

# Chapter 1

## Group theory

I assume you already know some group theory.

### 1.1 Some reminders

**Assumed knowledge:** The definitions of a group, group homomorphism, subgroup, left and right coset, normal subgroup, quotient group, kernel of a homomorphism, center, cyclic group, order of an element, symmetric group, cycle decomposition, transposition, even/odd permutation, alternating group, Lagrange's Theorem, Isomorphism theorems relating to a homomorphism  $f : G \rightarrow H$ , etc.

If  $N$  is a normal subgroup of a group  $G$  there is a bijection between the subgroups of  $G$  containing  $N$  and the subgroups of  $G/N$ . If  $H$  is a subgroup of  $G$  containing  $N$  the corresponding subgroup of  $G/N$  is  $H/N$ ; furthermore,  $H$  is normal in  $G$  if and only if  $H/N$  is normal in  $G/N$ ; and in that case,  $G/H \cong (G/N)/(H/N)$ .

For the most part I will write groups multiplicatively—thus, the product of two elements will be denoted by juxtaposition,  $gh$ . Sometimes if the group is abelian it makes sense to write the group operation additively as we usually do with the integers—the sum is denoted by  $g + h$ . Sometimes it is not clear which notation is best. For example, the binary operation in the cyclic group of order  $n$ ,  $\mathbb{Z}_n$ , is best written as  $+$  when we are thinking of  $\mathbb{Z}_n$  as a quotient of the integers or when we think of  $\mathbb{Z}_n$  as a ring.

The  $n^{\text{th}}$  roots of unity in  $\mathbb{C}$  form a group under multiplication and we denote this group by  $\mu_n$ . Although  $\mu_n$  is abelian we write its group operation multiplicatively. If we choose a primitive  $n^{\text{th}}$  root of unity, say  $\varepsilon$ , there is a group isomorphism  $\mathbb{Z}_n \rightarrow \mu_n$  given by  $a \mapsto \varepsilon^a$ . Sometimes we will simply write  $\{\pm 1\}$  for the group  $\mathbb{Z}_2$ .

Most of the time when we deal with a group we do not know whether or assume that it is abelian so it makes sense to write it multiplicatively.

The direct product of two groups  $G$  and  $H$  is denoted by  $G \times H$  and is defined to be the cartesian product with group operation

$$(g, h) \cdot (g', h') := (gg', hh').$$

It is easy to check that this is a group.

If  $G$  and  $H$  are abelian we often call their direct product the **direct sum** and denote it by  $G \oplus H$ . The reason for this is that  $G$  and  $H$  are  $\mathbb{Z}$ -modules with the action given by  $n \cdot g = g^n$ .

**Example 1.1.** *There is an isomorphism  $(\mathbb{R}^+, \cdot) \times \mathbb{R}/\mathbb{Z} \rightarrow (\mathbb{C}^*, \cdot)$ ,  $(r, [\theta + \mathbb{Z}]) \mapsto re^{2\pi i\theta}$ . If you prefer, there is an isomorphism  $(\mathbb{R}^+, \cdot) \times \mathbb{R}/2\pi\mathbb{Z} \rightarrow (\mathbb{C}^*, \cdot)$ ,  $(r, [\theta + 2\pi\mathbb{Z}]) \mapsto re^{i\theta}$ .*  $\diamond$

The **automorphism group** of a group  $G$  consists of all group isomorphisms  $\psi : G \rightarrow G$  and is denoted  $\text{Aut } G$ . It is obviously a group under composition. Sometimes if  $\sigma \in \text{Aut } G$  it is common to write  $g^\sigma$  for  $\sigma(g)$ . The danger in doing this is that  $g^{\sigma\tau} = (g^\tau)^\sigma$ ! The notation  $g^\sigma$  should not seem too odd because it is what we do already in some situations: consider the circle group

$$U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$$

of complex numbers of absolute value one under multiplication and the automorphism sending each  $z$  to its inverse  $z^{-1}$ . Thus  $\text{Aut } U(1)$  has a subgroup isomorphic to  $\mathbb{Z}_2$  that we usually denote by  $\{\pm 1\}$  and the action of the automorphism  $-1$  is denoted by  $z \mapsto z^{-1}$  rather than  $(-1)(z)$ !

The circle group is often denoted  $U(1)$  because it is the first in the family of unitary groups which are denoted  $U(n)$ ,  $n \geq 1$ .

But do be wary that with these conventions  $g^{\sigma\tau} = (g^\tau)^\sigma$ !

**Proposition 1.2.** *If  $p$  is a prime, then  $\text{Aut}_{\text{gp}}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ .*

**Proof.** Let's write  $\mathbb{Z}_p$  multiplicatively by identifying it with  $\mu_p$ , the set of  $p^{\text{th}}$  roots of unity in  $\mathbb{C}^\times$ .

If  $1 \leq i \leq p-1$ , the map  $\theta_i : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  defined by  $\theta_i(\varepsilon^j) = \varepsilon^{ij}$  is a group homomorphism. Because the only subgroups of  $\mathbb{Z}_p$  are itself and the trivial subgroup,  $\theta_i$  is both injective and surjective. Thus each  $\theta_i$  belongs to  $\text{Aut } \mathbb{Z}_p$ .

