy\, z - yx\, z) = tr(xy\, z) - tr(y\, xz)$.

Similarly,

$\langle x, [y, z] \rangle = tr(x\, [y, z]) = tr(x\, yz) - tr(x\, zy)$.

Finally, tr(y(x z)) = tr((x z)y).

The Killing form on g is nondegenerate in that

$\langle x, y \rangle = 0$ for all $y \in g$ implies $x = 0$.

We may restrict the Killing form on g to h, to give a map $h \times h \to \mathbb{C}$. It can be shown that this map is nondegenerate on h, so that

$x \in h$ and $\langle x, y \rangle = 0$ for all $y \in g$ implies $x = 0$.

We may thus define a map $h \to h^*$ given by $x \to f_x$ where

$f_x(y) = \langle x, y \rangle$ for $x, y \in h$,

which is a linear map $h \to h^*$. Thus each element of h* has a form f_x for just one $x \in h$, so we can define a map $h^* \times h^* \to \mathbb{C}$ by

$\langle f_x, f_y \rangle = \langle x, y \rangle$ for $x, y \in h$.

We may restrict this linear form to the real (Eudoxus) vector space $h^*_{\mathbb{U}}$. It can be shown from the representation of i as an integer matrix that its values lie in $\mathbb{U}$. Thus we have a map

$$h^*_{\mathbb{U}} \times h^*_{\mathbb{U}} \to \mathbb{U}.$$

This map has the property that

$$\langle \lambda, \lambda \rangle \geq 0 \text{ for all } \lambda \in h^*_{\mathbb{U}}.$$

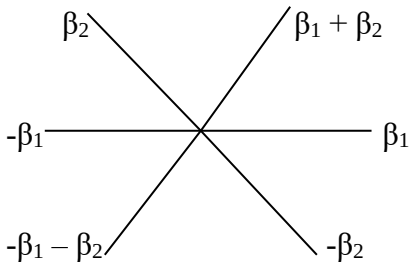
Furthermore $\langle \lambda, \lambda \rangle = 0$ implies $\lambda = 0$, so that the scalar product on $h^*_{\mathbb{U}}$ is positive definite. $h^*_{\mathbb{U}}$ is therefore a Euclidean space.

This Euclidean space $h^*_{\mathbb{U}}$ contains the set of roots Φ. The properties of the configuration formed by the roots in $h^*_{\mathbb{U}}$ is important in the classification of the simple Lie algebras g.

Example 5.12.2. Let $g = sl_2(\mathbb{C})$. Then dim h = 1. Let $\Pi = \{\beta_1\}$. Then $\Phi = \{\beta_1, -\beta_1\}$. The configuration formed by Φ in the 1-dimensional space $h^*_{\mathbb{U}}$ is

$$-\beta_1 \text{ ——— } 0 \text{ ——— } \beta_1$$

For $g = sl_3(\mathbb{C})$, dim h = 2, and $\Pi = \{\beta_1, \beta_2\}$, so $\Phi = \{\beta_1, \beta_2, \beta_1 + \beta_2, -\beta_1, -\beta_2, -\beta_1 - \beta_2\}$. The configuration formed by Φ in the 2-dimensional Euclidean space $h^*_{\mathbb{U}}$ is



The configuration formed by the root system Φ is best understood by introducing a certain group of non-singular linear transformations of $h^*_{\mathbb{U}}$ called the *Weyl group*. For each $\beta \in \Phi$ let s_β: $h^*_{\mathbb{U}} \to h^*_{\mathbb{U}}$ be the map defined by

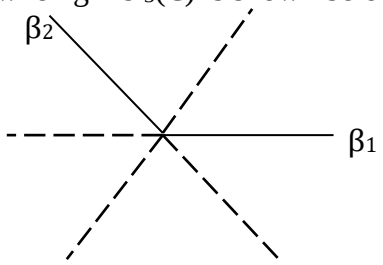
$$s_\beta(\lambda) = \lambda - 2\frac{\langle \beta, \lambda \rangle}{\langle \beta, \beta \rangle}\beta.$$

Note that $s_\beta(\beta) = -\beta$ and $s_\beta(\lambda) = \lambda$ whenever $\langle \beta, \lambda \rangle = 0$. Thus s_β is the reflection in the hyperplane orthogonal to β. Let W be the group generated by the maps s_β for all $\beta \in \Phi$. W is called the Weyl group.

