Monoids and Groups

joseph.muscat@um.edu.mt
1 October 2013

The simplest case of a universal algebra (*magma*) is a set X with a single binary operation $X^2 \to X$, $(x, y) \mapsto xy$. The morphisms are those maps such that

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

Isomorphisms are the bijective morphisms.

Elements x and y are indistinguishable by the operation when $ax = ay$, and $xa = ya$ for all $a \in X$. This is a congruence relation that can be factored away to leave only distinguishable elements. In any case one can introduce an identity 1 with

$$x1 = x = 1x.$$

1 is unique ($1 = 11' = 1'$, so any left identity equals any right identity). A morphism takes 1 to the identity of ϕX (since $\phi(x) = \phi(1x) = \phi(1)\phi(x)$), but $\phi(1) = 1$ is an extra property that ought to be satisfied by morphisms; its **kernel** is the sub-algebra $\phi^{-1}(1)$; zero object is $\{1\}$; not Cartesian-closed (the terminal and initial objects are the same, yet not all groups are isomorphic).

A *quasi-group* is a set with an operation that satisfies cancelation: every equation $ax = b$, and $xa = b$, has a unique solution; a *loop* is a quasi-group with identity.

*	**Finite**	**Finitely-Generated**	
Monoids $(xy)z = x(yz)$	$\mathbb{Z}_n$	Free monoid n^*	$\mathbb{N}^*$
Groups x^{-1}	‘product’ of simple groups, S_n; all simple groups known.	Free group A^*	B_∞
Solvable groups	‘product’ of abelian groups eg $\lvert G\rvert = p^r q^s$; D_n, $n \neq 2^r$; G odd;	e.g. invertible upper triangular $n \times n$ matrices	
Nilpotent groups	‘product’ of p-groups	e.g. Heisenberg group	
	$C_p^2 \rtimes C_p, C_{p^2} \rtimes C_p$ p-**groups** eg Q_n, D_{2^r} $C_p \,\big\vert\, C_{p^2}, C_p^2 \,\big\vert \ldots$		
Abelian groups	$C_{p^r} \times \ldots \times C_{q^s}$	$\mathbb{Z}^n \times G_{\text{finite}}$	eg $\mathbb{Q}+$, C_{p^∞}

1 Monoids

A **semi-group** is a set X with an operation which is associative,

$$(xy)z = x(yz).$$

A semi-group with an identity 1 is called a **monoid**. The model for monoids is the composition of morphisms $\phi : X \to X$ in any category (e.g. the functions X^X).

The ordered product of n-terms is associative (by induction), so can omit brackets $x_1 \cdots x_n$.

$\mathbb{N}$ acts on the monoid by defining x^n, where $x^{n^+} := x^n x$ and $x^0 := 1$; then

$$x^{m+n} = x^m x^n, \qquad x^{mn} = (x^m)^n.$$

Products $X \times Y$ and Exponentials X^A are again monoids:

$$(x_1, y_1)(x_2, y_2) := (x_1x_2, y_1y_2), \qquad (fg)(a) := f(a)g(a)$$

with identity $(1, 1)$ and the constant function 1 respectively.

A *zero* is a (unique) element 0 such that $0x = 0 = x0$ for all x. (One can always adjoin a zero.)

Examples:

-

$\mathbb{Z}_1$	1
1	1,

$\mathbb{Z}_2$	0	1
0	0	0,
1	0	1

	1	2
1	1	2
2	2	1

	1	2	3	4
1	1	2	3	4
2	2	2	4	4
3	3	2	1	4
4	4	2	2	4

- Free monoid on an alphabet $A = \{ a, b, \dots \}$: $A^* := \{ \_, a, b, aa, ab, bab, \dots \}$ with word concatenation; e.g. $\mathbb{N} \cong \{ 1 \}^*$.

  If one selects some words $w, u, \dots \in A^*$, then the relation $x \sim y$, defined as x and y being the same word except for some inserted w's, u's,..., is a congruence, which can be factored away to give the monoid $[\![A : w = 1, u = 1, \dots]\!] := A^*/\sim$.

- $\mathbb{N}$, or $\mathbb{Z}_n$ with multiplication $\pmod{n}$.

- The trivial monoid on any set X with $xy := 0$ for a selected element $0 \in X$, except $1x = x1 := x$ (if $X \neq 0$).

- In any category, the set of morphisms on any object $X \to X$, with composition.

- Every monoid is embedded in some X^X (using $a \mapsto \sigma_a$ where $\sigma_a(x) := ax$). The notation used for a function f when X is finite is $\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$. X is then called an *automaton* on X.
- In general, X *acts* on a set (or object) A when there is a morphism from X to A^A, i.e., $(xy) \cdot a = x \cdot (y \cdot a)$, $1 \cdot a = a$. Accordingly, each x may be 1-1, onto, etc. A morphism on an action is a map $f : A \to B$ such that $f(x \cdot a) = x \cdot f(a)$; its *kernel* is the relation $a \sim b \Leftrightarrow f(a) = f(b)$. Every action of X on A induces an action on its subsets, $x \cdot B := \{ x \cdot b : b \in B \}$. An action preserves a relation when $a \sim b \;\Rightarrow\; x \cdot a \sim x \cdot b$ for all x (it always preserves the relations $=$ and True).
- Subsets of a monoid 2^X: product $AB := \{ ab : a \in A, b \in B \}$ and identity $\{ 1 \}$.
- Any bounded semi-lattice with $\vee$ or $\wedge$.

There can be no general algorithm that decides whether (i) two words in a monoid are equal, and (ii) two monoids are isomorphic (even when finitely generated). Example: Let $A \subset \mathbb{N}$ be such that $n \in A$ is undecidable; then $[\![a, b, c, d : a^n b a^n = c^n d c^n, n \in A]\!]$ has unsolvable word problem.

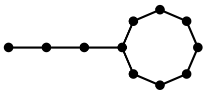
Sub-monoids: The sub-semigroup generated by a subset A is

$$[\![A]\!] = \{ a_1 \cdots a_n : a_i \in A, n \in \mathbb{N} \}$$

It must contain the same identity as X for it to be a sub-monoid. For example, the *cyclic* sub-monoids, $[\![a]\!] = \{ a^n : n \in \mathbb{N} \}$.

Proposition 1

Cyclic sub-monoids are isomorphic to
(i) $C_{n,k} := \{ 1, a, \ldots, a^{n+k-1} : a^{n+k} = a^n \}$ $(k \geqslant 1)$ **when finite, or to**
(ii) $C_{\mathbb{N}} := \{ 1, a, a^2, \ldots \}$ **when infinite.**



n, k, $n + k$ are called the *index*, *period*, and *order* of a.

For an element with finite order, $x^{m+s} = x^m \Leftrightarrow k|s$, and the index and period of x^i $(i < n + k)$ are $\lceil n/i \rceil$ and $\mathrm{lcm}(i, k)/i$ respectively.

An **idempotent** is an element e satisfying $e^2 = e$; 1 and 0 are examples. Every $C_{n,k}$ contains an idempotent (take $e := x^{mk}$ for $mk \geqslant n$; non-trivial if $n \geqslant 1$). A *root of unity* satisfies $a^k = 1$ for some k, $[\![a]\!] = C_{0,k}$.

A monoid is *periodic* when any cyclic sub-monoid $[\![a]\!]$ is finite, e.g. finite monoids. In particular, it is called *aperiodic* when $k = 1$ for each x. X is called *locally finite* when for any finite subset A, $[\![A]\!]$ is finite ($[\![a, b : a^2 = 1 = b^2]\!]$ is not locally finite).

Other examples of sub-monoids are the **local** sub-monoid eXe associated with an idempotent e, the **stabilizer** of a subset A by an action

$$N_A := \{\, x \in X : x \cdot a = a, \forall a \in A \,\},$$

and the **centralizer** of a subset $Y \subseteq X$,

$$Z(Y) := \{\, x \in X : xy = yx, \forall y \in Y \,\}.$$

It is the adjoint set for the relation $xy = yx$, so $A \subseteq Z(B) \Leftrightarrow B \subseteq Z(A)$, and the centralizer satisfies all the properties of self-dual maps: $A \subseteq B \Rightarrow Z(B) \subseteq Z(A)$, $A \subseteq Z(Z(A))$, $Z(Z(Z(A))) = Z(A)$. The **center** $Z(X) := \{\, a : \forall x \in X, ax = xa \,\}$ is a commutative sub-monoid; $Z(X \times Y) = Z(X) \times Z(Y)$.

The sub-monoids of X form a bounded lattice, with $H \wedge K = H \cap K$ and $H \vee K = [\![H \cup K]\!]$ (more generally, $\bigwedge_i H_i = \bigcap_i H_i$, $\bigvee_i H_i = [\![\bigcup_i H_i]\!]$); atoms in this lattice are cyclic sub-monoids.

1.1 Invertibility

The relation "$ax = b$ has a solution in x" is a pre-order, denoted $a|b$ (b is called a *multiple* of a and a a *divisor* of b); (also "$xa = b$ has a solution", or "$ax = b$ AND $xa = b$ have a solution"; all are here denoted by $|$). Write $a \equiv b$ for $a|b$ and $b|a$ (i.e., a, b are $|$-indistinguishable); this is a congruence, i.e., $x \equiv y \;\Rightarrow\; ax \equiv ay$; $X/\equiv$ is called a "pure" monoid.

There are three broad classes of elements:

(i) *Divisors of zero* are (non-zero) elements a, b such that $ab = 0$. In particular, a *nilpotent* satisfies $a^n = 0$ for some $n \in \mathbb{N}$. Divisors of zero give rise to nilpotents: $ab = 0 \;\Rightarrow\; (ba)^2 = 0$. A *super-nilpotent* has the property that any word with n a's in it is 0.

Monoids vary in their content of nilpotents: *reduced* monoids have only 0 as nilpotent, i.e., $x^2 = 0 \;\Rightarrow\; x = 0$ (since for $n \geqslant 2$, $x^n = 0 \;\Rightarrow\; x^{2(n-1)} = 0 \;\Rightarrow\; x^{n-1} = 0$); then $xy^n = 0 \;\Rightarrow\; xy = 0 = yx \;\Rightarrow\; xzy = 0$ (since $yxyyxy = 0$); *primary* monoids have all divisors of zero as nilpotent.

The map $A \mapsto \mathrm{rad}(A) := \{\, x \in X : x^n \in A, \exists n \in \mathbb{N} \,\}$ is a closure map on sets (for $\subseteq$); a 'closed' set is called *radical*, i.e., $x^n \in A \;\Rightarrow\; x \in A$. Examples are the set of nilpotents $r(0)$, and of the left zero divisors (since $a^n b = 0 \;\Rightarrow\; c := a^{n-1}b = 0$ OR $ac = 0$).

$$r(A \cup B) = r(A) \cup r(B), \quad r(A \cap B) \subseteq r(A) \cap r(B)$$

(ii) A *regular* element a satisfies $a = aba$ for some $b \in X$. So ab and ba are idempotents; there exist elements c (e.g. $c = bab$) such that $aca = a$, $cac = c$; equivalently, $a \equiv e$ an idempotent (since $a \equiv ab$; if $ax = e$, $ey = a$, then $a = eey = axa$). Regular elements may be divisors of zero.

