Fundamental concepts

1 Homomorphims

If G and H are groups, then a homomorphism from G to H is a map $\phi : G \to H$ that satisfies

$$\phi(xy) = \phi(x)\,\phi(y)$$

for all $x, y \in G$, i.e. the image of a product is the product of the images. Isomorphisms are nothing but bijective homomorphisms.

Homomorphisms preserve identity elements, i.e. $\phi(\mathbf{1}_G) = \mathbf{1}_H$, and commute with taking inverses, i.e. $\phi\left(x^{-1}\right) = \phi(x)^{-1}$ for $x \in G$.

Homomorphisms can be composed: if $\phi: G \to H$ and $\psi: H \to K$ are homomorphisms, then their composition

$$\begin{aligned} \psi \circ \phi : G &\to K \\ g &\mapsto \psi(\phi(g)) \end{aligned}$$

is a homomorphism from G to K.

The image of a homomorphism $\phi: G \to H$ is the subset $\phi(G) = \{\phi(x) | x \in G\}$ of H that consists of the images of the elements of G, while its kernel is the collection of elements mapped onto the identity element of H, i.e. the subset $\ker\phi = \{x \in G \mid \phi(x) = \mathbf{1}_H\}$ of G.

A homomorphism $\phi: G \to H$ is surjective precisely when $\phi(G) = H$, and it is injective when $\ker\phi = \mathbf{1}_G$.

2 Subgroups

A subset H of elements of a group G is a subgroup, denoted $H < G$, if the inverse and the product of any of its elements also belongs to H.

Remark. The above conditions insure that the identity element of G is contained in each of its subgroups.

The restriction of the group operation of G to the subgroup $H < G$ is a binary operation that satisfies the group axioms (associativity, existence of an identity element and of inverse elements), hence a subgroup is a group on its own.

Examples:

1. the set $\{\mathbf{1}_G\}$ consisting of the identity element alone is a subgroup, the trivial subgroup of G;

2. the additive group $(2\mathbb{Z},+)$ of even integers is a subgroup of the additive group $(\mathbb{Z},+)$ of all integers;

3. the group $\mathsf{U}(1)=\{z\in\mathbb{C}\mid|z|=1\}$ of complex phases (numbers of unit modulus) is a subgroup of the multiplicative group $\mathbb{C}^\times=\mathbb{C}\setminus\{0\}$ of non-zero complex numbers;

4. the group of orientation preserving symmetries (i.e. rotations) of a regular n-gon form a subgroup $\mathbf{C}_n$ of the dihedral group $\mathbb{D}_n$;

5. the centralizer $\mathtt{C}_G(X) = \{y \in G \mid xy = yx \text{ for all } x \in X\}$ of a subset $X \subseteq G$, consisting of those group elements that commute with all elements $x \in X$, is a subgroup of G, and in particular, the center $Z(G) = \mathtt{C}_G(G)$, consisting of those elements that commute with every other element, is an Abelian subgroup (elements and subgroups of the center are termed central);

6. the image $\phi(G)$ of a homomorphism $\phi : G \to H$ is a subgroup of its range, i.e. $\phi(G) < H$;

7. the kernel $\ker \phi = \{x \in G \mid \phi(x) = \mathbf{1}_H\}$ of a homomorphism $\phi : G \to H$ is a subgroup of its domain, i.e. $\ker \phi < G$.

Subgroups of the dihedral group $\mathbb{D}_3$:

- trivial subgroup $\{\mathbf{1}\}$ (order 1)
- subgroups $\mathbf{S}_i = \{\mathbf{1}, \sigma_i\} \cong \mathbb{Z}_2$ for $i = 1, 2, 3$ (order 2)
- rotation subgroup $\mathbf{C}_3 = \{\mathbf{1}, C, C^{-1}\} \cong \mathbb{Z}_3$ (order 3)
- whole group $\mathbb{D}_3 = \{\mathbf{1}, C, C^{-1}, \sigma_1, \sigma_2, \sigma_3\}$ (order 6)

Remark. The order of every subgroup divides 6.

The subgroups of a given group form a partially ordered set because

$$K < H \quad \text{and} \quad H < G \quad \text{implies} \quad K < G$$

i.e a subgroup of a subgroup is itself a subgroup.

The intersection of subgroups is again a subgroup, hence the subgroups of G form a lattice (the subgroup lattice $\mathcal{L}_G$): any collection S of subgroups has both a greatest lower bound (their intersection) and a lowest upper bound (the intersection of all subgroups containing the elements of S).

The subgroup lattice can be visualized by its Hasse-diagram, a graph with vertices corresponding to the different subgroups $H < G$, with vertices H and K connected by an edge if $H < K$ and if $H < L < K$ implies that either $L = H$ or $L = K$ (in other words, if K covers H), with the convention that K lies above H in the diagram.

Remark. The bottom vertex of the Hasse-diagram is the trivial subgroup, while the top vertex is the whole group.