W has favourable properties. Firstly it permutes the roots, that is, $w(\beta) \in \Phi$ for every $\beta \in \Phi$ and $w \in W$. Consequently W is finite, because there are only a finite number of permutations of Φ, in which Φ spans the linear transformations $h^*_{\mathbb{U}}$, where each of these permutations comes from just one such linear transformation. We also have $\Phi = W(\Pi)$, which means given any $\beta \in \Phi$, there exists a $\beta' \in \Pi$ and $w \in W$ such that $\beta = w(\beta')$. Furthermore, W is generated by the $s_{\beta'}$ for $\beta' \in \Pi$.

The importance of the Weyl group is that it enables us to reconstruct the full root system Φ given only the set Π of fundamental roots. For given Π the Weyl group is determined, being the group generated by the reflections $s_{\beta'}$ for $\beta' \in \Pi$. The root system Φ is then determined, since $\Phi = W(\Pi)$. Thus, given Π, the root system Φ is obtained by successive reflections $s_{\beta'}$ until no further vectors can be obtained.

An example when $g = sl_3(\mathbb{C})$ is shown below



Given β_1 and β_2 the remaining roots are obtained by reflecting successively by s_{β_1} and s_{β_2}. We note that

$$s_{\beta_i}(\beta_j) = \beta_j - 2\frac{\langle \beta_i,\ \beta_j\rangle}{\langle \beta_i,\ \beta_i\rangle}\,\beta_i.$$

If $\beta_i, \beta_j \in \Pi$ with $i \neq j$, then $s_{\beta_i}(\beta_j)$ is a root, and so is a $\mathbb{Z}$-combination of β_i and β_j. Since the coefficient of β_j is 1, the coefficient of β_i must be a nonnegative integer, because the given root lies in Φ^+. It follows that

$$2\frac{\langle \beta_i,\ \beta_j\rangle}{\langle \beta_i,\ \beta_i\rangle} \in \mathbb{Z} \text{ and is} \leq 0.$$

We define $A_{ij} = 2\frac{\langle \beta_i,\ \beta_j\rangle}{\langle \beta_i,\ \beta_i\rangle}$,
where the elements of A_{ij} are called *Cartan numbers*, and the matrix they form the *Cartan matrix*. We have $A_{ij} \in \mathbb{Z}$, where $A_{ii} = 2$ and A_{ij} for $i \neq j$ is ≤ 0.

Let θ_{ij} be the angle between β_i and β_j. This angle can be found from the cosine formula

$$< \beta_i, \beta_j > = < \beta_i, \beta_i >^{1/2} < \beta_j, \beta_j >^{1/2} \theta_{ij}.$$

Therefore

$$4\cos^2\theta_{ij} = 2\frac{\langle \beta_i,\ \beta_j\rangle}{\langle \beta_i,\ \beta_i\rangle}.2\frac{\langle \beta_j,\ \beta_i\rangle}{\langle \beta_j,\ \beta_j\rangle},$$

giving

$$4\cos^2\theta_{ij} = A_{ij}A_{ji}.$$

We will write $n_{ij} = A_{ij}A_{ji}$. Then $n_{ij} \in \mathbb{Z}$ and $n_{ij} \geq 0$. Further, because

$$-1 \leq \cos\theta_{ij} \leq 1$$

we get

$$0 \leq 4\cos^2\theta_{ij} \leq 4,$$

and since when $i \neq j$, $\theta_{ij} \neq 0$, we obtain

$$0 \leq 4\cos^2\theta_{ij} < 4.$$

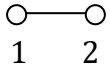
Thus the only possible values of n_{ij} are 0, 1, 2 and 3.

We will now encode these results about the system Π of fundamental roots in terms of a graph. The *Dynkin diagram* Δ of g is the graph with nodes labelled 1, ..., m mapping bijectively to the set Π of fundamental roots, so that the nodes i, j with $i \neq j$ are joined by n_{ij} bonds.