If idempotents commute, then the b in $a = aba$ is unique, called its 'inverse' (since $e_1 \equiv e_2 \;\Rightarrow\; e_2 = e_1 x = e_1 e_1 x = e_1 e_2 = e_2 y = e_1$, so if $a \equiv e$, then e is unique, i.e., $ab = e = ac$; thus $b = bab = bac = cac = c$).

(iii) An element a is left **cancellative** when $ax = ay \Rightarrow x = y$ (so $a|b$ uniquely; equivalently, the map $x \mapsto ax$ is 1-1; similarly for right-cancellative); the set of left(/right)-cancellative elements is a sub-monoid. Divisors of zero and idempotents (except 1) are not cancellative; more generally, a cancellative element has no finite "tail": either $[\![a]\!] = C_{0,k}$ or $[\![a]\!] = C_{\mathbb{N}}$ (since $a^{n+k} = a^n \Rightarrow a^k = 1$, a root of unity).

In particular are the left (/right) **invertible** elements, i.e., those a that have a left inverse b, such that $ba = 1$; (equivalently, $a \equiv 1$, or $x \mapsto xa$ is onto, or a is cancellative regular). For example, roots of unity $a^{-1} = a^{k-1}$.

A left and right invertible element has a unique *inverse*, denoted a^{-1} (since $b = b1 = bab' = 1b' = b'$). One can extend the definition $x^{-n} := (x^{-1})^n$ still satisfying the index laws (so $\mathbb{Z}$ acts on X).

Morphisms preserve $|$, idempotents, regular and invertible elements, and

$$\phi(x^{-1}) = \phi(x)^{-1}$$

(since $1 = \phi(1) = \phi(x^{-1}x) = \phi(x^{-1})\phi(x)$, etc.). Morphisms such that $\phi(0) = 0$ preserve divisors of zero and nilpotents.

An invertible element $a \in X$ acting on a set (or its subsets) is a bijection $\sigma_a : x \mapsto a \cdot x$, called a *permutation*.

Proposition 2

The set of invertible elements is a sub-monoid called a *group* $\mathcal{G}(X)$:

$$1^{-1} = 1, \quad (a^{-1})^{-1} = a, \quad (ab)^{-1} = b^{-1}a^{-1}$$

Proof. $1.1 = 1$; $a^{-1}a = 1$; $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = 1 = (b^{-1}a^{-1})(ab)$.

Note: If all elements are left-invertible then they are invertible, since $\forall x, \exists y, z,\ xy = 1 = yz$, so $yx = yxyz = yz = 1$.

Examples:

- The permutations $\mathcal{G}(X^X) = S(X)$.
- The multiplicative group $\mathcal{G}(\mathbb{Z}_n) = \Phi_n := \{\, m > 0 : \gcd(m, n) = 1 \,\}$.

  Proof: let $d := \gcd(a, n) = ra + sn$; if $d = 1$ then $ra = 1 \pmod{n}$; if $d \neq 1$ then $a = db$, $n = dc$, so $ac = bn = 0 \pmod{n}$.
- $\mathcal{G}(X \times Y) = \mathcal{G}(X) \times \mathcal{G}(Y)$.

Let G be a subgroup of X. The relation $x \sim y \Leftrightarrow y = xa,\ \exists a \in G$, is an equivalence relation, which partitions X into *cosets* xG. G is called a **normal** subgroup, $G \trianglelefteq X$, when the relation is a congruence, equivalent to $xG = Gx$ for all x (or $xG = Gy$ for some y); conversely, a congruence relation gives rise to the submonoid $M := [1]$, and $xM, Mx \subseteq [x]$. For a normal subgroup, $X/G := X/\!\sim$ is a monoid with operation $(xG)(yG) = (xy)G$ (see Universal Algebras).

1.1.1 Automorphisms

The *automorphisms* of X form another group $\mathrm{Aut}(X)$. The relation $x = \phi(y), \exists\phi \in \mathrm{Aut}(X)$ is an equivalence relation. A subset of X which is invariant under all automorphisms, $\phi A = A$, is called *characteristic*.

Conjugation by an invertible element a is the action $\tau_a : x \mapsto a^{-1}xa$, an automorphism of X (called an *inner* automorphism, $\mathrm{Inner}(X)$). $\tau_{ab} = \tau_a\tau_b$, so $a \mapsto \tau_a$ is a morphism $\mathcal{G}(X) \to \mathrm{Aut}(X)$, so $\mathrm{Inner}(X) \trianglelefteq \mathrm{Aut}(X)$ (but not characteristic unless trivial); the kernel of τ is $Z(X) \cap \mathcal{G}(X)$. A subset is called a **normal** subset when it is invariant under all inner automorphisms; e.g. every subset of the center. Note that $xa = \tau_a(ax)$, so xa and ax behave in analogous ways when a is invertible.

More generally, a and b are *weakly conjugate* when (i) $ax = xb$ for some x, (ii) $a = xy$, $b = yx$ for some x, y, or (iii) $b = x^{-1}ax$ for some x; (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). If a is nilpotent, then so is b (since $(yx)^{n+1} = y(xy)^n x = 0$).

1.2 Ideals

A **ideal** is a subset I such that $XIX \subseteq I$ (i.e., an upper closed set in $|$). So, if an ideal contains an invertible element then it is X; the intersection or union of ideals is an ideal; the smallest such is called the *minimal* ideal. Ideals are normal subsets of X, but not necessarily characteristic.

1. Each element a generates a ("principal") left ideal Xa ("multiples" of a), a right ideal aX, and the ideal XaX. There are three associated equivalence relations ($x|y$ AND $y|x$): $Xx = Xy$, $xX = yX$ and $XxX = XyX$, giving three partitions of equivalence classes L_x, R_x and J_x. (Note: $L_x \subseteq Xx$ but not necessarily equal.)

   For example, when $X = A^A$, $Xf = Xg \Leftrightarrow \mathrm{im}\, f = \mathrm{im}\, g$, $fX = gX \Leftrightarrow \ker f = \ker g$.

2. For any morphism, $\phi^{-1}0$ is an ideal; and conversely, every ideal is of this type for $\phi : x \mapsto \begin{cases} 0 & x \in I \\ 1 & x \notin I \end{cases}$.

3. The set of common divisors $\mathrm{Div}(A) := \mathrm{Lowerbounds}(A)$, and the set of common multiples $\mathrm{Mult}(A) := \mathrm{Upperbounds}(A)$, are ideals (for $a|b \Leftrightarrow xa = b$ AND $ay = b$, $\exists x, y$).

4. An element is called *invariant* when $aX = Xa$. They form a submonoid that includes the center and the invertibles. An invariant nilpotent element is super-nilpotent.

5. The coarsest partition contained in L and R is called H, induced by the equivalence relation $Xx = Xy$ AND $xX = yX$, i.e., $L_x \cap R_y = \varnothing$ or H_z for some z.

6. If $aX = bX$, so $a = bp$, $b = aq$, then the map $f_q : x \mapsto xq$ is a bijection $L_a \to L_b$ which permute $H_c \mapsto H_{cq}$, $R_c \mapsto R_c$.

   Proof. If $x \in L_a$, then $Xxp = Xap = Xb$, so $xp \in L_b$. Also, $x = x'a = x'bq = x'apq = xpq$; similarly any $x \in L_b$ satisfies $x = xqp$. So f_q is 1-1 and onto; and for $x \in L_a$, $xX = xpX$.

7. *Proposition* 3

   Either H_a is a subgroup (containing an idempotent e) or $H_a \cap H_a^2 = \varnothing$. If e is an idempotent, then $L_e = \{ x : x|e, xe = x \}$, and $H_e = \{ x : ex = x = xe, \exists a, b, ax = e = xb \}$ is the largest subgroup containing e.

   In particular H_1 is the group of invertibles.

   Proof. If $x, y \in H_e$, then $e = by = bey = baxy$ and $e = xa' = xea' = xyb'a'$, so $xy \in H_e$. Also, $ae = axa' = ea'$, so $xae = xa' = e$, $aex = ax = e$, which implies that ae is the inverse of x and belongs to H_e. Any subgroup G which contains x, e gives $x = xe = ex$, $e = x^{-1}x = xx^{-1}$, so $Xx = Xe$, $xX = eX$ and $x \in H_e$, i.e., $G \subseteq H_e$.

   If $H_a^2 \cap H_a \neq \varnothing$ then $a = bc$ (wolog) for some elements $b, c \in H_a$. Since $aX = bX$, f_c is a bijection on $H_b \to h_a$, so $H_a c = H_a$. Hence $c = ec$ for some $e \in H_a$, and as $cX = eX$, $e = cx$; so $e = cx = ecx = e^2$ is an idempotent.

8. The finest partition containing L and R (their join) is called D, induced by the equivalence relation $\exists z, Xx = Xz$ AND $zX = yX$ ($\Leftrightarrow$ $xX = rX, Xr = Xy$); J is coarser. Each D_a is the union of some L_x, and of some R_x.

   If idempotents $e \in D_{e'}$ then $H_e \cong H_{e'}$ (since $\exists a \in L_e \cap R_{e'}$; so $e = abe = ae'be =: ac$; but $e' = da = daba = e'ba = ca$, so the map $x \mapsto cxa$ is the required isomorphism $cxya = cxeya = (cxa)(cya)$.)

2 Commutative Monoids

satisfy $xy = yx$.

1. So there is only one notion of $|$, $L_a = R_a = H_a = J_a$, left inverses are inverses.

2. $(xy)^n = x^n y^n$, so $x \mapsto x^n$ is a morphism. The subsets $\{ x^n : x \in X \}$ are sub-monoids of squares, cubes, etc.

3. The operation itself $X^2 \to X$ is a morphism. The set of morphisms to a commutative monoid $\mathrm{Hom}(X,Y)$ is itself a commutative monoid (in fact a semi-ring) with $(\phi\psi)(x) := \phi(x)\psi(x)$, e.g. $\mathrm{Hom}(\mathbb{N}) = \mathbb{N}$. More generally, morphisms $\phi : X_1 \to Y$, $\psi : X_2 \to Y$, combine to form the morphism $X_1 \times X_2 \to Y$, $(x_1, x_2) \mapsto \phi(x_1)\psi(x_2)$.

Examples: $\mathbb{N}, +$ (divisibility is $\leqslant$); $\mathbb{N}, \times$; the monoid $\{1, a, a+b, a+2b, a+3b, \ldots\}$, where $a^2 = a \pmod b$, $a \leqslant b$, with multiplication; the center, which contains the subgroup $\mathcal{G}(X) \cap Z(X)$.

