2. Groups: basic definitions and examples

2.1. Definition and first examples

Reading. [Moore, §3, pp. 10–27].

Definition 2.1 (Group)**.** A *group* is a quartet $(G, \mathbf{m}, \mathbf{I}, e)$ in which

group
群

1. G is a set;
2. $\mathbf{m} : G \times G \to G$ is a multiplication;
3. $\mathbf{I} : G \to G$ is an inversion;
4. $e \in G$ is the identity element,

subject to the following conditions.

(i) *Associativity.* $\mathbf{m}\big(\mathbf{m}(g_1, g_2), g_3\big) = \mathbf{m}\big(g_1, \mathbf{m}(g_2, g_3)\big)$ for all $g_1, g_2, g_3 \in G$, written $(g_1 g_2)g_3 = g_1(g_2 g_3)$.

(ii) *Identity.* $eg = ge = g$ for all $g \in G$.

(iii) *Inverse.* $g\,\mathbf{I}(g) = \mathbf{I}(g)\,g = e$ for all $g \in G$. We write $\mathbf{I}(g) =: g^{-1}$.

Associativity is a real restriction, not a formality. Two familiar operations fail it: the vector cross product, since $(\vec{a}\times\vec{b})\times\vec{c} \neq \vec{a}\times(\vec{b}\times\vec{c})$ in general, and multiplication of the *octonions*.

octonions
八元数

Remark 2.2 (Notation and weaker structures).

1. The identity is written e, 1, 1_G, or 0, depending on context.
2. Dropping axioms in turn gives weaker structures, the *semi-group* and the *monoid*. Addition serves for all three; only the set changes.

semi-group
半群

monoid
幺半群

$$\underset{\{1,2,3,\dots\}}{\text{semi-group}} \xrightarrow{\text{identity}} \underset{\{0,1,2,\dots\}}{\text{monoid}} \xrightarrow{\text{inverses}} \underset{\mathbb{Z}}{\text{group}}$$

no identity — no inverses — $-n$ inverts n

Each arrow names the axiom that is added. A monoid need not sit inside any group. Take the same set $\{0, 1, 2, \dots\}$ under multiplication instead of addition. It is a monoid with identity 1, but no group contains it, since $0 \cdot 2 = 0 \cdot 3$ while $2 \neq 3$, and in a group $ab = ac$ forces $b = c$ on multiplying by a^{-1}.

manifold
流形

3. If in addition G is a *manifold*, meaning a space that near every point looks like an open region of $\mathbb{R}^n$, and $\mathbf{m}$, $\mathbf{I}$ are real analytic in local coordinates, then G is a *Lie group*.

Lie group
李群

4. We abbreviate $(G, \mathbf{m}, \mathbf{I}, e)$ to G whenever the operation is clear from context. One set may carry several: $\mathbb{Z}$ is a group under addition but not under multiplication.

Quiz 2.1. Is e unique? Is g^{-1} unique?

Example 2.3 (Numbers under addition and multiplication). Take $\mathbf{m}(a, b) = a + b$. Then $G = \mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$ is a group, with $e = 0$ and $\mathbf{I}(a) = -a$.

Take instead $\mathbf{m}(a, b) = ab$. Now $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ and $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ are groups, but $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ is not, because integers other than ± 1 have no integer inverse.

2.2. Subgroups, order, and cyclic groups

subgroup
子群

Definition 2.4 (Subgroup)**.** Let $(G, \mathbf{m}, \mathbf{I}, e)$ be a group and $H \subset G$ a nonempty subset on which $\mathbf{m}$ and $\mathbf{I}$ are closed, i.e. $\mathbf{m} : H \times H \to H$, $\mathbf{I} : H \to H$. Then $(H, \mathbf{m}, \mathbf{I}, e)$ is a *subgroup* of G. If $H \neq G$ the subgroup is *proper*.

Lemma 2.5 (Subgroup criterion)**.** *A nonempty subset $H \subset G$ is a subgroup if and only if $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$.*

Proof. A subgroup satisfies the condition. Conversely, H is nonempty, so pick $h \in H$. Then $e = hh^{-1} \in H$, next $h^{-1} = eh^{-1} \in H$ for every $h \in H$, and finally $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. □

Example 2.6 (Subgroups).

1. Under addition, $\mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$ is a chain of subgroups.
2. Under multiplication $\mathbb{R}^* \subset \mathbb{C}^*$, whereas $\mathbb{Z}^* \not\subset \mathbb{R}^*$ as a subgroup.
3. $\mathbb{R}_{>0} \subset \mathbb{R}^*$ is a subgroup.

order
阶

---

finite
有限群

Quiz 2.2. Let H_1 and H_2 be subgroups of G. Is $H_1 \cap H_2$ a subgroup? Is $H_1 \cup H_2$?

infinite
无限群

Definition 2.7 (Order)**.** The *order* $|G|$ of a group is the cardinality of the set G. If $|G| < \infty$ the group is *finite*; otherwise it is *infinite*.