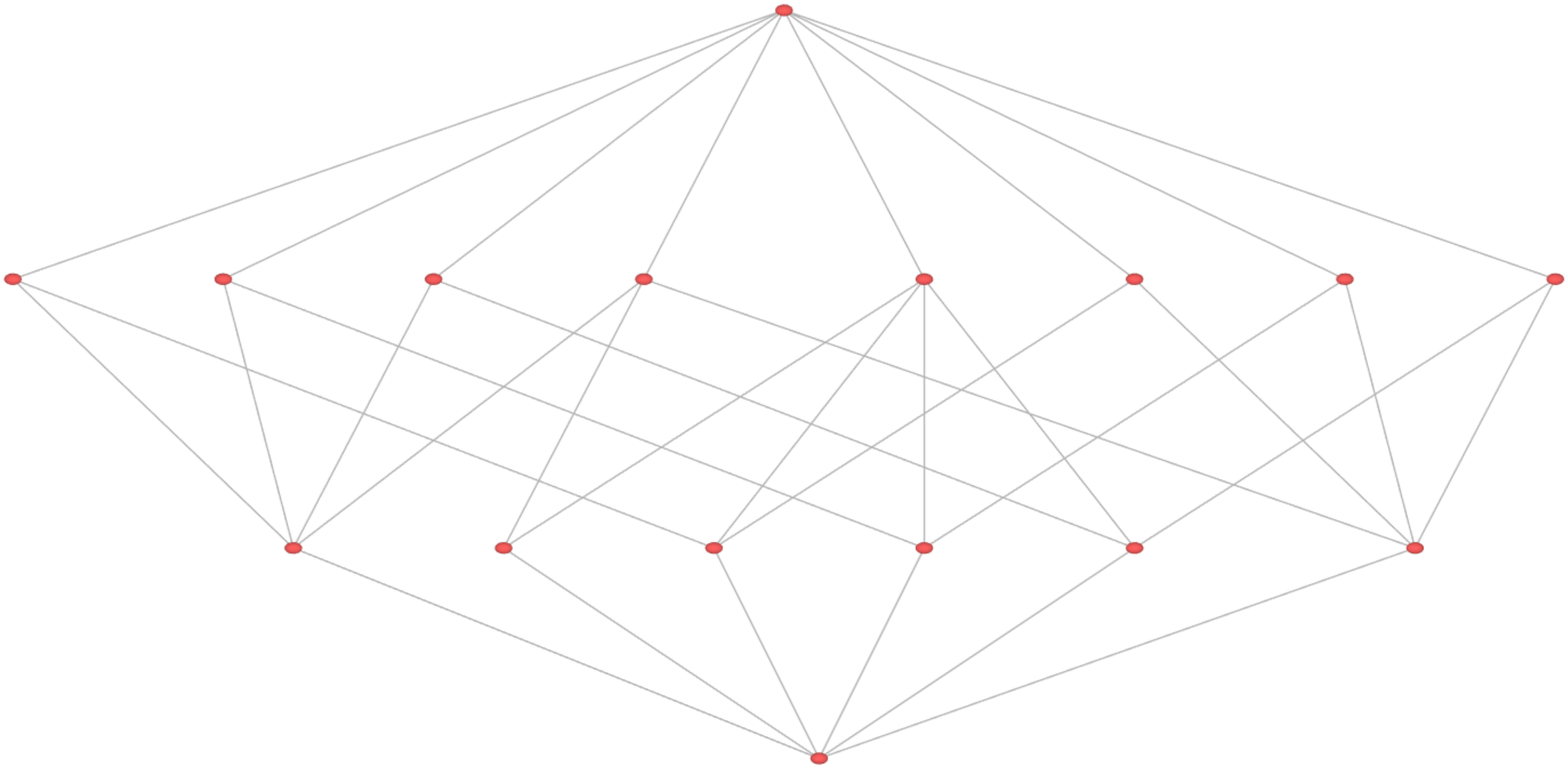


Figure 1. Subgroup lattice of the dihedral group $\mathbb{D}_6$

Note that every subgroup of a symmetric group of finite degree is finite; conversely, one has

> Cayley's theorem: every finite group is isomorphic to a subgroup of some symmetric group of finite degree.

This result implies that the study of finite groups could be reduced to that of groups of permutations , but this is not always convenient, for the degree of the corresponding symmetric group might be too big: for example, Cayley's theorem allows to view a group of prime order p as a subgroup of the symmetric group $\mathbb{S}_p$ of degree p, but it is much more convenient to represent it as the additive group of integers modulo p.

3 Generating sets

A subgroup $H < G$ is generated by a set $\mathscr{G} \subseteq G$ of group elements – equivalently, $\mathscr{G}$ is a generating set (aka. system of generators) for H – if H is the smallest subgroup of G containing $\mathscr{G}$ (i.e. H is the intersection of all subgroups of G containing $\mathscr{G}$).

The subgroup generated by $\mathscr{G} \subseteq G$, denoted $\langle \mathscr{G} \rangle$, contains all possible products of elements of $\mathscr{G}$, together with their inverses.

A group (subgroup) is finitely generated if it has a finite generating set, and cyclic if it can be generated by a single element.

Remark. A group (subgroup) may have many different generating sets, since any set of group elements that contain a generating set is itself a generating set; in particular, the system of all group elements is a generating set for the whole group.

The major use of generating sets is effective group description, i.e. the specification of a particular group as a subgroup of some bigger, well understood group via a generating set.

For example, a group G that consists of permutations of a set X is a subgroup of the symmetric group $\mathsf{Sym}(X)$ over X, hence it can be fully specified by giving a generating set $\mathscr{G} \subseteq \mathsf{Sym}(X)$ for which $G = \langle \mathscr{G} \rangle$, e.g. $\mathbb{S}_3 = \langle (1,2), (1,2,3) \rangle$ and $\mathbb{A}_4 = \langle (1,2,3), (2,3,4) \rangle$.