The product IJ of ideals is an ideal ($\subseteq I \cap J$). The radical of an ideal $\mathrm{rad}(I)$ is an ideal, and $\mathrm{rad}(IJ) = \mathrm{rad}(I) \cap \mathrm{rad}(J)$.

An element a may split up as $a = bc$ (without b, c being 1); this decomposition may continue until, perhaps, elements are reached that do not split this way. An element a is **irreducible** when $a = bc \;\Rightarrow\; a \equiv b$ OR $a \equiv c$; equivalently they are the atoms of $|$. It is **prime** when $a \not\equiv 1$ and $a|xy \;\Rightarrow\; a|x$ OR $a|y$; primes are irreducible ($p = xy \;\Rightarrow\; p|xy \;\Rightarrow\; p|x \;\Rightarrow\; p \equiv 1$).

A **prime** ideal is a proper ideal such that its complement is a sub-monoid,

$$xy \in P \Leftrightarrow x \in P \text{ OR } y \in P,$$

equivalently, $IJ \subseteq P \Leftrightarrow I \subseteq P$ OR $J \subseteq P$.

1. Morphisms pull back prime ideals to prime ideals $\phi^{-1}P$.

2. The union of prime ideals is a prime ideal, the largest being the complement of the group of invertibles (since if ab is invertible then so are a, b); the smallest is $\varnothing$.

3. Prime ideals are radical, i.e., $\mathrm{rad}(P) = P$. So every prime ideal that contains I also contains $\mathrm{rad}(I)$.

4. The set of prime ideals is called the *spectrum* of X; it has a Zariski topology in which the closed sets are $F_I = \{P \text{ prime ideal} : I \subseteq P\}$, where I is an ideal. It is a monoid (with $\cup$) which is isomorphic to $X^* := 2^X$ (monoid of morphisms to 2) via the map $\phi \mapsto \phi^{-1}0$. Then $X^{**} \cong X$.

Commutative monoids of idempotents are semi-lattices. Every commutative monoid gives rise to a congruence relation $x \sim x^n$ for all $n \geqslant 1$, $x \in X$; then $X/\!\sim$ is a semi-lattice, with $\mathrm{Spec}(X) \cong 2^X \cong 2^{X/\sim} \cong \mathrm{Spec}(X/\!\sim)$.

The set of elements $F_n := \{x : x^n = 1\}$ is a subgroup.

X can be embedded in a monoid in which all cancellative elements become invertible; the minimal group extension is the following construction $S^{-1}X$ for any cancellative sub-monoid S: take the monoid $X \times S$ and write pairs (x, s) as $\frac{x}{s}$; identify $\frac{x_1}{s_1} \approx \frac{x_2}{s_2} \Leftrightarrow x_1 s_2 = x_2 s_1$ (a congruence); X is embedded via $x \mapsto \frac{x}{1}$, and for any cancellative $t \in X$, $\left(\frac{t}{s}\right)^{-1} = \frac{s}{t}$.

For example, $\mathbb{N}, +$ gives rise to $\mathbb{Z}$; the equivalence classes are represented by either $(n, 0)$ or $(0, n)$ ($n \in \mathbb{N}$), the latter denoted by $-n$ (and (m, n) as $m - n$).

2.1 Commutative monoids with cancelation

The relation $a \equiv b$ becomes $a \sim b$ ($a = bc$ for some invertible c). When finitely generated, X is isomorphic to a quotient of $\mathbb{N}^m$.

2.1.1 Factorization

An **atomistic monoid** is a cancellative commutative monoid with the *factorization* property: Every non-invertible element has a factorization into irreducibles $x = a_1 \cdots a_k$. For example, when $|$ is a DCC order (each element a is either irreducible, or decomposes as bc, $b, c \not\equiv 1$; if both have factorizations, then so would $a_1 := a$; otherwise take a_2 to be b or c, whichever does not have a factorization; continuing like this gives a strict sequence $\cdots a_3 | a_2 | a_1$. By DCC, this sequence is finite, a contradiction unless a has a factorization of irreducibles).

Examples:

- The multiplicative monoid $\{\, 1, a, 2a, 3a, \ldots \,\}$ ($a \in \mathbb{N}$) has irreducibles but no primes, and can admit several factorizations into irreducibles (e.g. for a prime, the irreducible a divides $a(aqr) = (aq)(ar)$ but not aq or ar).

- The monoid $\{\, 1, 1 + a, 1 + 2a, \ldots \,\}$ has infinitely many primes (primes of $\mathbb{N}$ in X are primes of X; so apply Dirichlet's theorem). There need not be unique factorization, e.g. for $a = 3$, $100 = 4.25 = 10.10$, so 10 divides 4.25 but not 4 or 25.

- The "numerical monoid" $[\![a_1, \ldots, a_r]\!] = \{\, n_1 a_1 + \cdots + n_r a_r : n_i \in \mathbb{N} \,\}$ with addition.

Factorial Monoids are atomistic monoids with factorization that is unique up to invertibles.

1. Equivalently, irreducibles are primes.

   Proof. Let p be irreducible and $p|ab$; so $pc = (r_1 \cdots r_n)(s_1 \cdots s_m)$ and one of r_i or s_j must be p (up to an invertible). The converse is the following:

2. A *prime* decomposition is unique.

   Proof. Suppose $p_1 \cdots p_n q_1 \cdots q_m \equiv p_1 \cdots p_n r_1 \cdots r_k$ with q_i, r_j distinct; then by cancelation, $q_1 \cdots q_m \equiv r_1 \cdots r_k$ ($k \geqslant m$, say), so $q_i | r_j$, i.e., $r_j = q_i a$, and q_i can be eliminated; by induction $1 \equiv r_1 \cdots r_k$ so r_j is invertible, a contradiction.

3. $X/\equiv$ is isomorphic to the free monoid on the irreducibles.

4. The gcd $x \wedge y$ and lcm $x \vee y$ exist, and $|$ is a distributive lattice; they satisfy $xy = (x \wedge y)(x \vee y)$, $(ax) \wedge (ay) = a(x \wedge y)$, $(ax) \vee (ay) = a(x \vee y)$.

   Proof. If $x = pr$, $y = ps$, where r and s have no common primes, then $x \wedge y = p$, $x \vee y = prs$; thus $(ax) \wedge (ay) = ap$, $(ax) \vee (ay) = aprs$. If $x = prsa$, $y = prtb$, $z = pstc$, then $(x \wedge y) \vee z = (pr) \vee (pstc) = prstc = (prstca) \wedge (prstcb) = (x \vee z) \wedge (y \vee z)$.

Example: $\mathbb{N}$: it is clearly a DCC; suppose $pa = qb$ is the smallest number that does not have a unique factorization (so $p - q, b - a$ have unique factorizations); then $(p - q)a = q(b - a)$ is a smaller counterexample.

3 Groups

A **group** is a monoid G in which every element is invertible.

Examples:

- The *free group* generated by an alphabet $A = \{ a, b, \dots \}$: let B be a disjoint copy of A, then the monoid $[\![A \cup B : ab = 1 = ba, \dots]\!]$ is a group; e.g. the free group generated by 1 is $\mathbb{Z}$.

  Every group is the quotient of a free group.
- The set of automorphisms (*symmetries*) of an object in a category form a group. In particular, the permutations of a set, $S(X)$ $(= \mathcal{G}(X^X))$, called the *symmetric* group on X.
- $\mathbb{Q}^\times := \mathbb{Q} \smallsetminus 0$ with multiplication.
- The set of bounded rational-valued sequences that are bounded away from 0, with $(a_n)(b_n) := (a_n b_n)$.
- Periodic (e.g. finite) cancellative monoids, e.g. removing the tails from each $[\![x]\!]$.

A morphism is 1-1 iff $\phi^{-1}(1) = \{ 1 \}$; onto morphisms need not have a right-inverse; $\mathbb{Z}$ is a separator; the category is concrete, complete and co-complete.

3.1 Subgroups

The subgroup generated by a subset $A \subseteq G$ is

$$[\![A]\!] = \{ a_1 \cdots a_n : a_i \in A \text{ OR } a_i^{-1} \in A \text{ OR } a_i = 1, n \in \mathbb{N} \} = \bigcup_{n \in \mathbb{N}} (A \cup A^{-1})^n.$$

A set is *independent* when for all $a \in A$, $a \notin [\![A \smallsetminus a]\!]$.

1. The translates of a subgroup, xH called *cosets*, partition G into equally sized subsets; so $|H|$ divides $|G|$.
2. $[\![x]\!]$ is isomorphic to a cyclic group C_n or to $\mathbb{Z}$ via $i \mapsto x^i$. The order $o(x)$ divides $|G|$. Moreover,

   (a) $o(x^m) = \operatorname{lcm}(m, o(x))/m = o(x)/\gcd(m, o(x))$,

   (b) $x^a = y^b \;\Rightarrow\; o(x) | a\, o(y)$,

  (c) The number of elements of $[\![x]\!]$ of order n is $\phi(n)$ or 0 (since x^i has order n when $\gcd(i, o(x)) = o(x)/n$, iff $\gcd(i, n) = 1$).

3. The subgroups of G form a lattice.

   (a) $[\![H \cup K]\!] = HK \Leftrightarrow HK = KH$ (since $h_1k_1h_2k_2 = h_1h_3k_3k_2 \in HK$ and $(hk)^{-1} = k^{-1}h^{-1} = h_1k_1 \in HK$) (for example, when K is a normal subgroup);

   (b) $[\![H \cup K]\!] \cong [\![H]\!] \times [\![K]\!] \Leftrightarrow hk = kh$ AND $H \cap K = [\![1]\!]$. So if $G \cong H \times K$, there are induced idempotent morphisms $e : hk \mapsto h$, $f : hk \mapsto k$, such that $e \circ f = 1 = f \circ e$, $e \cdot f = \iota = f \cdot e$, $\ker e = K = \operatorname{im} f$. Conversely, given a right invertible morphism $\phi\psi = \iota$, then $G \cong \ker \phi \times \operatorname{im} \psi$ (with projection $\psi\phi$).

   (c) More generally, if $\bigcap_i H_i = \{ 1 \}$ then G is embedded in $\prod_i \frac{G}{H_i}$ via the map $x \mapsto (xH_i)$.

4. Morphisms map subgroups to subgroups, $[\![\phi A]\!] = \phi[\![A]\!]$; e.g. $x^{-1}[\![A]\!]x = [\![x^{-1}Ax]\!]$.

   A subgroup is normal iff $x^{-1}Hx = H$ for all x (i.e., when it is invariant under conjugation). The quotient G/H is a group.

   A subgroup is **characteristic** when it is invariant under any automorphism. A characteristic subgroup of a characteristic subgroup of G is characteristic in G.