Example 5.12.3. Let $g = sl_3(\mathbb{C})$. Then $\Pi = \{\beta_1, \beta_2\}$ and

$$s_{\beta_1}(\beta_2) = \beta_1 + \beta_2,\ s_{\beta_2}(\beta_1) = \beta_1 + \beta_2,$$

thus $A_{12} = A_{21} = -1$, and $n_{12} = 1$, giving the graph Δ

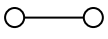


The Dynkin diagram is uniquely determined by g. The choice of fundamental system Π does not matter, since it can be shown that two fundamental systems Π_1 and Π_2 have the property that $\Pi_1 = w(\Pi_2)$ for some $w \in W$.

The Dynkin diagram of g has the following properties. Δ is a connected graph provided g is a nontrivial simple Lie algebra. Any two nodes are joined by at most 3 bonds. Let $Q(x_1, ..., x_m)$ be the quadratic form

$$Q(x_1, \cdots, x_m) = 2\sum_{i=1}^{m} x_i^2 - \sum_{i,j,i\neq j}^{m} \sqrt{n_{ij}}\, x_i x_j.$$

This quadratic form is determined by the Dynkin diagram. For example if Δ is



then we have

$$Q(x_1, x_2) = 2x_1^2 + 2x_2^2 - 2x_1x_2.$$

The quadratic form $Q(x_1, ..., x_m)$ is positive definite because it contains the scalar product in

$$Q(x_1, \cdots, x_m) = 2\left\langle \frac{\sum_{i=1}^{m} x_i\beta_i}{\sqrt{\beta_i,\beta_i}}, \frac{\sum_{i=1}^{m} x_i\beta_i}{\sqrt{\beta_i,\beta_i}} \right\rangle.$$

We will consider the problem of determining all graphs Δ with the above properties.

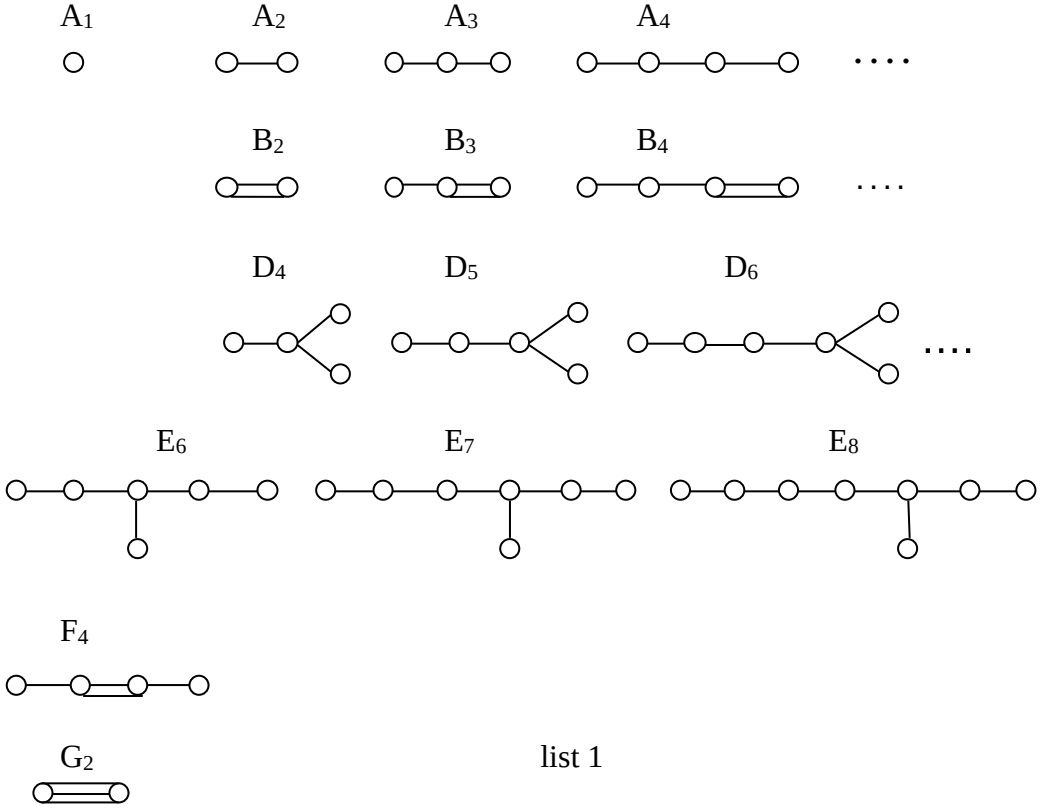
Theorem 5.12.4. *Consider graphs* Δ *with the following properties*:

(i) Δ *is connected*

(ii) *The number of nodes joining any two bonds is* 0, 1, 2 *or* 3

(iii) *The quadratic form* Q *determined by* Δ *is positive definite*.

Then Δ *must be one of the graphs in the following list*:



list 1

We first consider to what extent the Dynkin diagram determines the matrix of Cartan integers. Recall that

$$n_{ij} = A_{ij}A_{ji} \qquad i \neq j,$$

and that the A_{ij} are integers ≤ 0. Furthermore $A_{ij} = 0$ if and only if $A_{ji} = 0$.

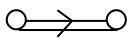
If $n_{ij} = 0$ then $A_{ij} = A_{ji} = 0$. If $n_{ij} = 1$ we must have $A_{ij} = -1$ and $A_{ji} = -1$. However, if $n_{ij} = 2$ we have two possibilities: either $A_{ij} = -1$ and $A_{ji} = -2$ or $A_{ij} = -2$ and $A_{ji} = -1$, and because

$$A_{ij} = 2\frac{\langle \beta_i,\ \beta_j\rangle}{\langle \beta_i,\ \beta_i\rangle},$$

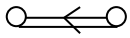
we obtain

$$\frac{A_{ij}}{A_{ji}} = \frac{\langle \beta_j,\ \beta_j\rangle}{\langle \beta_i,\ \beta_i\rangle}.$$

In the first case, we have $\langle \beta_i,\ \beta_i\rangle > \langle \beta_j,\ \beta_j\rangle$, and in the second case $\langle \beta_i,\ \beta_i\rangle < \langle \beta_j,\ \beta_j\rangle$, which we notate by putting an arrow on the Dynkin diagram pointing towards the long root, where the arrow can be thought of as an inequality between the root lengths. In the first case we have the diagram

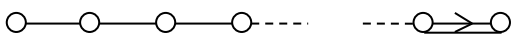


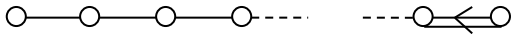
and for the second case



Likewise if $n_{ij} = 3$ there are two possible factorisations of $n_{ij} = A_{ij}A_{ji}$ which can be distinguished by putting similar directional arrows on the triple bond.

In the cases where $\Delta = B_2$, F_4 and G_2 in list 1, the diagrams are symmetric, so there is no difference, but when $\Delta = B_m$ for $m > 2$ we can find two different types of graph, which we denote by B_m and C_m in the diagrams below.

B_m 

C_m 

Thus for B_m the last fundamental root is shorter than the others, and for C_m it is longer. □

Written explicitly the Dynkin diagrams correspond to the matrices of Cartan integers

$$A_m = \begin{bmatrix} 2 & -1 & & & & & & \\ -1 & 2 & -1 & & & & 0 & \\ & -1 & 2 & -1 & & & & \\ & & -1 & & & & & \\ & & & & & -1 & & \\ & & 0 & & -1 & 2 & -1 & \\ & & & & & -1 & 2 & -1 \\ & & & & & & -1 & 2 \end{bmatrix}$$

$$B_m = \begin{bmatrix} 2 & -1 & & & & & & \\ -1 & 2 & -1 & & & & 0 & \\ & -1 & 2 & -1 & & & & \\ & & -1 & & & & & \\ & & & & & -1 & & \\ & & 0 & & -1 & 2 & -1 & \\ & & & & & -1 & 2 & -1 \\ & & & & & & -2 & 2 \end{bmatrix}$$