4 Cosets

A coset of a subgroup $H < G$ is a set of group elements of the form

$$\begin{aligned} xH &= \{xh \,|\, h \in H\} && \text{left} \\ Hx &= \{hx \,|\, h \in H\} && \text{right} \end{aligned}$$

for some $x \in G$ (with $1H = H1 = H$ the trivial coset).

Unless G is Abelian, left and right cosets usually differ, i.e. $xH \neq Hx$.

The subgroup $H < G$ is normal, denoted $H \triangleleft G$, if all left and right cosets coincide, i.e. $xH = Hx$ for all $x \in G$.

The coset spaces $G/H = \{xH \,|\, x \in G\}$ and $H \backslash G = \{Hx \,|\, x \in G\}$ are the collections of left and right cosets of H.

Examples:

1. the cosets (left or right) of the trivial subgroup $\{\mathbf{1}_G\} < G$ are the one element sets $\{x\}$ for $x \in G$;

2. $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$ has two cosets (even vs odd numbers);

3. the coset space of $\mathbb{C}^\times/\mathsf{U}(1)$ is in one-to-one correspondence with the positive real numbers;

4. the rotation subgroup $\mathbf{C}_n \lhd \mathbb{D}_n$ has two cosets, the trivial coset consisting of orientation preserving symmetries (rotations), and the coset $\sigma_1 \mathbf{C}_n = \{\sigma_1, \ldots, \sigma_n\}$ consisting of orientation reversing symmetries (reflections).

Remark. There is a bijective correspondence between G/H and $H\backslash G$, hence it is enough to study left cosets.

The index $[G\!:\!H]$ of a subgroup $H\!<\!G$ is the cardinality of its coset space

$$[G:H]=|G/H|=|H\backslash G|$$

Poincaré's theorem: the intersection of two finite index subgroups is again of finite index.

The cosets of a subgroup equipartition the set of group elements: each group element belongs to exactly one coset, and each coset has the same cardinality (equal to that of the trivial coset, i.e. the order of H).

Lagrange's theorem: if G is finite and $H < G$, then $|G| = [G:H]|H|$.

In particular, the order of any subgroup divides the order of the group.

Corollary. *Groups of prime order are cyclic.*

Proof. If G has prime order $|G| = p$, and $x \in G$ is a non-trivial element (i.e. $x \neq \mathbf{1}_G$), then the subgroup $\langle x \rangle$ generated by x has at least two different elements, hence its order is – by Lagrange's theorem – a divisor of p greater than 1, consequently it equals p, and $\langle x \rangle$ contains all of the group elements, hence $G = \langle x \rangle$. □

Remark. Not only the order, but the index of a subgroup is also a divisor of the order of the whole group.

5 Normal subgroups

A subgroup $N < G$ is a normal subgroup, denoted $N \triangleleft G$, if its right cosets coincide with its left cosets, i.e. $xN = Nx$ for all $x \in G$.

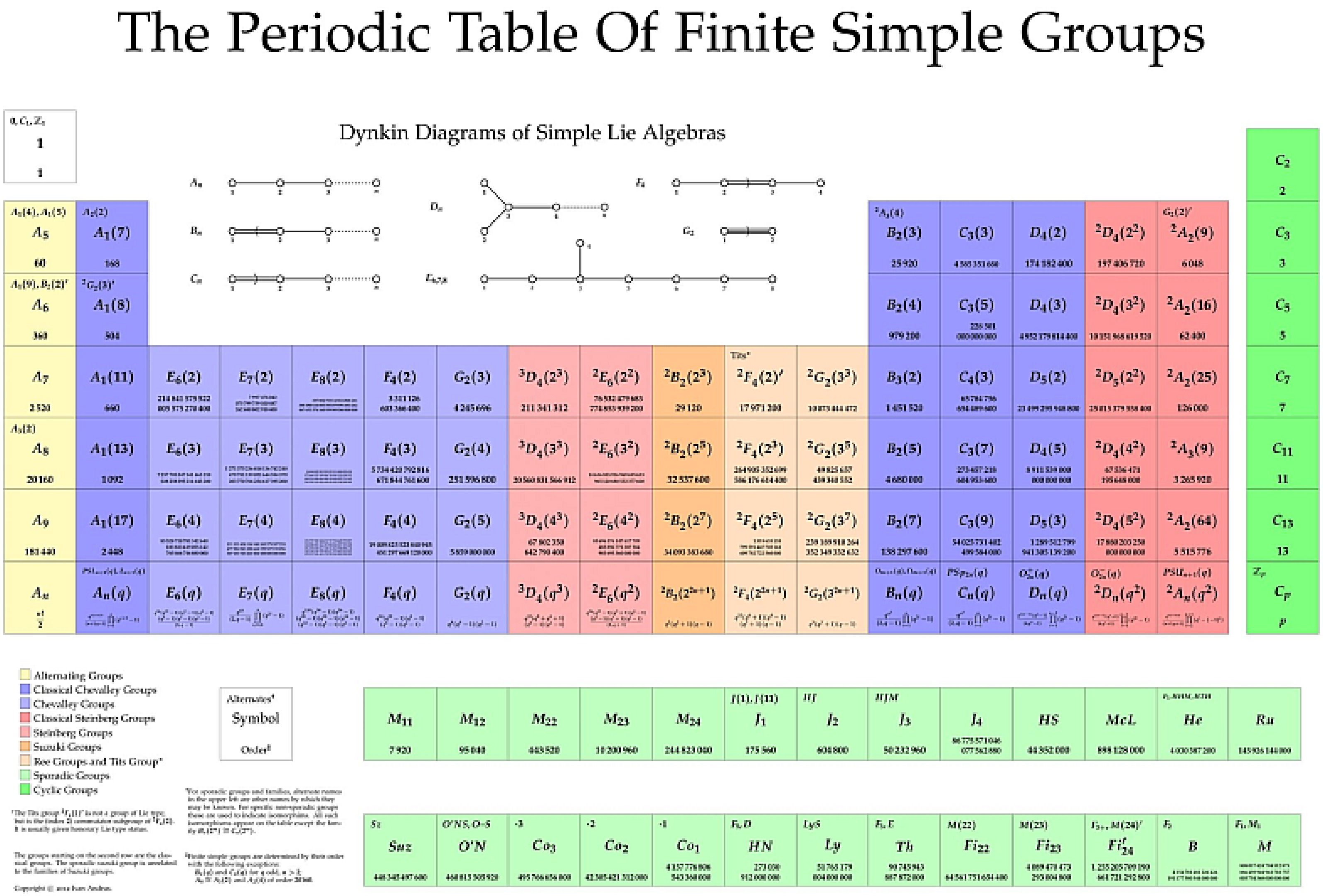
The trivial subgroup and the whole group are always normal: a group which has no other normal subgroup is called simple.