The *order of an element* $g \in G$ is the least positive integer n with $g^n = 1_G$, and is infinite if there is no such n.

the group of nth roots of unity
单位根群

Example 2.8 (The group of Nth roots of unity). Let

$$\mu_N = \{z \in \mathbb{C} \mid z^N = 1\}, \qquad \omega = \exp\Big(\frac{2\pi \mathrm{i}}{N}\Big),$$

so that $\mu_N = \{1, \omega, \dots, \omega^{N-1}\}$. Multiplication reads

$$\omega^i \, \omega^j = e^{\frac{2\pi \mathrm{i}}{N}(i+j \bmod N)} = \omega^k, \qquad k = i + j \bmod N,$$

so the group law on the exponents is addition modulo N. A group generated by a single element in this way is called *cyclic*.

cyclic
循环群

For $N = 4$, with $\omega_j = e^{\mathrm{i}\pi j/2}$, the element ω_1 has order 4 while ω_2 has order 2.

2.3. Equivalence relations and residue classes

Reading. [Moore, §2, pp. 6–10].

Definition 2.9 (Equivalence relation)**.** A binary relation $\sim$ on a set X is an *equivalence relation* if for all $a, b, c \in X$

equivalence relation
等价关系

(i) $a \sim a$ (reflexive)

(ii) $a \sim b \Leftrightarrow b \sim a$ (symmetric)

(iii) $a \sim b$ and $b \sim c \Rightarrow a \sim c$ (transitive)

The *equivalence class* of a is the subset

$$[a] := \{x \in X \mid x \sim a\} \subset X,$$

also written $\bar{a}$. We use the bar wherever it is unambiguous.

residue classes modulo n
剩余类

Example 2.10 (Residue classes modulo N). Write $N\mathbb{Z} := \{kN \mid k \in \mathbb{Z}\}$ for the multiples of N, and on $\mathbb{Z}$ declare

$$a \sim b \quad \text{whenever} \quad a - b \in N\mathbb{Z},$$

that is, whenever a and b differ by an integer multiple of N, equivalently whenever they leave the same remainder on division by N. The relation $\sim$ is an equivalence relation, and the class of j is

$$[\,j\,] \;=\; \bar{j} \;=\; \{j + kN \mid k \in \mathbb{Z}\}.$$

There are N of them, $\bar{0}, \bar{1}, \dots, \overline{N-1}$. Setting

$$\mathbf{m}(\bar{r}_1, \bar{r}_2) := \overline{r_1 + r_2}$$

makes them a group, written $\mathbb{Z}_N$ or $\mathbb{Z}/N\mathbb{Z}$. The second notation reads as $\mathbb{Z}$ divided by the subgroup $N\mathbb{Z}$, which is the quotient construction of Chapter 7.

For $N = 2$ the classes are $\bar{0}$, the even integers, and $\bar{1}$, the odd ones, with

$$\bar{0} + \bar{0} = \bar{0}, \qquad \bar{0} + \bar{1} = \bar{1}, \qquad \bar{1} + \bar{1} = \bar{0}.$$

Dropping the bars gives $\{0, 1\}$ under addition modulo 2. Relabelling instead $\bar{0} \mapsto 1$ and $\bar{1} \mapsto -1$ gives $\{1, -1\}$ under ordinary multiplication. All three are the same group.

2.4. Direct products and Abelian groups

direct product
直积

Definition 2.11 (Direct product)**.** Given groups G_1 and G_2, the *direct product* $G_1 \times G_2$ has elements (g_1, g_2) and multiplication

$$\mathbf{m}_{G_1 \times G_2}\big((g_1, g_2), (g_1', g_2')\big) := \big(\mathbf{m}_{G_1}(g_1, g_1'),\ \mathbf{m}_{G_2}(g_2, g_2')\big).$$

Its order is $|G_1| \cdot |G_2|$.

the klein four-group
克莱因四元群

Example 2.12 (The Klein four-group). Take $G_1 = G_2 = \mathbb{Z}_2 = \{1, -1\}$. Then $\mathbb{Z}_2 \times \mathbb{Z}_2$ has four elements

$$\mathbb{1} = (1, 1), \quad A = (-1, 1), \quad B = (1, -1), \quad C = (-1, -1),$$

Klein four-group
四元群

known as the Klein four-group V_4, or Vierergruppe.