Now define  $\phi : \mathbb{F}_p^\times \rightarrow \text{Aut } \mathbb{Z}_p$  from the multiplicative group of non-zero elements of  $\mathbb{F}_p$  by

$$\phi(\bar{i}) := \theta_i.$$

Here  $i$  is an integer and  $\bar{i}$  is its image in  $\mathbb{Z}/(p) = \mathbb{F}_p$ . Since

$$\left( \phi(\bar{i}) \circ \phi(\bar{j}) \right) (\varepsilon) = (\varepsilon^i)^j = \varepsilon^{ij} = \phi(\overline{ij})(\varepsilon),$$

$\phi$  is a group homomorphism. We already know that  $\mathbb{F}_p^\times \cong \mathbb{Z}_{p-1}$ , so it remains to show that  $\phi$  is an isomorphism.

If  $\theta \in \text{Aut } \mathbb{Z}_p$  then  $\theta$  is completely determined by its action on a generator, say  $\zeta \in \mu_p$ . If  $\theta(\zeta) = \zeta^k$ , then

$$\theta(\zeta^r) = \theta(\zeta)^r = (\zeta^k)^r = (\zeta^r)^k = \theta_k(\zeta^r)$$

so  $\theta = \theta_k$ . Hence  $\phi$  is surjective.

If  $\theta_i = \text{id}$ , then  $\varepsilon^i = \varepsilon$  for all  $\varepsilon \in \mu_p$ , so  $\varepsilon^{i-1} = 1$  and  $p$  must divide  $i - 1$ . Hence,  $i = 1$  and we conclude that  $\phi$  is injective.  $\square$

## 1.2 Semi-direct products

Suppose that  $\varphi : H \rightarrow \text{Aut } N$  is a group homomorphism. We define the semi-direct product

$$N \rtimes_{\varphi} H$$

to be the Cartesian product  $N \times H$  with multiplication

$$(x, a) \cdot (y, b) = (xy^{\varphi(a)}, ab)$$

for  $x, y \in N$  and  $a, b \in H$ . It is a little burdensome to carry the  $\varphi$  notation everywhere so we often suppress it and write

$$N \rtimes H$$

and

$$(x, a) \cdot (y, b) = (xy^a, ab). \quad (2-1)$$

One should check that this product is associative:

$$((x, a) \cdot (y, b)) \cdot (z, c) = (xy^a, ab) \cdot (z, c) = (xy^a z^{ab}, abc)$$

and

$$(x, a) \cdot ((y, b) \cdot (z, c)) = (x, a) \cdot (yz^b, bc) = (x(yz^b)^a, abc) = (xy^a(z^b)^a, abc)$$

and this equal to the other product because  $(z^b)^a = z^{ab}$ . Because  $N \rtimes H$  contains copies of both  $N$  and  $H$  as subgroups, namely  $\{(x, 1) \mid x \in N\}$  and  $\{(1, a) \mid a \in H\}$ , it is common to identify  $N$  and  $H$  with those subgroups. Thus we say that  $N$  and  $H$  are subgroups of  $N \rtimes H$ . It then makes sense to simply write the elements of  $N \rtimes H$  as  $xa$  with  $x \in N$  and  $a \in H$ . Notice that  $ax = x^a a$ . The mnemonic I use to remember the multiplication rule (??) is that elements of  $N \rtimes H$  like to be written as  $xa$  with the  $H$ -piece  $a$  on the right, but if I find an element  $ax$  with  $a \in H$  and  $x \in N$ , when I move the  $a$  to the right it twists the  $x$  as it moves past it— $ax = x^a a$ .

Notice that if  $a \in H \equiv (1, H) \subset N \rtimes H$ , then  $N$  is stable under conjugation by  $a \equiv (1, a)$ , and  $ana^{-1} = \varphi(a)(n)$  for all  $n \in N$ .

**Example 2.1** (The dihedral groups). *Let  $N$  be a cyclic group generated by  $\tau$ . Let  $s \in \text{Aut } N$  be the automorphism of order two defined by  $s(\tau) = \tau^{-1}$ . Let  $H = \{1, \sigma\} \cong \mathbb{Z}_2$  and let  $\phi : H \rightarrow \text{Aut } N$  be given by  $\phi(\sigma) = s$ . Then the semi-direct product  $N \rtimes H$  is isomorphic to the dihedral group*

$$D = \langle \tau, \sigma \mid \sigma^2 = 1, \sigma\tau\sigma = \tau^{-1}, \tau^n = 1 \rangle.$$

*This includes the infinite dihedral group which occurs when  $n = \infty$ , i.e.,  $N \cong \mathbb{Z}$ .*  
 $\diamond$

If  $H$  is a subgroup of  $\text{Aut } N$ , we may form  $N \rtimes H$ .

It is possible for the groups  $N \rtimes_{\phi} H$  and  $N \rtimes_{\psi} H$  to be isomorphic even if  $\phi$  and  $\psi$  are different homomorphisms.