Simple groups may be considered as the elementary ('atomic') constituents of which more general groups may be built up, and many questions may be reduced to the case of simple groups.

All subgroups of an Abelian group are normal, hence a finite Abelian group is simple if and only if it is cyclic of prime order.

Classification of finite simple groups:

1. the cyclic groups $\mathbb{Z}_p$ of prime order;
2. the alternating groups $\mathbb{A}_n$ for $n > 4$;
3. the finite Lie groups (finite analogs of Lie groups that form – apart from some exceptional cases – several infinite families, together with suitable twisted versions);
4. 26 sporadic groups, including the famous **Mathieu groups** and the **Monster** $\mathbb{M}$ (with more than 10^{58} group elements).



The Periodic Table Of Finite Simple Groups

Dynkin Diagrams of Simple Lie Algebras

A_n
B_n
C_n
D_n
$E_{6,7,8}$
F_4
G_2

$0, C_1, Z_1$ 1 1																	C_2 2
$A_1(4), A_1(5)$ A_5 60	$A_2(2)$ $A_1(7)$ 168											${}^2A_3(4)$ $B_2(3)$ 25 920	$C_3(3)$ 4 585 351 680	$D_4(2)$ 174 182 400	${}^2D_4(2^2)$ 197 406 720	$G_2(2)'$ ${}^2A_2(9)$ 6 048	C_3 3
$A_1(9), B_2(2)'$ A_6 360	${}^2G_2(3)'$ $A_1(8)$ 504											$B_2(4)$ 979 200	$C_3(5)$ 228 501 000 000 000	$D_4(3)$ 4 952 179 814 400	${}^2D_4(3^2)$ 10 151 968 619 520	${}^2A_2(16)$ 62 400	C_5 5
A_7 2 520	$A_1(11)$ 660	$E_6(2)$ 214 841 575 522 005 575 270 400	$E_7(2)$ [illegible]	$E_8(2)$ [illegible]	$F_4(2)$ 3 311 126 603 366 400	$G_2(3)$ 4 245 696	${}^3D_4(2^3)$ 211 341 312	${}^2E_6(2^2)$ 76 532 479 683 774 853 939 200	${}^2B_2(2^3)$ 29 120	Tits* ${}^2F_4(2)'$ 17 971 200	${}^2G_2(3^3)$ 10 073 444 472	$B_3(2)$ 1 451 520	$C_4(3)$ 65 784 756 654 489 600	$D_5(2)$ 23 499 295 948 800	${}^2D_5(2^2)$ 25 015 379 558 400	${}^2A_2(25)$ 126 000	C_7 7
$A_3(2)$ A_8 20 160	$A_1(13)$ 1 092	$E_6(3)$ [illegible]	$E_7(3)$ [illegible]	$E_8(3)$ [illegible]	$F_4(3)$ 5 734 420 792 816 671 844 761 600	$G_2(4)$ 251 596 800	${}^3D_4(3^3)$ 20 560 831 566 912	${}^2E_6(3^2)$ [illegible]	${}^2B_2(2^5)$ 32 537 600	${}^2F_4(2^3)$ 264 905 352 699 586 176 614 400	${}^2G_2(3^5)$ 49 825 657 439 340 552	$B_2(5)$ 4 680 000	$C_3(7)$ 273 457 218 604 953 600	$D_4(5)$ 8 911 539 000 000 000 000	${}^2D_4(4^2)$ 67 536 471 195 648 000	${}^2A_3(9)$ 3 265 920	C_{11} 11
A_9 181 440	$A_1(17)$ 2 448	$E_6(4)$ [illegible]	$E_7(4)$ [illegible]	$E_8(4)$ [illegible]	$F_4(4)$ 19 009 825 523 840 945 451 297 669 120 000	$G_2(5)$ 5 859 000 000	${}^3D_4(4^3)$ 67 802 350 642 790 400	${}^2E_6(4^2)$ [illegible]	${}^2B_2(2^7)$ 34 093 383 680	${}^2F_4(2^5)$ [illegible]	${}^2G_2(3^7)$ 239 189 910 264 352 349 332 632	$B_2(7)$ 138 297 600	$C_3(9)$ 54 025 731 402 499 584 000	$D_5(3)$ 1 289 512 799 941 305 139 200	${}^2D_4(5^2)$ 17 880 203 250 000 000 000	${}^2A_2(64)$ 5 515 776	C_{13} 13
A_n $\frac{n!}{2}$	$PSL_{n+1}(q), L_{n+1}(q)$ $A_n(q)$ [illegible]	$E_6(q)$ [illegible]	$E_7(q)$ [illegible]	$E_8(q)$ [illegible]	$F_4(q)$ [illegible]	$G_2(q)$ $q^6(q^6-1)(q^2-1)$	${}^3D_4(q^3)$ [illegible]	${}^2E_6(q^2)$ [illegible]	${}^2B_2(2^{2n+1})$ $q^2(q^2+1)(q-1)$	${}^2F_4(2^{2n+1})$ [illegible]	${}^2G_2(3^{2n+1})$ $q^3(q^3+1)(q-1)$	$O_{2n+1}(q), \Omega_{2n+1}(q)$ $B_n(q)$ [illegible]	$PSp_{2n}(q)$ $C_n(q)$ [illegible]	$O^+_{2n}(q)$ $D_n(q)$ [illegible]	$O^-_{2n}(q)$ ${}^2D_n(q^2)$ [illegible]	$PSU_{n+1}(q)$ ${}^2A_n(q^2)$ [illegible]	Z_p C_p p