Every example in this chapter so far satisfies $\mathbf{m}(a, b) = \mathbf{m}(b, a)$. That is a special property and deserves a name.

abelian group
阿贝尔群

Definition 2.13 (Abelian group)**.** G is *Abelian* if $ab = ba$ for all $a, b \in G$, and *non-Abelian* if there exist $a, b \in G$ with $ab \neq ba$. For Abelian groups one usually writes $\mathbf{m}(a, b)$ additively as $a + b$, with identity $e = 0$.

2.5. Matrix groups

Reading. [Moore, §3, pp. 10–27].

general linear group
一般线性群

Example 2.14 (General linear group). Let $M_n(\kappa)$ be the $n \times n$ matrices over a field κ (for us $\kappa = \mathbb{R}$ or $\mathbb{C}$). Then

$$GL(n, \kappa) := \{A \in M_n(\kappa) \mid \det A \neq 0\}$$

is a group under matrix multiplication. For $n \geq 2$ it is non-Abelian.

centre of a group
中心

Definition 2.15 (Centre of a group)**.** The *centre* of G is the set of elements that commute with everything,

$$Z(G) := \{z \in G \mid zg = gz \ \ \forall g \in G\} \subset G.$$

Proposition 2.16 (The centre is an Abelian subgroup)**.** *$Z(G)$ is a subgroup of G, and it is Abelian.*

Proof. By Definition 2.4 we must check that $Z(G)$ contains e and is closed under $\mathbf{m}$ and $\mathbf{I}$.

The identity. $eg = g = ge$ for every $g \in G$, so $e \in Z(G)$ and $Z(G)$ is not empty.

Closure under $\boldsymbol{m}$. Let $z_1, z_2 \in Z(G)$ and $g \in G$. Moving g past each factor in turn,

$$(z_1 z_2)g = z_1(z_2 g) = z_1(g z_2) = (z_1 g)z_2 = (g z_1)z_2 = g(z_1 z_2),$$

so $z_1 z_2 \in Z(G)$.

Closure under $\boldsymbol{I}$. Let $z \in Z(G)$ and $g \in G$. From $zg = gz$, multiply on both sides by z^{-1},

$$z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1} \quad \Longrightarrow \quad gz^{-1} = z^{-1}g,$$

so $z^{-1} \in Z(G)$. Hence $Z(G)$ is a subgroup.

Abelian. Let $z_1, z_2 \in Z(G)$. Since z_1 commutes with *every* element of G, and z_2 is in particular an element of G, we get $z_1 z_2 = z_2 z_1$. So any two elements of the centre commute, and $Z(G)$ is Abelian. □

For the general linear group the centre is as small as it can be.

Proposition 2.17 (Centre of the general linear group)**.**

$$Z\big(GL(n,\kappa)\big) = \{\, \lambda \mathbb{1}_n \mid \lambda \in \kappa^* \,\}.$$

Proof. A scalar matrix commutes with every matrix, which gives one inclusion.

For the other, let A commute with everything in $GL(n,\kappa)$, and let E_{ij} denote the matrix with a 1 in position (i,j) and zeros elsewhere. Since E_{ij} is not invertible it is not itself available here, but for $i \neq j$ the matrix $\mathbb{1} + E_{ij}$ is, and A commutes with it exactly when A commutes with E_{ij}. Comparing entries,

$$(AE_{ij})_{kl} = A_{ki}\,\delta_{jl}, \qquad (E_{ij}A)_{kl} = \delta_{ki}\,A_{jl},$$

so $A_{ki}\,\delta_{jl} = \delta_{ki}\,A_{jl}$ for all k, l. Putting $k = i$ and $l = j$ gives $A_{ii} = A_{jj}$, so every diagonal entry is the same. Putting $l = j$ with $k \neq i$ gives $A_{ki} = 0$, so every off-diagonal entry vanishes. Hence $A = \lambda\mathbb{1}$, with $\lambda \neq 0$ since A is invertible. □

The standard matrix groups are the subgroups of $GL(n,\kappa)$ that preserve some structure.