$$C_m = \begin{bmatrix} 2 & -1 & & & & & \\ -1 & 2 & -1 & & & 0 & \\ & -1 & 2 & -1 & & & \\ & & -1 & & & & \\ & & & & -1 & & \\ & 0 & & & -1 & 2 & -1 \\ & & & & & -1 & 2 \end{bmatrix}$$

$$D_m = \begin{bmatrix} 2 & -1 & & & & & \\ -1 & 2 & -1 & & & 0 & \\ & -1 & 2 & -1 & & & \\ & & -1 & & & & \\ & & & & -1 & & \\ & 0 & & & -1 & 2 & -1 \\ & & & & & -1 & 2 \end{bmatrix}$$

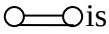
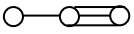
$$G_2 = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$$

$$F_4 = \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -2 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix}$$

$$E_6 = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{bmatrix}$$

$$E_7 = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{bmatrix}$$

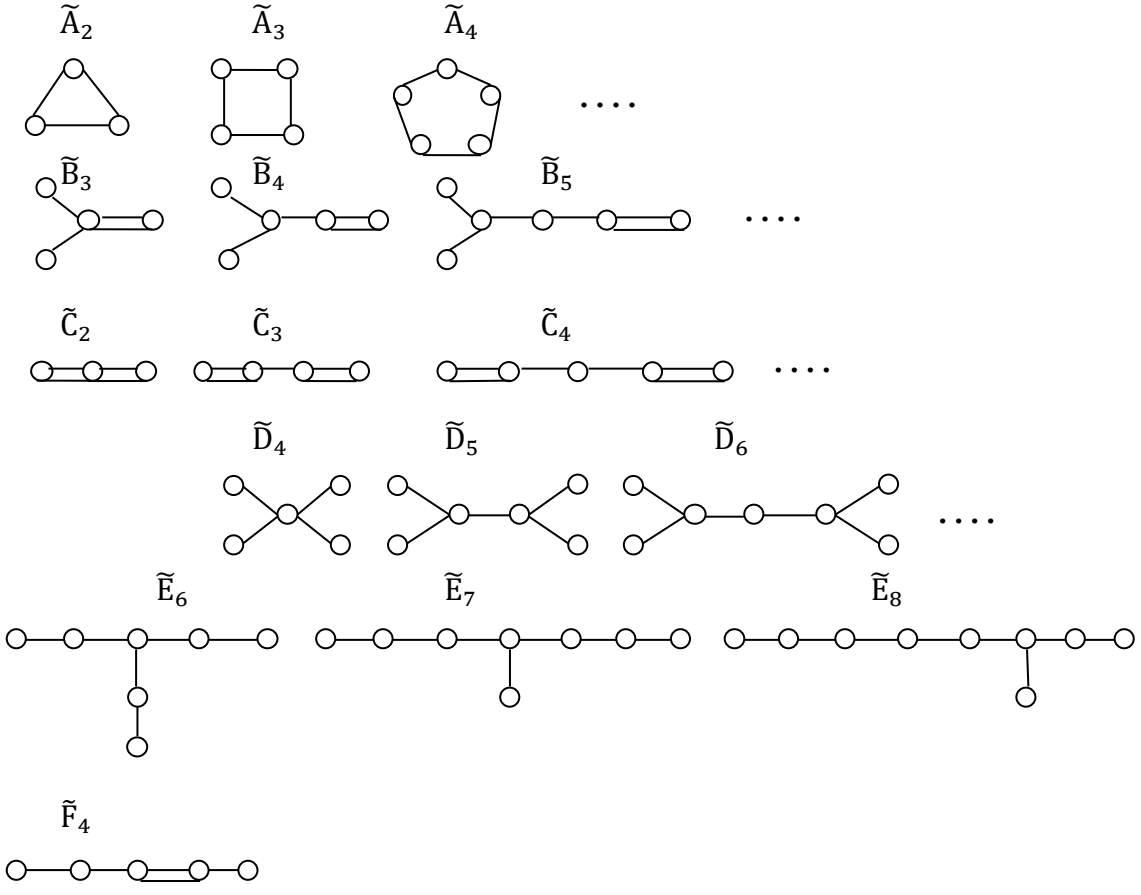
$$E_8 = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{bmatrix}$$

Proof of theorem 5.12.4. A *subgraph* of a graph Δ is obtained from Δ by removing certain nodes or decreasing certain bond lengths or both (so  is a subgraph of ). The list of graphs given in the theorem will be called the standard list. We note that each subgraph of a graph on the standard list is also on the standard list. It is not difficult to show that if the quadratic form of a graph Δ is positive definite, then the quadratic form of any subgraph of Δ is positive definite also.