🟨	Alternating Groups
🟦	Classical Chevalley Groups
🟦	Chevalley Groups
🟥	Classical Steinberg Groups
🟥	Steinberg Groups
🟧	Suzuki Groups
🟧	Ree Groups and Tits Group*
🟩	Sporadic Groups
🟩	Cyclic Groups

Alternates[1]
Symbol
Order[2]

M_{11} 7 920	M_{12} 95 040	M_{22} 443 520	M_{23} 10 200 960	M_{24} 244 823 040	$J(1), J(11)$ J_1 175 560	HJ J_2 604 800	HJM J_3 50 232 960	J_4 86 775 571 046 077 562 880	HS 44 352 000	McL 898 128 000	F_7, HHM, HTH He 4 030 387 200	Ru 145 926 144 000
Sz Suz 448 345 497 600	$O'NS, O\text{-}S$ $O'N$ 460 815 505 920	$\cdot 3$ Co_3 495 766 656 000	$\cdot 2$ Co_2 42 305 421 312 000	$\cdot 1$ Co_1 4 157 776 806 543 360 000	F_5, D HN 273 030 912 000 000	LyS Ly 51 765 179 004 000 000	F_3, E Th 90 745 943 887 872 000	$M(22)$ Fi_{22} 64 561 751 654 400	$M(23)$ Fi_{23} 4 089 470 473 293 004 800	$F_{3+}, M(24)'$ Fi'_{24} 1 255 205 709 190 661 721 292 800	F_2 B [illegible]	F_1, M_1 M [illegible]

*The Tits group ${}^2F_4(2)'$ is not a group of Lie type, but is the (index 2) commutator subgroup of ${}^2F_4(2)$. It is usually given honorary Lie type status.

The groups starting on the second row are the classical groups. The sporadic suzuki group is unrelated to the families of Suzuki groups.

Copyright © 2012 Ivan Andrus.

[1] For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups these are used to indicate isomorphisms. All such isomorphisms appear on the table except the family $B_n(2^m) \cong C_n(2^m)$.

[2] Finite simple groups are determined by their order with the following exceptions: $B_n(q)$ and $C_n(q)$ for q odd, $n > 2$; $A_8 \cong A_3(2)$ and $A_2(4)$ of order 20160.

The intersection of normal subgroups is normal again, hence the normal subgroups form a (modular) sublattice of the subgroup lattice.

Congruence relation: equivalence relation compatible with product

$$\boxed{\left.\begin{array}{l} x_1 \equiv y_1 \\ x_2 \equiv y_2 \end{array}\right\} \Rightarrow \; x_1 x_2 \equiv y_1 y_2}$$

One-to-one correspondence between normal subgroups and congruence relations: the cosets of a normal subgroup are the equivalence classes of a congruence relation, while the congruence class $\{x \in G \,|\, x \equiv \mathbf{1}_G\}$ of the identity element is a normal subgroup.

6 Factor groups

For two subsets $X, Y \subseteq G$ of group elements let

$$XY = \{xy \,|\, x \in X,\ y \in Y\} \subseteq G$$

Associative operation on subsets, but inverses exist only for singletons.

The product of cosets of a subgroup is usually the union of several cosets, but for a normal subgroup, the product of cosets is a single coset!

For a normal subgroup $N \lhd G$ and group elements $x, y \in G$

$$(xN)(yN) = (xy)N$$

Factor group G/N: collection of cosets of the normal subgroup $N \lhd G$ with the above product (with the trivial coset as identity element).