5. The kernel $\phi^{-1}1$ of a morphism is a normal subgroup, and $\phi^{-1}(x)$ are its cosets.

6. The isomorphism theorems hold: $G/\ker\phi \cong \phi G$; if $H \leqslant G$ and $K \trianglelefteq G$ then $H \cap K \trianglelefteq G$ and $K \trianglelefteq HK$; moreover $HK/K = H/H \cap K$. (see Universal Algebras).

7. A subset A generates the normal subgroup $[\![g^{-1}ag : g \in G, a \in A]\!]$.

8. Every subgroup contains a normal subgroup $\bigcap_g g^{-1}Hg$, called its *core*.

9. Normal subgroups form a modular lattice.

   Proof. $H \vee K = HK$, and $xHK = HxK = HKx$. If $H \subseteq K$, and $k \in (HL) \cap K$, then $k = hl$, so $l = h^{-1}k \in K \cap L$, i.e., $k \in H(L \cap K)$, so $(H \vee L) \wedge K = H \vee (L \wedge K)$.

   (Note: a normal subgroup of a normal subgroup of G need not be a normal subgroup of G).

10. If a subgroup has 2 cosets, then it is a normal subgroup (since $H \cup xH$ and $H \cup Hx$ are both partitions, so $xH = Hx$). G thus divides into “even” and “odd” elements.

11. Any subgroup of a free group is again free (but may have bigger alphabets).

12. The *Cayley digraph* associated with $[\![A]\!]$ has edges $x \rightsquigarrow y \Leftrightarrow x \in yA$.

The center $Z(G)$ is characteristic (but $G \mapsto Z(G)$ is not a functor on groups).

The *torsion* subgroup is the set of elements with finite order; it is characteristic. The *order* of the torsion subgroup is the maximum order of its elements. Finitely-generated torsion groups are finite when the order is not large e.g. for orders 2,3,4,6; but for large enough orders, they may be infinite.

The *Frattini* subgroup is the intersection of all maximal subgroups; it is characteristic.

3.2 Group Actions/Representations

The map $a \mapsto \sigma_a$ embeds G in $S(G)$, the group of permutations of G. More generally, a morphism $G \to S(X)$ is called a representation or *action* ($1 \cdot x = x$, $(gh) \cdot x = g \cdot (h \cdot x)$). Two actions are called equivalent when there is a map $\phi : G \to G, X \to X$ such that

$$\phi(g) \cdot \phi(x) = \phi(g \cdot x)$$

A group action is a category (or groupoid), with $x \in X$ as the objects and $g \in G$ as the morphisms.

The action extends to subsets of X, $g \cdot A = \{\, g \cdot a : a \in A \,\}$; and to function Y^X, $(g \cdot f)(x) := f(g^{-1} \cdot x)$ (so the category of G-actions is a topos, with Ω consisting of the set of left-ideals of X and the action $gI = \{\, h : hg \in I \,\}$).

The **orbit** of $x \in X$ is $Gx := \{\, g \cdot x : g \in G \,\}$;

The **fixed points** of $g \in G$ is the set $X_g := \{\, x \in X : g \cdot x = x \,\}$;

The **stabilizer** subgroup of x is $G_x := \{\, g \in G : g \cdot x = x \,\}$.

Also, $X_G := \{\, x \in X : G \cdot x = x \,\}$ and $G_X := \{\, g \in G : g \cdot x = x, \forall x \,\} = \ker \sigma = \bigcap_{x \in X} G_x = \bigcap_{g \in G} gG_xg^{-1}$.

1. X partitions into orbits (since $1 \cdot x = x$ and $g \cdot x = h \cdot y \Rightarrow x = g^{-1}h \cdot y \in Gy \Rightarrow Gx = Gy$).

2. The size of an orbit equals the number of cosets of the corresponding stabilizer subgroup $|Gx| = |G| \,/\, |G_x|$ (since $g \cdot x = h \cdot x \Leftrightarrow h^{-1}g \cdot x = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x$); so

$$|X| = |G| \sum_{[x]} \frac{1}{|G_x|} = |X_G| + \sum_{[x], G_x \neq G} \frac{|G|}{|G_x|}.$$

3. $y = g \cdot x \Leftrightarrow G_y = gG_xg^{-1}$. Thus G_x determines the action of G on Gx.

4. The action of G on one orbit is called *transitive*; two transitive actions (on orbits Gx and Gy) are equivalent $\Leftrightarrow \exists g \in G, g^{-1}G_xg = G_y$, so that the number of transitive actions is equal to the number of conjugacy classes of stabilizer subgroups.

   ($\phi(g \cdot x) = g \cdot \phi(x) = ga \cdot y$, so $g \cdot x = x \Leftrightarrow ga \cdot y = a \cdot y \Leftrightarrow a^{-1}ga \in G_y$; conversely, let $\phi(g \cdot x) := ga \cdot y$ a bijective map from Gx to Gy)

5. G acts transitively on the cosets gH of a subgroup H. The stabilizer group of gH is gHg^{-1}. Conversely, any transitive action is equivalent to left multiplication by G on the cosets of G_x. Thus transitive actions are in 1-1 correspondence with the conjugacy classes of subgroups, via $G \mapsto \{ G_x : x \in G \}$.

6. The number of orbits equals the average number of fixed points of G, i.e.,

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

   Proof. The number of pairs (g, x) such that $g \cdot x = x$ is equal to $\sum_g |X_g|$ but is also equal to $\sum_{x \in X} |G_x| = \sum_x |G| / |Gx| = |G| \, . \, |X/G|$.

   For example (Polya), the number of necklaces with n beads, each of k possible colors, is $\frac{1}{2n} \sum_{d|n} \phi(d)k^{n/d} + \frac{1}{2}k^{\lceil n/2 \rceil}$ (by the action of D_n on k^n).

7. An action may transfer some elements of an orbit together in equally sized "blocks"; i.e., there may be a partition of an orbit such that $g \cdot A_i = A_j$ for each $g \in G$; e.g. $[\![(1, 2, 3, 4)]\!]$ acts on $\{ 1, 2, 3, 4 \}$ transitively but in blocks $\{ 1, 3 \}$, $\{ 2, 4 \}$. An action is called *primitive* when it preserves only the trivial equivalence relations (partitions). It must be transitive since the orbits are preserved.

   Primitive action iff G_x are maximal subgroups of G (Proof. If x is in block A, but $g \cdot x$ is in B, then $g \cdot A = B$; so a g which moves x in A still fixes A, so $G_A \supset G_x$. Conversely, if $G_x \subset H \subset G$, then the non-trivial partition $gH \cdot x$, $g \in G$, is preserved).

8. An action is called *n-transitive* when it maps any n ordered elements to any n elements.

9. An action is *faithful* when it is 1-1 ($G_X = [\![1]\!]$), i.e., $g \cdot x = h \cdot x, \forall x \Rightarrow g = h$. G/G_X acts faithfully on X.

   It is *free* when $g \cdot x = h \cdot x, \exists x \Rightarrow g = h$, i.e., each g, except 1, has no fixed points. It is *regular* when for any x, y, $g \cdot x = y$ has a unique solution for g; iff transitive and free; iff equivalent to the action of left multiplication on G.

10. For finite actions, each g creates a partition of X into finite orbits of size n_i; this can be encoded by the symbolic product $x_{n_1} \cdots x_{n_k}$. The *cycle index* of the action is the polynomial that consists of the sum of such products for all g.

More generally, a morphism $G \to \mathrm{Aut}(X)$ is called a *representation*, e.g. automorphisms of fields (called modular representations, when the field is finite), of vector spaces (linear representations), of Banach spaces (leads to topological groups and Lie groups), of compact geometrical objects (crystallography), of topological spaces (topological group actions).

3.3 Conjugates

Conjugation is another action of G on itself. They are the translations $x \mapsto axb$ that fix the identity.

1. The orbits of conjugation are called the *conjugacy classes* $C(x)$ of G; stabilizer groups are called the *centralizers* N_x (or normalizers when the action is on subgroups); $|C(x)| = |G| / |N_x|$, $|G|\,|C(x)| = \sum_{C(x)} |N_x|$, $|G| = \sum_{C(x)} |C(x)| = |Z(G)| + \cdots$.

2. $\bigcap_x x^{-1}Hx$ is the largest normal subgroup in H (since it is equal to the kernel of the morphism of the action by translations on H).

3. The quotient $\mathrm{Aut}(G)/\mathrm{Inner}(G)$ is called the *outer* automorphism group of G.

   If $g \notin H \trianglelefteq G$, then τ_g is an outer automorphism of H; conversely, by extending H by an element g, an outer automorphism becomes inner, by defining $g^{-1}xg := \phi(x)$.

4. The series $G \xrightarrow{\tau} \mathrm{Aut}(G) \xrightarrow{\tau} \mathrm{Aut}(\mathrm{Aut}(G)) \cdots$ continues until perhaps, it ends in a *complete* group, when τ is an isomorphism $\mathrm{Aut}(G) = \mathrm{Inner}(G) \cong G$ (so center is trivial). For example, G^n for G non-abelian simple; S_n $(n \neq 6)$.

5. There can be no general algorithm that decides whether $x, y \in G$ are conjugates (otherwise one can decide whether any two words are the same by checking if $x^{-1}y$ is conjugate to 1).

Adjoint: the mapping $x \mapsto [a, x] := a^{-1}x^{-1}ax$ is called the *commutator*;

$$yx = xy[y, x], \quad [x, y]^{-1} = [y, x], \quad \phi([x, y]) = [\phi(x), \phi(y)],$$

ϕ any morphism.

The commutator subgroup of sets A, B, is

$$[A, B] := [\![[a, b] : a \in A, b \in B]\!].$$

The *derived* group of G is $G' := [G, G]$ ($G \mapsto [G, G]$ is a functor); it is a characteristic subgroup and $G/[G, G]$ is the largest abelian image of G (since G/H is abelian $\Leftrightarrow$ $[G, G] \leqslant H$), and is the left-adjoint of the identity map from the category of abelian groups to that of groups.

3.4 Types of Groups

There are various ways that a group can be decomposed into simpler/smaller groups.

A group can be rebuilt from a normal subgroup H and its image $K := G/H$ as a product group: pick representatives k_i from each coset k_iH, via $s : G/H \to G$, so $g = kh$ for some unique $k = s(gH)$ and $h \in H$, and $k_1k_2 = s(k_1k_2H)f(k_1, k_2)$; then

$$g_1g_2 = k_1h_1k_2h_2 = k_1k_2\tau_{k_2}(h_1)h_2$$

since H is normal. Thus one can take the set $H\times K$ with a product $(h_1, k_1)(h_2, k_2) := (f(k_1, k_2)\tau_{k_2}(h_1)h_2, k_1k_2)$ via the map $(h, gH) \mapsto gh$ (τ_k can be outer automorphisms of H if G is unknown; and f must satisfy certain properties for this product to be associative). Such a product is called *semi-direct* $H \rtimes K$ when K is isomorphic to a subgroup of G, so $f = 1$ (H is said to be *complemented* by K); it is a direct product when also $\tau_k = 1$.