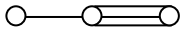
Now the quadratic form of a graph Δ is represented by a symmetric matrix M.

We recall from linear algebra that $Q(x_1, ..., x_m)$ is positive definite if and only if all the leading minors of M have positive determinant. However the leading minors of M are simply matrices M corresponding to certain subgraphs of Δ. In order to show that $Q(x_1, ..., x_m)$ is positive definite it is therefore sufficient to check that det M > 0 for each graph Δ on the standard list. This is readily verified.

We now wish to prove conversely that the graphs on the standard list are the only ones satisfying the given conditions. In order to do this we introduce a second list.



$\widetilde{G}_2$ list 2



It may be readily checked that each graph Δ on list 2 has a quadratic form $Q(x_1, ..., x_m)$ with symmetric matrix M satisfying det M = 0. Thus $Q(x_1, ..., x_m)$ is not positive definite. Hence any graph Δ satisfying our given conditions can contain no subgraph on list 2.

Let Δ be a graph satisfying our conditions (i) (ii) and (iii). Then Δ has no cycles, otherwise Δ would contain a subgraph of type $\widetilde{A}_m$ Δ has at most one multiple bond, otherwise Δ would contain a subgraph of type $\widetilde{C}_m$. Δ cannot have both a multiple bond and a branch point, otherwise it would contain a subgraph $\widetilde{B}_m$. Also Δ cannot have more than one branch point, otherwise Δ would contain a subgraph $\widetilde{D}_m$.

Suppose Δ has a triple bond. Then Δ must be G_2, as otherwise Δ would contain a subgraph $\widetilde{G}_2$. We may therefore assume that Δ contains no other triple bond than for G_2.

Suppose Δ has a double bond. Then Δ contains no branch point, so is a chain. If the double bond is at one end of the chain then $\Delta = B_m$, if not then Δ must be F_4, otherwise Δ would contain a subgraph $\widetilde{F}_4$.

So we may assume that Δ contains only single bonds. If Δ has no branch points then $\Delta = A_m$. So posit Δ contains a branch point, which must have only three branches because it cannot contain a subgraph $\widetilde{D}_4$. Let the length of the branches be m_1, m_2 and m_3, with $m = m_1 + m_2 + m_3 + 1$ and $m_1 \geq m_2 \geq m_3$. Then $m_3 = 1$, otherwise Δ would contain a subgraph $\widetilde{E}_6$. Also $m_2 \leq 2$ otherwise Δ would contain a subgraph $\widetilde{E}_7$. If $m_2 = 1$ then $\Delta = D_m$. So suppose $m_2 = 2$. Then $m_1 \leq 4$, otherwise Δ would contain a subgraph $\widetilde{E}_8$. If $m_1 = 2$ then $\Delta = E_6$. If $m_1 = 3$ then $\Delta = E_7$. Lastly if $m_1 = 4$ then $\Delta = E_8$.

Therefore Δ must be one of the graphs on list 1, the standard list. □

The classification of the simple Lie algebras was achieved by W. Killing in a series of papers in Mathematische Annalen between 1888 and 1890, and independently by Eli Cartan in his Paris thesis of 1894.

5.13 Vertex operator algebras.

The classification for positive definite quadratic forms given by the Dynkin diagram list 1 is complete. We know there exist sporadic simple groups going beyond this classification. Thus groups given by zargon brackets of chapter 4, section 16, exist outside this classification. We show that vertex operator algebras have infinite quadratic forms outside the classification. List 2, used to exclude Dynkin diagrams not in list 1, is not itself a complete classification of zero quadratic forms.