Examples:

1. the factor group $G/\left\{\mathbf{1}_G\right\}$ is isomorphic to G;

2. $\mathbb{C}^{\times}/\mathsf{U}(1)$ is isomorphic to the multiplicative group of positive real numbers, since any $z\in\mathbb{C}^{\times}$ has a polar decomposition $z=ru$ with $r>0$ and $u\in\mathsf{U}(1)$;

3. the factor group $\mathbb{D}_n/\mathbf{C}_n$ is isomorphic to $\mathbb{Z}_2$;

4. $\mathbb{A}_n$ is a normal subgroup of index 2 in $\mathbb{S}_n$, and $\mathbb{S}_n/\mathbb{A}_n \cong \mathbb{Z}_2$.

Remark. In general, if p denotes the smallest prime divisor of the order, than any subgroup of index p is normal, and the corresponding factor group is isomorphic with $\mathbb{Z}_p$.

Correspondence theorem: subgroups of the factor group G/N are of the form H/N, where $H < G$ is a subgroup of G containing the normal subgroup N (with normal subgroups corresponding to normal ones).

In other words, the (normal) subgroup lattice of the factor group G/N is completely determined by the (normal) subgroup lattice of G.

Isomorphism theorems:

1. if $N \triangleleft G$ and $H < G$ then $N \triangleleft NH < G$, $N \cap H \triangleleft H$ and

$$H/(N \cap H) \cong NH/N$$

2. if $K \triangleleft N \triangleleft G$ and $K \triangleleft G$, then $N/K \triangleleft G/K$ and

$$(G/K)/(N/K) \cong G/N$$

7 Subnormal series and soluble groups

A subnormal series is a finite sequence of subgroups

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$

where each term is a normal subgroup of the preceding one.

A composition series is a subnormal series where all factor groups G_{i-1}/G_i (the composition factors) are simple groups.

Example: $\mathbb{S}_4 \triangleright \mathbb{A}_4 \triangleright \mathtt{V} \triangleright \mathbb{Z}_2 \triangleright \{1\}$, with respective factor groups (isomorphic to) $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$ and $\mathbb{Z}_2$.

Composition series provide (in some sense) the dissection of group ’molecules’ into their ’atomic constituents’ (simple groups).

Jordan-Hölder theorem: if a group has several composition series, then all have the same length, and their composition factors coincide.

All finite groups have a composition series (possibly several), but infinite ones (e.g. the additive group of integers) not necessarily.

A group is soluble if it has a subnormal series where all factor groups G_{i-1}/G_i are Abelian (commutative).

Remark: by the above example, the group $\mathbb{S}_4$ is soluble.

Soluble groups play a prominent role in Galois theory (solving polynomial equations by radicals), differential equations (solubility by quadratures), algorithmic methods, etc.

Solubility is a kind of relaxed commutativity, in particular all subgroups and factor groups of a soluble group are themselves soluble.

Feit-Thompson theorem: finite groups of odd order are soluble.

Remark: $\mathbb{S}_n$ is soluble only for $n \leq 4$, explaining the Abel-Ruffini theorem (only equations of degree less than 5 can be solved by radicals).

The commutator of the group elements $x, y \in G$ is the group element

$$[x, y] = x^{-1} y^{-1} x y$$

The subgroup $G' = \langle \{[x, y] \mid x, y \in G\} \rangle$ generated by all commutators is the commutator subgroup (aka. derived subgroup) of G.

Two group elements commute iff their commutator equals the identity, hence G' is trivial precisely when G is Abelian.

The commutator subgroup G' is always a normal subgroup of G, and the factor group G/G' is always Abelian (what is more, it is the smallest normal subgroup $N \lhd G$ such that G/N is commutative).

Derived series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_i$$

with $G_{i+1} = G_i'$ (need not terminate in the trivial subgroup).

A group G is soluble iff its derived series is subnormal, i.e. reaches the trivial subgroup in a finite number of steps.

8 The homomorphism theorem

For a normal subgroup $N \lhd G$, the natural projection

$$\begin{aligned} \pi_N : G &\to G/N \\ x &\mapsto xN \end{aligned}$$

is a homomorphism with kernel equal to N.

Homomorphism theorem: the kernel of a homomorphism $\phi : G \to H$ is a normal subgroup, $\ker\phi \lhd G$, and its image is isomorphic with the corresponding factor group, $\phi(G) \cong G/\ker\phi$.

Up to isomorphism, the homomorphic images (an external attribute) of a given group coincide with its factor groups (an internal attribute).

9 Cyclic (sub)groups

The powers of the group element $x \in G$ are defined recursively as $x^1 = x$ and $x^{n+1} = xx^n$ for an integer n; in particular, $x^0 = xx^{-1} = \mathbf{1}_G$ and $x^{-n} = \left(x^{-1}\right)^n = (x^n)^{-1}$ for all $n \in \mathbb{Z}$.

Since the multiplication of powers corresponds to the addition of their exponents, the smallest subgroup containing $x \in G$ (the cyclic subgroup $\langle x \rangle$ generated by it) has as elements its different powers: $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Remark: any cyclic group is Abelian because the addition of integers is commutative.