(However, note that knowing the group types of two of G, H, and G/H does not determine the other; e.g. "$(C_2 \times C_4)/C_2$" can mean either $C_2 \times C_2$ or C_4 depending on which $C_2 \trianglelefteq (C_2 \times C_4)$ subgroup is taken; "$(C_2 \times C_4)/C_4 \cong (C_2 \times C_4)/(C_2 \times C_2)$"; "$C_4/C_2 \cong (C_2 \times C_2)/C_2$".)

One can therefore keep looking for normal subgroups inside normal subgroups until, perhaps, a **simple** group is reached which doesn't have any non-trivial normal subgroups. To make this more procedural, a 'composition' series of normal subgroups are found

$$1 \trianglelefteq \cdots \trianglelefteq H_i \trianglelefteq H_{i^+} \trianglelefteq \cdots \leqslant G,$$

so that H_{i^+}/H_i is simple; thus every group is a 'product' of simple groups (building blocks). Since the normal subgroups form a modular lattice, the composition series has a unique length of 'unique' groups. But the length may be infinite, e.g. $\mathbb{Z}^{\mathbb{Z}}$ has an infinite ascending and descending chain of sub-groups of sequences of the type $(\ldots, *, *, 0, 0, \ldots)$. Note that non-trivial morphisms to/from a simple group are onto/1-1 respectively.

In particular, one can 'decompose' any group into a direct product of subgroups $G_1 \times \cdots \times G_k$ until, perhaps, what is left are 'indecomposable' groups. Also one can create a 'characteristic' series using maximal characteristic subgroups.

An obvious characteristic subgroup which gives an abelian factor is the derived group G'; when this is proper, it can be factored out (G/G', also called its first homology group), and the process repeated $G_{k+1} := G'_k$ to get the *derived series*

$$\ldots \trianglelefteq [G_k, G_k] \trianglelefteq \ldots \trianglelefteq [G, G] \trianglelefteq G.$$

Eventually perhaps, a **perfect** group is reached when $[G, G] = G$; for example non-abelian simple groups are perfect. If the process continues indefinitely, one can continue from the derived group $\bigcap_k G_k$. So G is a 'product' of abelian groups and a perfect group. Finite products, direct limits, and images of perfect groups are perfect. A finer series than the derived series is $G_{k+1} := [G_k, G]$, called the *lower central series*.

A group is **solvable** when the composition series ends at $[\![1]\!]$ and each factor G/H is abelian (cyclic when G is finite), so G is a 'product' of simple abelian groups. Products, images and subgroups of solvable groups are solvable.

A *polycyclic group* is a solvable group in which the factors G/G' are cyclic.

The *upper central series* is an ascending sequence of the 'centers' Z_k such that Z_{k+1}/Z_k is the center of G/Z_k, i.e., starting with the center Z, find the center of G/Z which maps back to a characteristic subgroup of G, thus $[\![1]\!] \trianglelefteq Z \trianglelefteq Z_2 \trianglelefteq \cdots$. The series continues until perhaps $Z_{k+1} = Z_k$, i.e., G/Z_k has trivial center.

Nilpotent groups are ones for which the upper central series reaches G in a finite number of steps (equivalently, the lower central series reaches $[\![1]\!]$ finitely). Nilpotent groups are solvable, and are products of p-groups with a free group (so products of nilpotent groups are nilpotent).

Torsion groups: every element has finite order. Products, subgroups, and images are also torsion groups.

p-**groups**: every element has order of type p^k for some fixed prime p. Products, subgroups, and images are also p-groups.

Higman: Every countable group is embedded in a 2-generated group.

3.5 Abelian Groups

when $xy = yx$. For example, the free abelian group on an alphabet A, isomorphic to $\mathbb{Z}^{(A)}$.

The direct product $G \times H$ is isomorphic to the free abelian product $(G \cup H)^*$. Morphisms can be multiplied together $\phi * \psi(x) = \phi(x)\psi(x)$ (the category is abelian and concrete (functor to groups), but not cartesian closed).

Inner automorphisms are trivial, but $x \mapsto x^{-1}$ is a non-trivial automorphism, unless $x^2 = 1$ for all x (but even in this case, there is the non-trivial automorphism $x \leftrightarrow y$, except for the groups C_1 and C_2).

A *divisible* group is an abelian group for which $x^n = a$ has a solution for every a and $n \in \mathbb{N}$; equivalently $G = \{\, x^n : x \in G \,\}$ for all n, or every morphism $H \subset K \to G$ can extend to a morphism $K \to G$. They are products of $\mathbb{Q}$ or $\mathbb{Z}(p_\infty) := \{\, z : z^{p^k} = 1 \,\}$, and every abelian group can be embedded in a divisible group.

The *dual* of an abelian group G is $G^* := \mathrm{Hom}(G, \mathbb{Z})$ (or $\mathrm{Hom}(G, \mathbb{Z}_n)$ if G has order n). Every morphism $\phi : G \to H$ gives rise to a morphism $\phi^\top : H^* \to G^*$, $\phi^\top(\psi)(x) := \psi \circ \phi(x)$.

(Prüfer) Every finitely generated abelian group is the finite product of cyclic groups. Every abelian m-group is the finite product of groups of form $\mathbb{Z}_r^{(n)}$.

3.6 Finite Groups

H is a subgroup of a finite group G, when it is closed under the operation (since $[\![x]\!]$ contains 1 and x^{-1}); each element has a finite order.

Proposition 4

Sylow's theorem

Let $|G| = p^m q^r \cdots$ (prime decomposition), then G has n subgroups of order p^m, such that $n|\,|G|$ and $n = 1 \pmod{p}$; all such *Sylow* p-subgroups S_p are conjugate to each other.

Every element of G can be written as a unique commuting product of elements in the Sylow subgroups.

Proof. Consider the G-action of translation on all subsets of G of size p^m. The stabilizers G_A of order p^m have orbits of size $s := |G|\,/\,|G_A| = q^r \cdots$; but $p \not| \binom{p^m s}{p^m} = ns + p\lambda$ (the class equation), so that $p \not| n$ and $n > 0$.

Now let P, Q be any two subgroups of order p^m; let P act on the cosets of Q by translation, and consider those l stabilizers that equal P, so that their orbit has size 1; this means that for some $g \in G$ and any $x \in P$, $xgQ = gQ$, i.e., $g^{-1}Pg = Q$; then the class equation is $s = l + p\lambda$ so $p \not| l$ and $l > 0$.

Let P act by conjugation on the n p-subgroups Q, k of which are fixed by all of P, $\forall x \in P, x^{-1}Qx = Q$, i.e., $P \leqslant N_G(Q)$; so $n = k + p\lambda$, so $p \not| n$ and $k > 0$; so P, Q are Sylow p-subgroups of $N_G(Q)$, hence conjugates; but $Q \trianglelefteq N_G(Q)$, so $P = Q$; so $n = 1 \pmod{p}$. Note $n = |G/N_G(P)|$.

Let G act by conjugation on the n p-subgroups Q. By the above, there is one orbit, so $n|\,|G|$.

The (maximal) Sylow p-subgroups S_p together contain every element of order p^i, and each has trivial intersection with an S_q. For any g, $o(g) = p_1^{m_1} \cdots p_k^{m_k}|\,|G|$; but

$$1 = r_1 \frac{o(g)}{p_1^{m_1}} + \cdots + r_k \frac{o(g)}{p_k^{m_k}}$$

so $g = g^{r_1 p_2^{m_2} \cdots p_k^{m_k}} \cdots g^{r_k p_1^{m_1} \cdots p_{k-1}^{m_{k-1}}} = x_1 \cdots x_k$, where each x_i has order $p_i^{m_i}$. If $g = x_1 x = y_1 y$ with $y_1^{m_1} = 1$, $x^m = y^m = 1$, then $x_1^m = (x_1 x)^m = (y_1 y)^m = y_1^m$, so $x_1 = x_1^{r_1 p_1^{m_1} + sm} = x_1^{sm} = y_1^{sm} = y_1$.

□

The Frattini subgroup of a finite group is nilpotent.

If, in a group G, every element is its own inverse, then G is abelian (since $xyxy = 1 = xxyy$).

Finite p-Groups:

1. The center contains an element $x \neq 1$ of some maximal order p^k, so $x, \ldots, x^{p^{k-1}}$ have orders $p^k, \ldots, p$; so G is nilpotent.

   Proof. $p^m = |G| = |Z| + \sum_{C(x)} |G| / |N_x|$, so $p|\,|Z|$. G/Z is again a p-group with non-trivial center.

2. G contains normal subgroups of order $1, p, p^2, \ldots, p^n$; the number of subgroups of order p^r is $n_r = 1 \pmod p$.

   Proof. There is an element x of order p in the center; so $G/[\![x]\!]$ has size p^{n-1}; by induction it has normal subgroups of order p^i, so their pullbacks have size p^{i+1}.

3. G is a finite p-group iff its size is p^n for some n (otherwise there is an element of order q).

4. G has at least one non-trivial outer automorphism.

5. When $|G| = p^2$, G is abelian.

   Proof. $|Z| = p \;\Rightarrow\; G/Z = [\![g]\!] \;\Rightarrow\; xy = g^i z_1 g^j z_2 = g^j z_2 g^i z_1 = yx$.

6. If $|G| = p^3$ with p an odd prime, then either G is abelian or it is isomorphic to one of:

   (a) $[\![a, b : 1 = a^{p^2} = b^p, ba = a^{1+p}b]\!]$

   (b) $[\![a, b, c : 1 = a^p = b^p = c^p, ba = ab, cb = bc, ca = abc]\!]$

7. If $|G| = p^4$ there are 15 different types (except $p = 2$, when there are 14 types). The classification of groups of size p^n for $n \geqslant 5$ depends on p.

8. Experimentally, almost all finite groups are 2-groups. Examples of families of 2-groups are

   (a) C_{2^n}, D_{2^n}, Q_{2^n},

   (b) $[\![a, b : a^{2^n} = 1, b^2 = 1, ba = a^{1+2^{n-1}}b]\!]$,

   (c) $[\![a^{2^n} = 1, b^2 = 1, ba = a^{-1+2^n}b]\!]$,

Proposition 5

Every abelian group is isomorphic to a direct product of cyclic groups.

Proof: The Sylow p-subgroups are unique and normal (in fact characteristic), generate G, and have trivial intersection, so G is their direct product.