1. **Special linear group**

   special linear group
   特殊线性群

   $$SL(n,\kappa) = \{A \in GL(n,\kappa) \mid \det A = 1\}.$$

2. **Orthogonal and special orthogonal**

   orthogonal group
   正交群

   $$O(n,\kappa) = \{A \in GL(n,\kappa) \mid AA^T = \mathbb{1}\}, \qquad SO(n,\kappa) = \{A \in O(n,\kappa) \mid \det A = 1\}.$$

   From $AA^T = \mathbb{1}$ we get $(\det A)^2 = 1$, hence $\det A = \pm 1$. In particular A is invertible, and multiplying $AA^T = \mathbb{1}$ on the left by A^{-1} gives $A^T = A^{-1}$, so

$A^T A = \mathbb{1}$ as well. The two conditions say the same thing and either serves as the definition. This is the general fact that a one-sided inverse of a square matrix is automatically two-sided.

unitary group
酉群

3. **Unitary and special unitary**

$$U(n) := \{A \in GL(n,\mathbb{C}) \mid AA^\dagger = \mathbb{1}\}, \qquad SU(n) = \{A \in U(n) \mid \det A = 1\}.$$

Here $(\det A)(\det A)^* = 1$, so $|\det A| = 1$ and $\det A = e^{i\theta}$. Again A is invertible, so $A^\dagger = A^{-1}$ and $A^\dagger A = \mathbb{1}$ holds equally.

indefinite orthogonal group
不定正交群

4. **Indefinite orthogonal group**

$$O(p,q) := \{A \in GL(p+q,\mathbb{R}) \mid A^T J_{p,q} A = J_{p,q}\}, \qquad J_{p,q} = \begin{pmatrix} -\mathbb{1}_p & 0 \\ 0 & \mathbb{1}_q \end{pmatrix}.$$

The Minkowski case is $J_{1,3} = \mathrm{diag}(-1,1,1,1)$, giving $O(1,3)$, the Lorentz group. Write a spacetime point as $x = (t, \vec{r}\,)$ in units with $c = 1$, where $\vec{r}$ is the spatial position. The quantity preserved is the spacetime interval

$$x^T J_{1,3}\, x = -t^2 + \vec{r}\cdot\vec{r},$$

so $O(1,3)$ consists of the linear coordinate changes that leave it unchanged.

proper time
固有时

For a timelike separation the interval is negative, and the *proper time* τ between the two events is

$$\tau^2 = t^2 - \vec{r}\cdot\vec{r},$$

the time recorded by a clock moving inertially between them.

symplectic group
辛群

5. **Symplectic group**

$$Sp(2n,\kappa) = \{A \in GL(2n,\kappa) \mid A^T J A = J\}, \qquad J = \begin{pmatrix} 0 & \mathbb{1}_n \\ -\mathbb{1}_n & 0 \end{pmatrix},$$

which is the structure preserved by canonical transformations in classical mechanics.

The last two conditions can also be written the other way round. Taking determinants in $A^T J A = J$ gives $(\det A)^2 = 1$, so A is invertible and $A^T = JA^{-1}J^{-1}$. Both forms square to a multiple of the identity, $J_{p,q}^2 = \mathbb{1}$ and $J^2 = -\mathbb{1}$ for the symplectic J, so J^2 commutes with A^{-1} and

$$AJA^T = AJ^2A^{-1}J^{-1} = J^2AA^{-1}J^{-1} = J^2J^{-1} = J.$$

Proposition 2.18 (Determinant of a symplectic matrix)**.** *Every $A \in Sp(2n,\kappa)$ has* $\det A = 1$.

Proof. From $A^T J A = J$ one gets $(\det A)^2 = 1$, hence $\det A = \pm 1$. To rule out -1, use the *Pfaffian* $\mathrm{Pf}(M)$, a polynomial in the entries of an antisymmetric $2n \times 2n$ matrix M ($M^T = -M$) with the two properties

Pfaffian
普法夫值

$$\mathrm{Pf}(M)^2 = \det M, \qquad \mathrm{Pf}(B^T M B) = \det(B)\ \mathrm{Pf}(M)$$

for any $2n\times 2n$ matrix B. Our J is antisymmetric with $\det J = 1$, so the first gives $\mathrm{Pf}(J)^2 = 1$ and in particular $\mathrm{Pf}(J) \neq 0$. Putting $M = J$ and $B = A$ in the second, and using $A^T J A = J$,

$$\mathrm{Pf}(J) = \mathrm{Pf}(A^T J A) = \det(A)\ \mathrm{Pf}(J).$$

Dividing by $\mathrm{Pf}(J)$ leaves $\det A = 1$. □

Example 2.19 ($SO(2,\mathbb{R})$ and $U(1)$). A matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $AA^T = \mathbb{1}$ and $\det A = 1$ has the form $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ with $a^2 + b^2 = 1$, so

$$R(\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} = e^{-\phi J}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and $R(\phi_1)R(\phi_2) = R(\phi_1 + \phi_2)$.