The map $\phi_x : \mathbb{Z} \to G$ that assigns to each integer n the $n^{\mathtt{th}}$ power of $x \in G$, i.e. $\phi_x(n) = x^n$, is actually a homomorphism

$$\phi_x(n+m) = x^{n+m} = x^n x^m = \phi_x(n)\phi_x(m)$$

The image of ϕ_x consists of all powers of x, hence

$$\langle x \rangle = \phi_x(\mathbb{Z}) \cong \mathbb{Z}/\ker\phi_x$$

according to the homomorphism theorem; in particular, the index $[\mathbb{Z} : \ker\phi_x]$ equals the order of $x \in G$, i.e. the order of the cyclic subgroup $\langle x \rangle < G$.

A subgroup H of the additive group $(\mathbb{Z}, +)$ of integers is either trivial or consists of the different multiples of some positive integer n (equal to its index): $H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

Since $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ (the additive group of residue classes modulo n)

- if the order of $x \in G$ is infinite, then $\ker \phi_x = \{0\}$, and $\langle x \rangle$ is isomorphic to $\mathbb{Z}$, the additive group of integers (infinite cyclic case);
- if the order of $x \in G$ is a finite number n, then $\ker \phi_x$ is a subgroup of $\mathbb{Z}$ of index n, hence $\ker \phi_x = n\mathbb{Z}$ and $\langle x \rangle$ is isomorphic to $\mathbb{Z}_n$.

Structure theorem of cyclic groups: the order of a cyclic group is either finite or countably infinite, and two cyclic groups are isomorphic precisely when they have the same order.

10 Direct product of groups

The direct product $G \times H$ of the groups G and H is a new group, whose elements are ordered pairs (x, y) with $x \in G$ and $y \in H$, endowed with component-wise multiplication

$$\boxed{(x_1, y_1)\,(x_2, y_2) = (x_1 x_2, y_1 y_2)}$$

$G \times H$ has order $|G \times H| = |G||H|$, its identity element is $(\mathbf{1}_G, \mathbf{1}_H)$, and inverses are given by $(x, y)^{-1} = \left(x^{-1}, y^{-1}\right)$.

Considered as a binary operation between isomorphism classes of groups, the direct product is commutative and associative

$$G_1 \times G_2 \cong G_2 \times G_1 \qquad \text{and} \qquad G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$$

Examples:

1) for coprime integers n and m

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

and in general $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{\mathrm{lcm}(n,m)} \times \mathbb{Z}_{\mathrm{gcd}(n,m)}$;

2) $\mathsf{GL}_\mathsf{n}(\mathbb{C}) \cong \mathsf{SL}_n(\mathbb{C}) \times \mathbb{C}^\times$;

3) $\mathsf{U}(n) \cong \mathsf{SU}(n) \times \mathsf{U}(1)$;

4) $\mathbb{D}_{4n+2} \cong \mathbb{D}_{2n+1} \times \mathbb{Z}_2$;

5) the additive group $(V, +)$ of a linear space of dimension n over a field $\mathbb{F}$ is isomorphic with the n-fold direct product of the additive group of $\mathbb{F}$

$$(V, +) \cong \underbrace{(\mathbb{F}, +) \times \cdots \times (\mathbb{F}, +)}_{n}$$

$$\hat{G}=\{(x,\mathbf{1}_H)\mid x\in G\}\quad\text{and}\quad\hat{H}=\{(\mathbf{1}_G,y)\mid y\in H\}$$

are normal subgroups of the direct product that

1) generate the whole product, $\left\langle \hat{G},\hat{H}\right\rangle = G\times H$;

2) have trivial intersection, $\hat{G}\cap\hat{H}=\{(\mathbf{1}_G,\mathbf{1}_H)\}$;

3) have pairwise commuting elements: $(x,\mathbf{1}_H)(\mathbf{1}_G,y)=(x,y)=(\mathbf{1}_G,y)(x,\mathbf{1}_H)$;

4) are isomorphic with the direct factors: $\hat{G}\cong G$ and $\hat{H}\cong H$;

5) $(G\times H)/\hat{G}\cong H$ and $(G\times H)/\hat{H}\cong G$.

Conversely, any group having normal subgroups $\hat{G}$ and $\hat{H}$ satisfying 1)-3) is isomorphic to their direct product $\hat{G}\times\hat{H}$.

The direct product of Abelian (in particular cyclic) groups is Abelian.

Conversely, one has the following structure theorem.

Frobenius-Stickelberger theorem: any finite Abelian group can be decomposed into a direct product of cyclic groups of prime power order.

The above decomposition is unique up to the ordering of the factors (the elementary divisors).

In case of finitely generated Abelian groups, a finite number of infinite cyclic factors (each isomorphic to the additive group of integers) may also appear in the decomposition.

11 Group presentations

A subset $X \subseteq F$ is a free generating system of the group F if every map $\phi : X \to G$ into an arbitrary group G is the restriction of a unique homomorphism $\phi^\flat : F \to G$.

A group is free if it has a free generating system.

For any set X there exists a group F_X (the free group over X) with free generating set X.

$F_X \cong F_Y$ precisely when $|X| = |Y|$, hence any two free generating systems of a free group have the same cardinality (the rank of the group, which determines it up to isomorphism).

Remark. Free generating systems are the analogues for free groups of the different bases of a linear space (with rank corresponding to dimension).

Nielsen-Schreier theorem: every subgroup of a free group is free.

If F is free of rank n and $H < F$, then H is free of rank $1 + [F:H]\,(n-1)$.

von Dyck's theorem: every group is a homomorphic image of a free group!