Lemma: If $x_1, \ldots, x_n$ generate G then so do $x_1 x_2^r, x_2, \ldots, x_n$ ($r \in \mathbb{Z}$) since

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = (x_1 x_2^r)^{\alpha_1} x_2^{\alpha_2 - r\alpha_1} \cdots x_n^{\alpha_n}.$$

Among all sets of generators $x_1,\ldots,x_n$ of G pick one which has a relation $x_1^{m_1}\cdots x_k^{m_k}=1$ ($m_i\neq 0$) with the least possible value of $m:=\min_i|m_i|=m_1$ say. Let $m_i=q_im+r_i$, then

$$(x_1x_2^{q_2}\cdots x_k^{q_k})^m x_2^{r_2}\cdots x_k^{r_k}=1$$

so $r_i=0$ to avoid contradicting the minimality of m. Let $y:=x_1x_2^{q_2}\cdots x_k^{q_k}$, so that $y^m=1$ and $y,x_2,\ldots,x_n$ still generate G. If $z\in\llbracket y\rrbracket\cap\llbracket x_2,\ldots,x_n\rrbracket$ then $1=y^sx_2^{s_2}\cdots x_n^{s_n}$ (with $|s|<m$). This would contradict the minimality of m again unless $s=0$ and $z=y^{-s}=1$. Hence $G\cong\llbracket y\rrbracket\times\llbracket x_2,\ldots,x_n\rrbracket$, and the result follows by induction.

□

Other results:

1. (Frobenius) $\gcd(|G|,n)|\#\{\,g:g^n\in\llbracket a\rrbracket\,\}$; hence $n|\,|G|\;\Rightarrow\;n|\#\{\,g:g^n=1\,\}$.

   Proof. Let $|G|=p^\alpha m$ (coprime) and $n=p^\beta k$ with $k|m$. Let $F_i:=\{\,x\in G:x^i=1\,\}$, $N_i(y):=N(y)\cap F_i$. Every $a\in G$ can be written uniquely as $a=xy=yx$, $x^{p^\alpha}=1=y^m$, so $G=\bigcup_{y\in F_m}yN_{p^\alpha}(y)$. For each $y\in F_m$, either $y\in Z$ in which case $N_{p^\alpha}(y)=F_{p^\alpha}$ or $y\notin Z$ when $N(y)\subset G$; in this case $|N(y)|=p^\gamma c$; either $\gamma=\alpha$ when $p^\alpha|\,|N(y)|$ and $p^\alpha|\,|N_{p^\alpha}(y)|$ by induction, or $\gamma<\alpha$ when the conjugates of y group together to give (by induction)
   $$\frac{|G|}{|N(y)|}\,|N_{p^\alpha}(y)|=\frac{|G|}{p^\gamma c}\,|N_{p^\gamma}(y)|=\frac{|G|}{p^\gamma c}p^\gamma d$$
   In any case $|N_{p^\alpha}(y)|$ is a multiple of p^α. But $p^\alpha|\,|G|$, so $p^\alpha|\,|F_m\cap Z|\,|F_{p^\alpha}|$. But if $p|\,|F_m\cap Z|$ then there would be an element $y\neq 1$ of order p yet $y^m=1$, a contradiction. Hence $p^\alpha|\,|F_{p^\alpha}|$.

   The difference between F_{p^α} and $F_{p^{\alpha-1}}$ are those x of order p^α, of which there are a multiple of $\phi(p^\alpha)=p^{\alpha-1}(p-1)$. So $p^{\alpha-1}|\,\left|F_{p^{\alpha-1}}\right|$, and by downward induction $p^\beta|\,\left|F_{p^\beta}\right|$.

   Now $a^n=1\Leftrightarrow a=xy=yx$, $x^{p^\beta}=1=y^k$. Repeating as above, $F_n=\bigcup_{y\in F_k}yN_{p^\beta}(y)$, and $|N(y)|=p^\gamma c$; either $\gamma\geqslant\beta$ or $\gamma<\beta$; in either case $p^\beta|\,|F_n|$. Repeating for the other prime factors of n gives $n=p^\beta\cdots|\,|F_n|$.

2. Corollaries: If $|G|=mn$ with m, n co-prime, and $H\trianglelefteq G$ with $|H|=n$ then $\#\{\,g:g^n=1\,\}=n$. If $K\trianglelefteq H\trianglelefteq G$ and $|H|=mn$ co-prime and $|K|=n$ then $K\trianglelefteq G$.

3. If $|G|=mn\nmid n!$, and $|H|=m$ then G is not simple; e.g. $|G|=pq$, $|G|=p^2q^2$ are not simple (more generally, $|G|=p^mq^n$ are solvable). In particular, if G has a subgroup H with p cosets, p the smallest prime in $|G|$, then H is normal.

   Proof: If G acts faithfully by translation on the cosets of H, then $mn|n!$; so the kernel of the action is a non-trivial normal subgroup.

4. If $|G| = p$ (prime) then $G \cong C_p$.

   If $|G| = pq$ (distinct primes), then G is isomorphic to either $C_p \times C_q$ or to $[\![a, b : a^q = b^p = 1, ba = a^{-1}b]\!]$ (if $q|p-1$).

5. If $|G| < |H|^2, |K|^2$ where $K \trianglelefteq G$, then $H \cap K \neq [\![1]\!]$ (from $|HK| \,/\, |K| = |H| \,/\, |H \cap K|$)

6. Let ϕ be an automorphism; if $p|o(\phi)$ but $p \not| o(G)$ then ϕ must interchange some conjugacy classes.

7. The *order sequence* of a group is a list of the orders of the elements. The order sequence need not identify a group, e.g. Q and $C_4 \times C_4$ have the same order sequence $(1, 2^{(3)}, 4^{(12)})$.

8. (Feit-Thompson) Odd sized groups are solvable. This result led to the classification of non-abelian simple groups because these are not solvable, hence even, hence have elements of order 2, which limits the number of possibilities.

9. (Burnside) A finitely-generated group of order 1,2,3,4,6, is finite; but for large enough order, the group can be infinite. It is unknown if $[\![a, b : x^5 = 1]\!]$ is finite.

10. For an abelian group, $\prod G = \prod_{g \in G} g = \begin{cases} g_0 & \text{there is one element } g_0^2 = 1 \\ 1 & \text{there are more} \end{cases}$

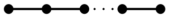
    (proof: Each g is paired with its inverse except for $g^2 = 1$; these form a subgroup and cancel each other out in threes or fours.)

3.7 Examples

Several group examples are special cases of *Coxeter* groups:

$$[\![a_1, \ldots, a_n : a_i^2 = 1, (a_i a_j)^{m_{ij}} = 1]\!]$$

($m_{ji} = m_{ij}$ since $(a_j a_i)^{m_{ij}+1} = a_j (a_i a_j)^{m_{ij}} a_i = a_j a_i$); so $m_{ij} = 2$ when a_i, a_j commute. The associated Coxeter diagram is a graph with each vertex representing a generator, and with $m_{ij} - 2$ edges joining a_i and a_j. Disconnected Coxeter diagrams correspond to the direct product of groups. (Geometrically, a_i represent reflections through n vectors (called roots) at angles of of π/m to each other.)

Symmetric groups: $S_n := S(n) = \mathcal{G}(n^n)$; of size $n!$; it is a Coxeter group with $n-1$ generators and $(a_i a_{i+1})^3 = 1$:  Every permutation can be written as a unique commuting product of cycles (= the orbits), and as a product of transpositions ($(ab \cdots c) = (ab) \cdots (ac)$), so a permutation may be odd or even depending on the number of transpositions. The conjugacy classes of S_n are characterized by the cycle structure, e.g. $2^2 3 4^3$; so are in 1-1 correspondence with the partitions of n. S_n is n-transitive. The number of permutations that move all objects $= n! - n(n-1)! + \binom{n}{2}(n-2)! + \cdots \approx n!/e$ by Sylvester's principle. S_n is complete, except S_6 (S_5 acts on its six Sylow 5-subgroups; it also acts on $1, \ldots, 5$; 'the' outer automorphism of S_6 interchanges these two,e.g. $(12) \leftrightarrow (16)(24)(35)$, $(123) \leftrightarrow (134)(256)$, $(1234) \leftrightarrow (1452)$). (Geometrically, they are the automorphism group of simplices (tetrahedra) and related lattice.)

The *alternating group* A_n consists of the even permutations, a normal subgroup of S_n (since it has two cosets), $A_n \trianglelefteq S_n < A_{n+2}$; for $n \geqslant 5$, A_n is simple. A_n is $(n-1)$-transitive. The conjugacy classes of A_n are the same as those of S_n, except that those that consist of only odd cycles split up into two classes of equal size. A_n has an outer automorphism given by $x \mapsto a^{-1}xa$ where a is an odd permutation.

(Proof that A_n is simple: The conjugacy classes of A_5 have sizes 1,15,20,24; no combination of these that includes the identity (1) divides 5!. If A_n is simple and $H \trianglelefteq A_{n+1}$, then H is transitive ($(1a)(2b)(12\cdots)(1a)(2b) = (ab\cdots)$) so $A_{n+1} = HA_n$ with $H \cap A_n = \{1\}$, so H has size n; thus H contains unique permutations $\sigma_i : 1 \mapsto i$; yet $(ab)\sigma_i(ab) \in H$ with $a, b \neq 1, i$ also maps $1 \mapsto i$ and is distinct.)

Cyclic groups: $C_n = [\![a : a^n = 1]\!]$; it is abelian of size n; has cyclic subgroups of any order $m|n$, $[\![a^{n/m}]\!]$. Cyclic groups of prime order are simple. $b = a^m$ is a generator of C_n iff m is coprime to n (since its order is $n/\gcd(m,n)$). Thus the morphisms of C_n are the maps $x \mapsto x^m$, and are automorphisms when m is coprime to n, $\mathrm{Aut}(C_n) = \Phi_n$.

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n, \qquad \text{when } m, n \text{ co-prime}$$

(Proof: The map $i \mapsto (i \pmod m, i \pmod n)$ is a morphism, 1-1 ($i = 0 \pmod m = 0 \pmod n \Rightarrow mn|i$), and onto, since to solve $i = p \pmod m = q \pmod n$, let $tm + sn = 1$, and take $i = psn + qtm \pmod{mn}$.)

Half the elements of C_{2n} are squares, and xy is a square iff both x, y are or both aren't squares.

The *multiplicative group* $\Phi_n := \mathcal{G}(\mathbb{Z}_n)$ (of size $\phi(n)$).

$$\begin{aligned} \Phi_{mn} &\cong \Phi_m \times \Phi_n \quad \text{if } m, n \text{ are coprime} \\ \Phi_{p^n} &\cong C_{p-1} \times C_{p^{n-1}},\ (p \neq 2) \quad \text{cyclic} \\ \Phi_{2^n} &\cong C_2 \times C_{2^{n-2}} \quad \text{except } \Phi_2 = C_1 \end{aligned}$$

Proof: $\mathcal{G}(\mathbb{Z}_{mn}) \cong \mathcal{G}(\mathbb{Z}_m) \times \mathcal{G}(\mathbb{Z}_n)$. For $p \neq 2$, the map $a \mapsto (a \mod p)$ is a morphism $\Phi_{p^n} \to \Phi_p$ with kernel H; but there is an element w with order $p-1$ which generates $K := \Phi_p \cong C_{p-1}$ and $H \cap K = 1$, $HK = KH$. For $p = 2$, Φ_{2^k} has 2^{k-1} elements, generated by -1 of order 2, and 3 of order 2^{k-2}.