Meanwhile $U(1)$ consists of $z(\phi) = e^{\mathrm{i}\phi}$ with $z(\phi_1)z(\phi_2) = z(\phi_1 + \phi_2)$. The two group laws are identical, and

$$SO(2) \ \cong\ U(1) \ \sim\ S^1,$$

where $\cong$ means the same group and $\sim$ the same space. Here S^n denotes the unit sphere in $\mathbb{R}^{n+1}$, a surface of dimension n, so S^1 is the circle in the plane. The correspondence is $R(\phi) = e^{-\phi J} \leftrightarrow e^{\mathrm{i}\phi}$. Here and throughout, $SO(n)$ abbreviates $SO(n,\mathbb{R})$, the case that describes rotations of Euclidean space; any other field is written out.

Example 2.20 ($SU(2)$ and the three-sphere). A general element of $SU(2)$ takes the form

$$g = \begin{pmatrix} z & -w^* \\ w & z^* \end{pmatrix}, \qquad |z|^2 + |w|^2 = 1.$$

Writing $z = x_0 + \mathrm{i}x_1$ and $w = x_2 + \mathrm{i}x_3$ the constraint becomes $\sum_{i=0}^{3} x_i^2 = 1$, which is the unit sphere in $\mathbb{R}^4$, so

$$SU(2) \ \sim\ S^3.$$

Key points

- $GL(n,\kappa)$ is the ambient group; every other matrix group here is the subgroup preserving some structure —a determinant, a metric, or a symplectic form.
- $SO(2) \cong U(1) \sim S^1$ and $SU(2) \sim S^3$: matrix groups carry a geometry, which is what makes them Lie groups.
- $O(1,3)$ is the Lorentz group; $Sp(2n,\mathbb{R})$ is the group of linear canonical transformations. The abstract definitions are not abstract in practice.

Key terms. general linear group 一般线性群 · special linear group 特殊线性群 · orthogonal group 正交群 · unitary group 酉群 · symplectic group 辛群 · centre 中心

2.6. Generators and presentations

Reading. [Moore, §10, pp. 191–199].

Definition 2.21 (Generated subgroup)**.** If X is a subset of G, the smallest subgroup of G containing X is denoted $\langle X \rangle$ and is called the *subgroup generated by* X; equivalently, X *generates* $\langle X \rangle$.

If $G = \langle X \rangle$ with $|X| < \infty$, the group is *finitely generated*. The condition is on the generating set, not on the group. The integers under addition are generated by the single element 1,

$$\mathbb{Z} = \langle 1 \rangle,$$

so $\mathbb{Z}$ is finitely generated although it is infinite.

group presentation
群展示

Definition 2.22 (Group presentation)**.** A *presentation* of G is an expression

$$G = \langle\, g_1, \dots, g_n \mid R_1, \dots, R_r \,\rangle,$$

in which the *generators* $g_1, \dots, g_n$ generate G, and the *defining relations* $R_1, \dots, R_r$ are equations among them from which every other relation follows. Equations that merely happen to hold are not enough. A generator of $\mathbb{Z}_2$ satisfies $a^4 = 1$, but $\langle a \mid a^4 = 1 \rangle$ is $\mathbb{Z}_4$.

For instance

$$\mu_N = \langle\, \omega = e^{2\pi \mathrm{i}/N} \,\rangle = \langle\, \omega \mid \omega^N = 1 \,\rangle.$$

By convention the identity is not listed among the generators.

Why presentations? Because they are efficient: every finite group has a generating set of at most $\log_2 |G|$ elements.

Put $H_0 = \{e\}$. While $H_j \neq G$, choose $g \in G \setminus H_j$ and set $H_{j+1} = \langle H_j, g \rangle$. The sets H_j and $H_j g$ are disjoint, since $h_1 = h_2 g$ would give $g = h_2^{-1} h_1 \in H_j$, and both lie in H_{j+1}. Multiplication by g is a bijection between them, so $\left|H_{j+1}\right| \geq 2\left|H_j\right|$. After ℓ choices $2^\ell \leq |G|$, and the chosen elements generate G, so $\ell \leq \log_2 |G|$.