If G is generated by $X \subseteq G$, then the inclusion map $\mathrm{i}_X : X \to G$ that sends each $x \in X$ to itself extends to a unique homomorphism $\mathrm{i}_X^\flat : F_X \to G$, and because X is a generating set, the image of $\mathrm{i}_X^\flat$ is the whole of G, and

$$G = \mathrm{i}_X^\flat(F_X) \cong F_X / \ker \mathrm{i}_X^\flat$$

by the homomorphism theorem.

Because the kernel of $\mathfrak{i}^\flat_X$ is itself free (by the Nielsen-Screier theorem), it can be characterized by a free generating set $K \subseteq F_X$, and G itself is completely described by X and K. For infinite groups this is ineffective, as the kernel has infinite rank (its index being equal to the order of G).

Since the kernel is a normal subgroup, instead of a free generating set one may consider a subset R whose normal closure (the intersection of all normal subgroups containing it) equals the kernel.

A presentation $\langle X | R \rangle$ of the group G consists of a generating set $X \subseteq G$ and a subset $R \subseteq F_X$ (relators) whose normal closure is the kernel of $\mathfrak{i}^\flat_X$. G is finitely presented if it has a presentation in which both X and R are finite: such groups are amenable to algorithmic methods.

Examples of finitely presented groups:

1) $\langle\{x\}\,|\,\{x^n\}\rangle$ for $n > 1$ is a presentation of the additive group $\mathbb{Z}_n$ of residue classes modulo n (i.e. the cyclic group of order n);

2) a presentation of the group $\mathbb{D}_n$ $(n > 2)$ is $\big\langle\{\sigma_1, \sigma_2\}\,|\,\big\{\sigma_1^2, \sigma_2^2, (\sigma_1\sigma_2)^n\big\}\big\rangle$;

3) $\big\langle\{s, t\}\,|\,\big\{s^2, t^3, (st)^n\big\}\big\rangle$ is a presentation of

- the symmetry group **T** of a tetrahedron for $n = 3$;
- the symmetry group **O** of an octahedron for $n = 4$;
- the symmetry group **I** of an icosahedron for $n = 5$;
- an infinite hyperbolic symmetry group for $n > 5$.

Combinatorial group theory: study groups using finite presentations.

Powerful algorithms available (Knuth-Bendix, Todd-Coxeter, Reidemeister-Schreier, etc.), but not always terminating.

Basic algorithmic problem (word problem): for a finite presentation $\langle X|R\rangle$, decide whether two elements $w_1, w_2 \in F_X$ are mapped to the same element, i.e. whether $\mathfrak{i}^{\flat}_X(w_1) = \mathfrak{i}^{\flat}_X(w_2)$.

Isomorphism problem: decide whether two finite presentations $\langle X_1|R_1\rangle$ and $\langle X_2|R_2\rangle$ describe isomorphic groups.

There is no algorithm solving the above problems in a finite number of steps for all groups, and even worse, there are explicit examples of groups where the word problem has no solution (is undecidable).

12 Conjugacy classes

The group elements $x, y \in G$ (resp. subgroups $H, K < G$) are conjugate, if there exists $g \in G$ such that $xg = gy$ (resp. $Hg = gK$).

The conjugacy class of a group element (resp. subgroup) is the set of all group elements (resp. subgroup) conjugate to it.

Two conjugacy classes are either equal or disjoint, and each element (resp. subgroup) belongs to a conjugacy class, hence conjugacy classes form a partition of the set of all group elements (resp. subgroups).

Members of the same conjugacy class are related by automorphisms, hence they have many algebraic properties (e.g. their order) in common.

The identity element forms a conjugacy class in itself, the trivial class.

More generally, any central element (i.e. a group element commuting with all other group elements) forms a class in itself (such conjugacy classes of size 1 are called central classes).

A subgroup forms a conjugacy class in itself precisely when it is normal.

The cosets of the centralizer $\mathtt{C}_G(x)=\{y\in G\,|\,xy=yx\}$ of a group element $x\in G$ are in one-to-one correspondence with the different conjugates of x; in particular, the number of the latter is equal to the index $[G:\mathtt{C}_G(x)]$.

Consequence: the size of a conjugacy class divides the order of the group.

Example: the elements of the dihedral group $\mathbb{D}_3$ form the following conjugacy classes

$$\mathcal{C}_1 = \{\mathbf{1}\}\,,\ \mathcal{C}_2 = \left\{C, C^{-1}\right\} \quad \text{and} \quad \mathcal{C}_3 = \{\sigma_1, \sigma_2, \sigma_3\}$$

The first class is the trivial one, the second contains the order 3 rotational (orientation-preserving) symmetries, while the class $\mathcal{C}_3$ consists of the (orientation-reversing) reflection symmetries of order 2.

The subgroups of $\mathbb{D}_3$ fall into 4 conjugacy classes: the trivial subgroup $\{\mathbf{1}\}$, the rotation subgroup $\mathtt{C}_3 = \left\{1, C, C^{-1}\right\}$, and the whole group $\mathbb{D}_3$ form a conjugacy class in themselves (because they are normal subgroups), while the 3 cyclic subgroups $\langle\sigma_i\rangle = \{1, \sigma_i\}$ of order 2 (generated by the reflection symmetries σ_i) form a single conjugacy class.