So Φ_n is cyclic iff $n = 2, 4, p^n, 2p^n$ (p odd prime). And $\frac{\phi(n)}{n} = \prod_{p_i|n}(1 - \frac{1}{p_i})$ from formula for $\phi(mn)$. $\prod \Phi_n = \begin{cases} +1 & \Phi_n \text{ not cyclic or } n = 2 \\ -1 & \text{cyclic, except } n = 2 \end{cases}$, e.g. $(p-1)! = 1 \pmod p$.

Dihedral groups: $D_n := \llbracket a, b : a^n = 1, b^2 = 1, b^{-1}ab = a^{-1} \rrbracket$ (or $1 = a^2 = b^2 = (ab)^n$); they are Coxeter groups $\overset{n}{\bullet\!\!-\!\!\bullet}$ of size $2n$; the rotations $\llbracket a \rrbracket$ form a normal subgroup; the automorphisms are $a \mapsto a^m$, $b \mapsto a^r b$, $(\gcd(m,n) = 1$, so $n\phi(n)$ in all); of these the ones with $m = \pm 1$, $r = -2mi$, are the inner ones).

For n odd, the conjugacy classes are $\{ 1 \}$, $\{ a, a^{-1} \}, \ldots, \{ a^{(n-1)/2}, a^{(n+1)/2} \}$, $\{ b, ab, \ldots, a^{n-1}b \}$; the center is trivial.

For n even, the conjugacy classes are $\{ 1 \}$, $\{ a, a^{-1} \}, \ldots, \{ a^{n/2} \}$, $\{ b, a^2 b, \ldots, a^n b \}$, $\{ ab, a^3 b, \ldots, a^{n-1}b \}$; the center is $Z(G) = \{ 1, a^{n/2} \}$; there is an outer automorphism interchanging the two reflection classes; when m is odd, $D_{2m} \cong C_2 \times D_m$ $(= \llbracket a^m \rrbracket \times \llbracket a^2, b \rrbracket)$; the group of inner automorphisms is $D_{n/2}$ when n is even.

Quasi-dihedral groups: two versions, both of size $8n$,

$$SD_n := \llbracket a, b : a^{4n} = 1, b^2 = 1, ba = a^{2n-1}b \rrbracket$$
$$QD_n := \llbracket a, b : a^{4n} = 1, b^2 = 1, ba = a^{2n+1}b \rrbracket$$

Dicyclic groups: $\mathrm{Dic}_n := \llbracket a, b : a^{2n} = 1, b^2 = a^n, b^{-1}ab = a^{-1} \rrbracket$; so $b^i a^j = a^{\pm j} b^i$; of size $4n$; contains the normal subgroup $\llbracket a \rrbracket$; the center is $\{ 1, b^2 \}$, with image D_n. The *quaternion* groups Q_m are the special case when $n = 2^m$.

The *Heisenberg* groups: $H_n := \llbracket a, b : a^n = b^n = [a,b]^n = [a,[a,b]] = [b,[a,b]] = 1 \rrbracket$ (n odd prime); of size n^3.

The *wreathed* groups $W_n := \llbracket a, b, c : a^n = 1, b^n = 1, c^2 = 1, ba = ab, cb = ac, ca = bc \rrbracket$; have order $2n^2$.

The *Mathieu* groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}; M_{12} is generated by $(2074B6A8953)$ and $(10)(2B)(3A)(49)(58)(67)$; M_{24} is generated by a rotation $(2, 3 \cdots, 24)$ and the inversion
$(1,2)(3,24)(4,5)(6,23)(7,12)(8,9)(10,11)(13,22)(14,15)(16,21)(17,18)(19,20)$; it is the automorphism group of the Witt design. M_{11} and M_{23} are 4-transitive, M_{12} and M_{24} are 5-transitive; all are simple. Along with S_n and A_n, they are the only permutation groups which are more than 3-transitive.

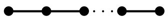
The number of finite monoids grows much faster than that of groups:

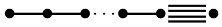
Size	Monoids	Comm. monoids	Groups	Comm. Groups
1	1	1	1	1
2	2	2	1	1
3	6	5	1	1
4	27	19	2	2
5	156	78	1	1
6	1373	421	2	1
7	17730	2637	1	1
8	858977		5	3

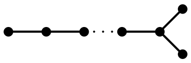
The first few groups up to size 20 are:

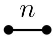
Size	Group	Comm./ Center	Conjugacy Classes Size and order	Alternative definition
1	C_1	-	1^1	S_1, A_1, A_2, Φ_2
2	C_2	-	$1^1 1^2$	S_2, D_1, Φ_3, Φ_4, Φ_6
3	C_3	-	$1^1 [2]^3$	A_3
4	C_4	-	$1^1 1^2 [2]^4$	D_2, Φ_5, Φ_{10}
	$C_2 \times C_2$	-	$1^1 [3]^2$	Φ_8, Φ_{12}
5	C_5	-	$1^1 [4]^5$	
6	C_6	-	$1^1 1^2 [2]^3 [2]^6$	Φ_7, Φ_9, Φ_{14}, Φ_{18}
	S_3	1	$1^1 3^2 2^3$	D_3
7	C_7	-	$1^1 [6]^7$	
8	C_8	-	$1^1 1^2 [2]^4 [4]^8$	
	$C_4 \times C_2$	-	$1^1 [3]^2 [4]^4$	SD_1, Φ_{15}, Φ_{16}, Φ_{30}
	$C_2 \times C_2 \times C_2$	-	$1^1 [7]^2$	Φ_{24}
	D_4	C_2	$1^1 1^2 2^2 2^2 2^4$	QD_1
	Q_1	C_2	$1^1 1^2 2^4 2^4 2^4$	Dic_2
9	C_9	-	$1^1 [2]^3 [6]^9$	
	$C_3 \times C_3$	-	$1^1 [8]^3$	
10	C_{10}	-	$1^1 1^2 [4]^5 [4]^{10}$	Φ_{11}, Φ_{20}, Φ_{22}
	D_5	1	$1^1 5^2 2^5 2^5$	
11	C_{11}	-	$1^1 [10]^{11}$	
12	C_{12}	-	$1^1 1^2 [2]^3 [2]^4 [2]^6 [4]^{12}$	Φ_{13}, Φ_{26}
	$C_2 \times C_2 \times C_3$	-	$1^1 [3]^2 [2]^3 [6]^6$	Φ_{21}, Φ_{28}, Φ_{36}, Φ_{42}
	D_6	C_2	$1^1 1^2 3^2 3^2 2^3 2^6$	
	A_4	1	$1^1 3^2 4^3 4^3$	$A_4' \cong C_2 \times C_2$
	Dic_3	C_2	$1^1 1^2 2^3 3^4 3^4 2^6$	
13	C_{13}	-	$1^1 [12]^{13}$	
14	C_{14}	-	$1^1 1^2 [6]^7 [6]^{14}$	
	D_7	1	$1^1 7^2 2^7 2^7 2^7$	
15	C_{15}	-	$1^1 [2]^3 [4]^5 [8]^{15}$	
16	C_{16}	-	$1^1 [3]^2 [2]^3 [6]^6$	Φ_{17}, Φ_{34}
	$C_8 \times C_2$	-	$1^1 [3]^2 [4]^4 [8]^8$	Φ_{32}
	$C_4 \times C_4$	-	$1^1 [3]^2 [12]^4$	
	$C_4 \times C_2 \times C_2$	-	$1^1 [7]^2 [8]^4$	Φ_{40}, Φ_{48}, Φ_{60}
	$C_2 \times C_2 \times C_2 \times C_2$	-	$1^1 [15]^2$	
	D_8	C_2	$1^1 1^2 4^2 4^2 2^4 2^8 2^8$	
	$D_4 \times C_2$	$C_2 \times C_2$	$1^1 1^2 1^2 1^2 2^2 2^2 2^2 2^2 2^4 2^4$	
	Q_2	C_2	$1^1 1^2 2^4 4^4 4^4 2^8 2^8$	Dic_4
	$Q_1 \times C_2$	$C_2 \times C_2$	$1^1 1^2 1^2 1^2 2^4 2^4 2^4 2^4 2^4 2^4$	
	SD_2	C_2	$1^1 1^2 2^4 4^2 4^4 2^8 2^8$	
	QD_2	C_4	$1^1 1^2 1^4 1^4 2^2 2^4 2^8 2^8 2^8 2^8$	
	$(C_2 \times C_2) \rtimes C_4$	$C_2 \times C_2$	$1^1 1^2 1^2 1^2 2^2 2^2 2^4 2^4 2^4 2^4$	$\llbracket a, b, c : a^4 = b^2 = c^2 = 1, ba = ab, cb = bc, ca = abc \rrbracket$
	$C_4 \rtimes C_4$	$C_2 \times C_2$	$1^1 1^2 1^2 1^2 2^4 2^4 2^4 2^4 2^4 2^4$	$\llbracket a, b : a^4 = b^4 = 1, ba = a^3 b \rrbracket$
	$D_4 \otimes C_4$	C_4	$1^1 1^2 2^2 2^2 2^2 1^4 1^4 2^4 2^4 2^4$	$\llbracket a, b, c : a^4 = b^2 = 1, c^2 = a^2, ba = a^3 b, ca = ac, cb = bc \rrbracket$
17	C_{17}	-	$1^1 [16]^{17}$	
18	C_{18}	-	$1^1 1^2 [2]^3 [2]^6 [6]^9 [6]^{18}$	Φ_{19}, Φ_{27}, Φ_{38}, Φ_{54}
	$C_3 \times C_3 \times C_2$	-	$1^1 [3]^2 [8]^3 [6]^6$	
	D_9	1	$1^1 2^3 2^9 2^9 2^9 9^2$	
	$S_3 \times C_3$	C_3	$1^1 3^2 3^2 3^2 1^3 1^3 2^3 2^3 2^3$	
	$(C_3 \times C_3) \rtimes C_2$	1	$1^1 3^2 1^3 1^3 2^3 2^3 2^3 3^6 3^6$	$\llbracket a, b, c : a^3 = b^3 = c^2 = 1, ba = ab, ca = a^2 c, cb = b^2 c \rrbracket$
19	C_{19}	-	$1^1 [18]^{19}$	
20	C_{20}	-	$1^1 1^2 [2]^4 [4]^5 [4]^{10} [8]^{20}$	Φ_{25}, Φ_{33}, Φ_{44}, Φ_{50}
	$C_5 \times C_2 \times C_2$	-	$1^1 [3]^2 [4]^5 [12]^{10}$	Φ_{66}
	D_{10}	C_2	$1^1 1^2 5^2 5^2 2^5 2^5 2^{10} 2^{10}$	
	Dic_5	C_2	$1^1 1^2 5^4 5^4 2^5 2^5 2^{10} 2^{10}$	
	GA(1,5)	1	$1^1 1^2 5^4 5^4 2^5 2^5 2^{10} 2^{10}$	$\llbracket a, b : a^5 = b^4 = 1, ba = a^2 b \rrbracket$