Example 2.23 (The Klein four-group, presented). With $A = (-1, 1)$, $B = (1, -1)$, $C = (-1, -1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$ we have $A^2 = B^2 = \mathbb{1}$ and $C = AB$, so

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle\, A, B \mid A^2 = B^2 = (AB)^2 = 1 \,\rangle.$$

Quiz 2.3. None of the three relations above can be spared. Show that dropping any one of them leaves an infinite group, so that all three are needed to pin down V_4.

dihedral group
二面体群

Example 2.24 (Dihedral group).

$$D_n := \langle\, A, B \mid A^n = B^2 = (AB)^2 = 1 \,\rangle,$$

the symmetry group of the regular n-gon: A is a rotation and B a reflection. Note $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 2.25 (Quaternion group). The quaternion units satisfy

quaternion group
四元数群

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j,$$

giving the eight-element group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ with presentation

$$Q = \langle\, a, b \mid a^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1} \,\rangle = \langle i, j \rangle.$$

The quaternion units can be written with the *Pauli matrices*

$$\sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma^2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \qquad \sigma^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

Pauli matrices
泡利矩阵

which are Hermitian, traceless, and square to the identity. They satisfy

$$\sigma^i \sigma^j = \delta^{ij}\mathbb{1} + \mathrm{i}\,\epsilon^{ijk}\sigma^k.$$

For any two operators A and B the *commutator* and the *anticommutator* are

$$[A, B] := AB - BA, \qquad \{A, B\} := AB + BA.$$

The first vanishes exactly when $AB = BA$, the second exactly when $AB = -BA$. Antisymmetrising and symmetrising the product rule above in i and j gives

commutator
对易子

anticommutator
反对易子

$$[\sigma^i, \sigma^j] = 2\mathrm{i}\,\epsilon^{ijk}\sigma^k, \qquad \{\sigma^i, \sigma^j\} = 2\delta^{ij}\mathbb{1},$$

so two distinct Pauli matrices always anticommute. In quantum mechanics the spin-$\tfrac{1}{2}$ operators are $S^i = \tfrac{\hbar}{2}\sigma^i$.

Setting $i = -\mathrm{i}\sigma^1$, $j = -\mathrm{i}\sigma^2$ and $k = -\mathrm{i}\sigma^3$ reproduces the quaternion relations, so $Q = \langle -\mathrm{i}\sigma^1, -\mathrm{i}\sigma^2 \rangle \subset SU(2)$.

Quiz 2.4. What is $Z(Q)$?

Remark 2.26 (Two senses of "generator"). The matrices $-\mathrm{i}\sigma^1$ and $-\mathrm{i}\sigma^2$ have just appeared as generators of Q in the sense of this section, every element of Q being a finite product of them and their inverses. In quantum mechanics the Pauli matrices are called the generators of $SU(2)$, and that is a different use of the word. They are not elements of $SU(2)$, since $\det \sigma^k = -1$. They are the matrices standing in the exponent,

$$U = \exp\!\Big(-\tfrac{\mathrm{i}}{2}\,\theta_k\,\sigma^k\Big) \in SU(2),$$

and strictly it is $\mathrm{i}\sigma^k$, not σ^k, that lies in the Lie algebra of $SU(2)$, the traceless anti-Hermitian matrices.

A finite generating set yields only countably many finite products, while $SU(2)$ is uncountable. So $SU(2)$ is not finitely generated in the sense of this section.

2.7. Application: the Pauli group and stabilizer codes

Reading. [NC, §10.5]. Toric code: [Kitaev].

qubit
量子比特

A *qubit* is a two-dimensional complex vector space with basis $|0\rangle = \binom{1}{0}$, $|1\rangle = \binom{0}{1}$. The Pauli matrices acting on it carry standard names $X = \sigma^1$, $Y = \sigma^2$, $Z = \sigma^3$, of which two are used constantly:

$$X|0\rangle = |1\rangle\,, \quad X|1\rangle = |0\rangle \qquad \text{(bit flip, NOT)},$$

$$Z|0\rangle = |0\rangle\,, \quad Z|1\rangle = -|1\rangle \qquad \text{(phase flip)}.$$

Pauli group
泡利群

The single-qubit *Pauli group* is

$$P_1 = \{\pm 1, \pm \mathrm{i}, \pm X, \pm Y, \pm Z, \pm \mathrm{i}X, \pm \mathrm{i}Y, \pm \mathrm{i}Z\} = \langle X, Y, Z\rangle,$$

sixteen elements, closed under multiplication by $\sigma^i\sigma^j = \delta^{ij}\mathbb{1} + \mathrm{i}\epsilon^{ijk}\sigma^k$. The phase enters through $XYZ = \mathrm{i}\mathbb{1}$. For n qubits,

$$P_n = \{\, \mathrm{i}^k A_1 \otimes \cdots \otimes A_n \;:\; k \in \{0,1,2,3\},\ A_j \in \{\mathbb{1}, X, Y, Z\}\,\},$$

where the tensor product is the operator acting on each qubit separately, $(A_1 \otimes \cdots \otimes A_n)|b_1 \cdots b_n\rangle = (A_1|b_1\rangle) \otimes \cdots \otimes (A_n|b_n\rangle)$. There are 4^{n+1} elements, the four phases times the 4^n strings, because the phases of the separate factors collapse into one overall phase.

stabilizer code
稳定子码

Definition 2.27 (Stabilizer code)**.** Let $S \subset P_n$ be an *Abelian* subgroup not containing $-\mathbb{1}$. The associated *code space* is

$$\mathscr{C} = \{|\psi\rangle \,:\, g|\psi\rangle = |\psi\rangle \quad \forall g \in S\},$$

the simultaneous $+1$ eigenspace of every element of S.

Both conditions on S matter. Commuting operators can be diagonalised simultaneously, so the constraints $g|\psi\rangle = |\psi\rangle$ can be imposed together; and $-\mathbb{1}|\psi\rangle = |\psi\rangle$ has no nonzero solution, so a subgroup containing $-\mathbb{1}$ would leave $\mathscr{C} = 0$.

quantum error correction
量子纠错

The construction is for . A qubit in contact with its surroundings does not always stay where it was put, and the disturbances it suffers are built from the Pauli operators, a bit flip X_i or a phase flip Z_i on one of the qubits. One qubit of information is therefore stored in several physical ones, spread out so that the likely disturbances can be spotted and undone.

The group does the spotting. Every element of S is Hermitian and squares to $\mathbb{1}$, so it is an observable with eigenvalues ± 1, and on a state of $\mathscr{C}$ it reads $+1$. Suppose an error $E \in P_n$ has occurred. Any two elements of P_n either commute or anticommute, so for each generator g of S,

$$g\big(E|\psi\rangle\big) = \pm\, E\, g|\psi\rangle = \pm\, E|\psi\rangle\,,$$

the sign being $+$ when g and E commute and $-$ when they anticommute. Measuring the generators therefore returns a list of signs, the *error syndrome* of E. It depends on E and not on $|\psi\rangle$, so the measurement gives information about the error without revealing what was stored.

error syndrome
伴随式

Example 2.28 (The three-qubit code). Take

$$S = \langle\, Z_1Z_2,\ Z_2Z_3 \,\rangle \subset P_3,$$

where Z_1Z_2 is short for $Z\otimes Z\otimes \mathbb{1}$ and Z_2Z_3 for $\mathbb{1}\otimes Z\otimes Z$. Both generators square to $\mathbb{1}$, they commute, and their product is Z_1Z_3, so the group has four elements,

$$S = \{\, \mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1},\quad Z\otimes Z\otimes\mathbb{1},\quad \mathbb{1}\otimes Z\otimes Z,\quad Z\otimes\mathbb{1}\otimes Z \,\},$$

and $S \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, the Klein four-group of Example 2.23.

On a basis state $|b_1b_2b_3\rangle$ with $b_i \in \{0,1\}$ the operator Z_iZ_j has eigenvalue $+1$ if $b_i = b_j$ and -1 otherwise. The two stabilizer conditions say that the first two bits agree and the last two agree, which leaves $|000\rangle$ and $|111\rangle$, so

$$\mathscr{C} = \operatorname{span}\{|000\rangle, |111\rangle\}.$$

One qubit of information sits in three, with $|000\rangle$ and $|111\rangle$ in the roles of $|0\rangle$ and $|1\rangle$.

Now store a state $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ of $\mathscr{C}$ and let one qubit be flipped. Since X and Z anticommute while X and $\mathbb{1}$ commute, X_1 anticommutes with Z_1Z_2 and commutes with Z_2Z_3, and similarly for X_2 and X_3. The syndromes are

Error	Z_1Z_2	Z_2Z_3
none	$+1$	$+1$
X_1	-1	$+1$
X_2	-1	-1
X_3	$+1$	-1

all four different, so the measurement says which qubit was flipped and applying X to that qubit restores $|\psi\rangle$. What Z_iZ_j measures is whether qubits i and j agree, which is a comparison and not a reading.

An ideal measurement of either stabilizer generator leaves its eigenstates unchanged. Here $|000\rangle$ and $|111\rangle$ carry the same eigenvalue under Z_1Z_2, and the same under Z_2Z_3, so $\alpha|000\rangle + \beta|111\rangle$ is an eigenstate of both whatever α and β are. The outcome is certain and the state is left alone. After an error the same holds, since $X_i|000\rangle$ and $X_i|111\rangle$ again share a syndrome. The measurement separates the four error sectors and cannot see inside any of them, which is exactly why α and β survive it.