The finite Coxeter groups are:

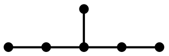
1. A_N with N generators 
   (automorphism group of simplices, size $(N+1)!$), i.e., the symmetric group S_{N+1}

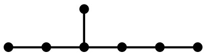
2. BC_N with N generators 
   (automorphism group of cubes and associated two lattices, size $2^N N!$),

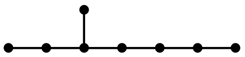
3. D_N with N generators 
   (automorphism group of a lattice, size $2^{N-1}N!$),

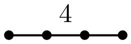
4. I_n 

   (automorphism groups of regular polygons, size $2n$), i.e., dihedral groups D_n

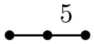
5. E_6 
   (automorphisms of a 6-D lattice, size 51840)

6. E_7 
   (automorphisms of a 7-D lattice, size 2903040)

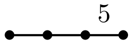
7. E_8 
   (automorphisms of an 8-D lattice, size 696729600)

8. F_4 

   (automorphism group of the 120-cell in $\mathbb{R}^4$, size 1152)

9. H_3 

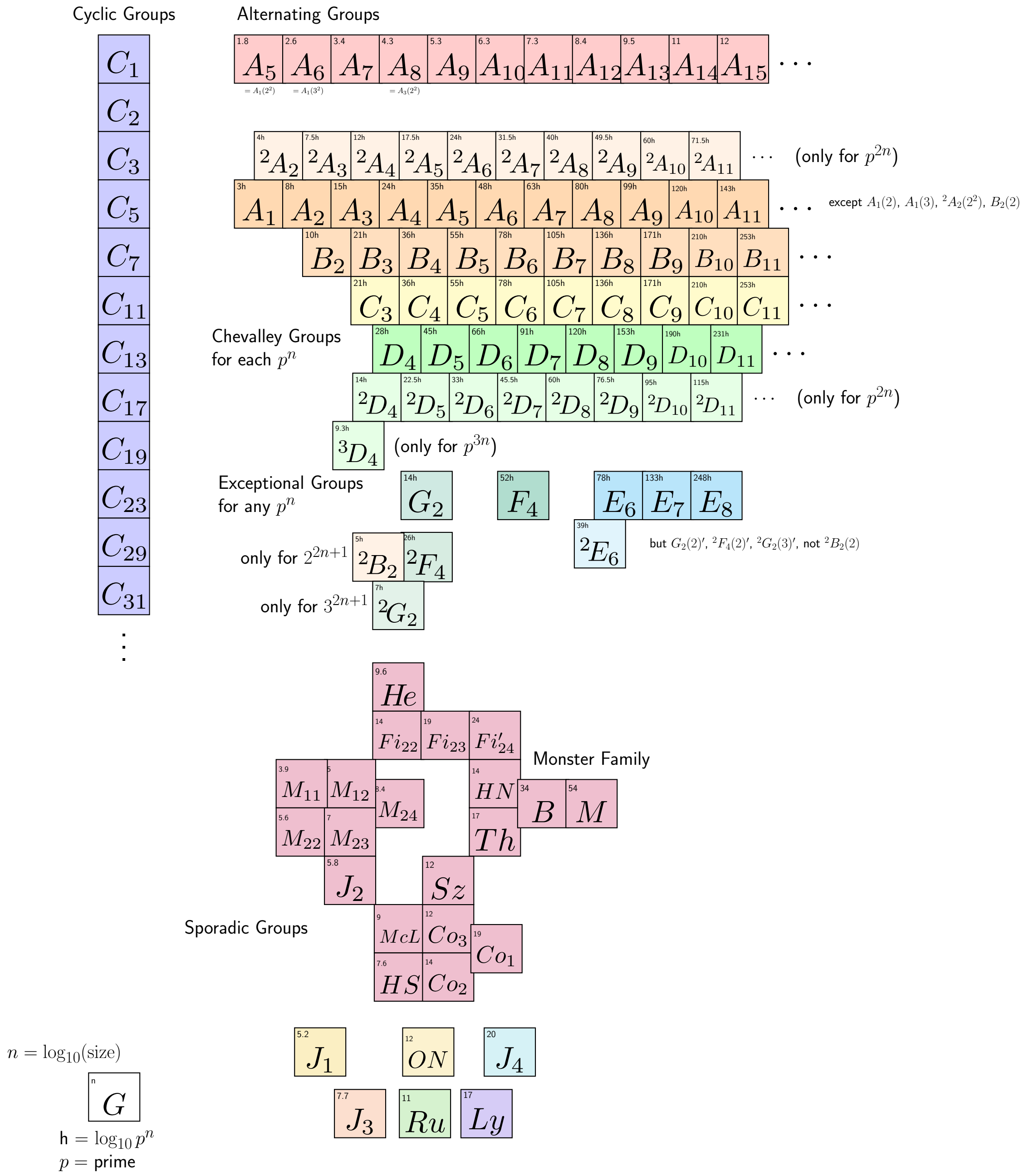
   (automorphism group of dodecahedron/icosahedron, size 120),

10. H_4 

    (automorphism group of the 120-vertex 'icosahedron' in $\mathbb{R}^4$, size 14400).

3.7.1 Finite Simple Groups

All the finite simple groups are known:


Cyclic Groups
C_1 C_2 C_3 C_5 C_7 C_{11} C_{13} C_{17} C_{19} C_{23} C_{29} C_{31} ⋮
Alternating Groups
1.8 A_5 2.6 A_6 3.4 A_7 4.3 A_8 5.3 A_9 6.3 A_{10} 7.3 A_{11} 8.4 A_{12} 9.5 A_{13} 11 A_{14} 12 A_{15} …
$= A_1(2^2)$ $= A_1(3^2)$ $= A_3(2^2)$
4h $^2A_2$ 7.5h $^2A_3$ 12h $^2A_4$ 17.5h $^2A_5$ 24h $^2A_6$ 31.5h $^2A_7$ 40h $^2A_8$ 49.5h $^2A_9$ 60h $^2A_{10}$ 71.5h $^2A_{11}$ … (only for p^{2n})
3h A_1 8h A_2 15h A_3 24h A_4 35h A_5 48h A_6 63h A_7 80h A_8 99h A_9 120h A_{10} 143h A_{11} … except $A_1(2)$, $A_1(3)$, $^2A_2(2^2)$, $B_2(2)$
10h B_2 21h B_3 36h B_4 55h B_5 78h B_6 105h B_7 136h B_8 171h B_9 210h B_{10} 253h B_{11} …
21h C_3 36h C_4 55h C_5 78h C_6 105h C_7 136h C_8 171h C_9 210h C_{10} 253h C_{11} …
Chevalley Groups for each p^n
28h D_4 45h D_5 66h D_6 91h D_7 120h D_8 153h D_9 190h D_{10} 231h D_{11} …
14h $^2D_4$ 22.5h $^2D_5$ 33h $^2D_6$ 45.5h $^2D_7$ 60h $^2D_8$ 76.5h $^2D_9$ 95h $^2D_{10}$ 115h $^2D_{11}$ … (only for p^{2n})
9.3h $^3D_4$ (only for p^{3n})
Exceptional Groups for any p^n
14h G_2 52h F_4 78h E_6 133h E_7 248h E_8
39h $^2E_6$
but $G_2(2)'$, $^2F_4(2)'$, $^2G_2(3)'$, not $^2B_2(2)$
only for 2^{2n+1} 5h $^2B_2$ 26h $^2F_4$
only for 3^{2n+1} 7h $^2G_2$
9.6 He
14 Fi_{22} 19 Fi_{23} 24 Fi'_{24}
Monster Family
3.9 M_{11} 5 M_{12} 8.4 M_{24} 14 HN 34 B 54 M
5.6 M_{22} 7 M_{23} 17 Th
5.8 J_2 12 Sz
Sporadic Groups
9 McL 12 Co_3 19 Co_1
7.6 HS 14 Co_2
5.2 J_1 12 ON 20 J_4
7.7 J_3 11 Ru 17 Ly
$n = \log_{10}(\text{size})$
n G
h $= \log_{10} p^n$
$p =$ prime

3.7.2 Countable Groups

$\mathbb{Z}$ has an infinite descending series $0 \leqslant \cdots 8\mathbb{Z} \leqslant 4\mathbb{Z} \leqslant 2\mathbb{Z} \leqslant \mathbb{Z}$. Its morphisms form the ring $\mathbb{Z}$.

$\mathbb{Q}$: its morphisms are $x \mapsto ax$ (since $\phi(m) = m\phi(1) = ma$, $n\phi(1/n) = a$, so $\phi(m/n) = (m/n)a$); thus $\mathrm{Hom}(\mathbb{Q})$ is isomorphic to $\mathbb{Q}$.

C_{p^∞}-group: $\{\, e^{2\pi i n/p^m} \,\} = [\![a_1, a_2, \ldots : a_1^p = e, a_2^p = a_1, \ldots]\!]$. It is the direct limit of C_{p^n}; it is divisible.

The **Artin** groups:

$$[\![a_1, \ldots, a_n : \underbrace{a_i a_j a_i \cdots a_{i/j}}_{m_{ij}} = \underbrace{a_j a_i a_j \cdots}_{m_{ij}}]\!]$$

There is a morphism from the Artin group with parameters m to the Coxeter group with the same parameters m, with kernel being a *pure Artin group*.

Braid groups $B_n(X)$: ways of mapping $n \to n$ on a surface X keeping track of over/under; multiplication by composition. The classical braid groups B_n are $B_n(\mathbb{R}^2) = [\![a_1, \ldots, a_{n-1} : a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1}, a_i a_j = a_j a_i]\!]$ (each a_i represents a transposition), e.g. $B_3 = [\![a, b : aba = bab]\!]$; they are the Artin groups with associated Coxeter group S_n. There is a normal form for elements (by "pulling the strings"). Contains the Brunnian braid subgroup of braids that have only one strand doing all the over/under twining; $B_n \subset B_{n+1}$; there is a morphism $B_n \to S_n$, $a_i \to (i\ i+1)$, with kernel being P_n, the subgroup of "pure" braids; and a morphism $B_n \to \mathbb{Z}$, $x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} \mapsto m_1 + m_2 + \cdots + m_k$. (The Braid group on an infinite number of vertices is uncountable.)