Remark 2.29 (What the code does not correct). A phase flip produces no syndrome. Z_1 commutes with both generators, so the measurement returns $(+1,+1)$, the same answer as for an undisturbed state. Yet $Z_1 \notin S$ and the stored state has changed,

$$Z_1\big(\alpha|000\rangle + \beta|111\rangle\big) = \alpha|000\rangle - \beta|111\rangle,$$

a phase flip of the stored qubit. The same holds for Z_2 and Z_3.

The cost is not only that these errors go uncorrected. If each of the three physical qubits independently picks up a phase flip with probability p, the stored qubit picks one up whenever an odd number of them do, with probability

$$3p(1-p)^2 + p^3,$$

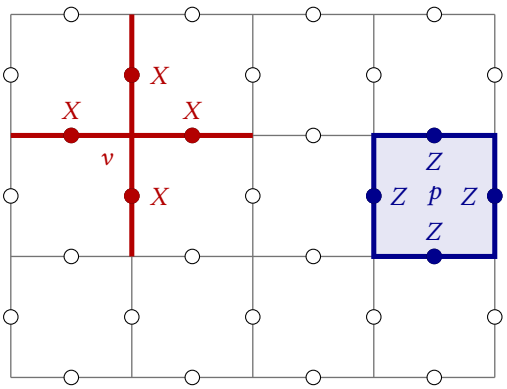
which is about $3p$ for small p. Bit flips are suppressed from p to about $3p^2$, and phase flips are made three times more likely. The benefit therefore depends on the relative rates of bit and phase flips.

Correcting an arbitrary error on one physical qubit takes more qubits. Shor's nine-qubit code does it by nesting a three-qubit code against bit flips inside a three-qubit code against phase flips, and five is the smallest number of qubits for which any such code exists.

Example 2.30 (Toric code). Kitaev's toric code puts the same construction on a lattice. Take a square lattice on a torus, meaning a square grid whose left edge is identified with its right and whose top is identified with its bottom, and place one qubit on every edge. For each vertex v and each face p set

$$A_v = \prod_{e \ni v} X_e, \qquad B_p = \prod_{e \in \partial p} Z_e,$$

the products running over the four edges meeting at v and over the four edges bounding p.



All of these operators commute. Two stars commute, both being products of X, and two faces commute, both being products of Z. A star and a face share either no edge or exactly two, and on a shared edge X and Z anticommute, so in the second case the two sign changes cancel and $A_v B_p = B_p A_v$. Hence $S = \langle A_v,\, B_p \rangle$ is an Abelian subgroup of P_n, where n is the number of edges, and the toric code is a stabilizer code in the sense of Definition 2.27.

Commuting operators have a common eigenbasis, so a state can be labelled by the eigenvalues of every A_v and every B_p at once. Each of these is ± 1, so

$$H = -\sum_v A_v - \sum_p B_p$$

is lowest on the states where all of them read +1, and the ground space of H is exactly the code space $\mathscr{C}$.

That ground space is four-dimensional, and the four belongs to the torus rather than to the lattice. The two independent ways round the torus each carry a binary label, so the ground states fall into four sectors labelled by $\mathbb{Z}_2 \times \mathbb{Z}_2$. On a sphere the ground state would instead be unique, and on a surface with g handles there would be 4^g of them. This is the meeting point of quantum information, topology, and strongly correlated physics, and it is as far as this course goes. For the excitations and their statistics, and for a treatment written for physics undergraduates, see Simon's lecture notes [Simon, chs. 24–25].

Quiz 2.5. Show that $\prod_v A_v = \mathbb{1}$ and $\prod_p B_p = \mathbb{1}$, the products running over every vertex and every face of the lattice on the torus. The generators are therefore not independent.

Key points

- $\langle X \rangle$ is the smallest subgroup containing X; a presentation names generators together with their defining relations.
- Every finite group has a generating set of at most $\log_2 |G|$ elements.
- D_n, V_4, Q and P_1 are the small finite groups this course keeps returning to.

Key terms. generator 生成元 · presentation 群展示 · dihedral group 二面体群 · quaternion group 四元数群 · Pauli group 泡利群 · stabilizer code 稳定子码

References for this chapter

[NC] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. 10th Anniversary. Cambridge: Cambridge University Press, 2010.

[Kitaev] A. Y. Kitaev. "Fault-tolerant quantum computation by anyons". In: *Annals of Physics* 303 (2003), p. 2. arXiv: `quant-ph/9707021`.

[Simon] S. H. Simon. *Topological Quantum. Lecture Notes and Proto-Book*. Chapters 24–25; published as *Topological Quantum*, Oxford University Press, 2023. 2021. URL: `https://www-thphys.physics.ox.ac.uk/people/SteveSimon/topological2021/TopoBook-Sep28-2021.pdf` (visited on 09/08/2026).