**Proposition 2.2.** *Let  $\phi : H \rightarrow \text{Aut } N$  be a group homomorphism and  $\beta \in \text{Aut } H$ . Then  $N \rtimes_{\phi} H \cong N \rtimes_{\phi\beta} H$ .*

**Proof.** Define

$$\Phi : N \rtimes_{\phi\beta} H \cong N \rtimes_{\phi} H$$

by

$$\Phi(x, a) := (x, \beta(a)).$$

This is obviously a bijective map from  $N \times H$  to itself. Also

$$\begin{aligned} \Phi\left((x, a)(y, b)\right) &= \Phi\left((x\phi\beta(a)(y), ab)\right) \\ &= \left(x\phi\beta(a)(y), \beta(ab)\right) \\ &= (x, \beta(a))(y, \beta(b)) \\ &= \Phi\left((x, a)\right)\Phi\left((y, b)\right) \end{aligned}$$

so  $\Phi$  is a group homomorphism.  $\square$

**Example 2.3.** *View elements of  $V = \mathbb{Z}_n \oplus \mathbb{Z}_n$  as column vectors forming a group under addition. Then  $\text{GL}(2, \mathbb{Z}_n)$  the group of invertible  $2 \times 2$  matrices with entries in the ring  $\mathbb{Z}_n$  acts on  $V$  by left multiplication. Let define  $\phi : \mathbb{Z}_n \rightarrow \text{GL}(2, \mathbb{Z}_n)$  be the map*

$$\phi(c) = \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix}.$$

*Thus, with our notation above,  $\mathbb{Z}_n$  acts on  $V$  by  $(a, b)^a := (a, b - ac)$ . The associated semidirect product  $G = V \rtimes \mathbb{Z}_n$  is isomorphic to the group of unipotent upper triangular matrices via the map*

$$(a, b, c) \mapsto \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

*This is an example of a discrete Heisenberg group.*  $\diamond$

**Example 2.4.** Let  $H$  and  $Z$  be abelian groups in which the group operations are written additively and multiplicatively respectively. Suppose that  $\psi : H \times H \rightarrow Z$  is a function. Then the following two conditions are equivalent:

1.  $\psi(0, 0) = 1$  and  $\psi(a, b)\psi(a + b, c) = \psi(a, b + c)\psi(b, c)$  for all  $a, b, c \in H$ ;
2.  $G = Z \times H$  is a group under the operation

$$(w, a) \cdot (z, b) = (wz\psi(a, b), a + b).$$

Suppose these conditions are satisfied. Then there is an “exact” sequence  $1 \rightarrow Z \rightarrow G \rightarrow H \rightarrow 1$  given by  $z \mapsto (z, 0)$  and  $(z, a) \mapsto a$ .

Let  $U_n$  denote the group of units in  $\mathbb{Z}_n$ , and set  $Z = \mathbb{Z}_n$ . Consider the ring of  $2 \times 2$  matrices over  $\mathbb{Z}_n$  and take the multiplicative Let  $G$  be the subgroup of the additive group of  $2 \times 2$  matrices over  $\mathbb{Z}_n$  consisting of the elements

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in U_n, b \in \mathbb{Z}_n \right\}.$$

Then  $G$  is isomorphic to the group constructed above with  $H = U_n \times U_n$  and  $Z = \mathbb{Z}_n$ .  $\diamond$

**Groups of order 8.** The abelian ones are  $\mathbb{Z}_8$ ,  $\mathbb{Z}_4 \times \mathbb{Z}_2$ , and  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ . The non-abelian ones are  $D_4$ , the dihedral group that is the symmetry group of the square, and  $Q = \{\pm 1, \pm i, \pm j, \pm k\}$  the quaternion group sitting inside Hamilton’s ring of quaternions  $\mathbb{H}$ . Recall that  $\mathbb{H}$  is the 4-dimensional  $\mathbb{R}$ -vectorspace with basis  $1, i, j, k$  made into a ring via the multiplication rules

$$i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ij = k, jk = i, ki = j.$$

Let’s write

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle.$$

Thus  $D_4 = \{1, \tau, \sigma^i, \sigma^i\tau \mid 1 \leq i \leq 3\}$ . The groups look similar: the center of  $D_4$  is  $\{1, \sigma^2\}$  and the center of  $Q$  is  $\{\pm 1\}$ , and the two groups have conjugacy classes of the same sizes:

$$\begin{aligned} D_4 : & \quad \{1\}, \{\sigma^2\}, \{\sigma, \sigma^{-1}\}, \{\tau, \sigma^2\tau\}, \{\sigma\tau, \sigma^3\tau\} \\ Q : & \quad \{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\} \end{aligned}$$

We saw above that  $D_4$  is a semidirect product  $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$ . Although  $N = \langle i \rangle$  is a normal cyclic subgroup of  $Q$  of order 4,  $Q$  is *not* a semidirect product  $N \rtimes H$  because the elements not in  $N$ , namely  $\pm j, \pm k$ , all have order 4. This (more or less) shows that  $Q$  is not isomorphic to  $D_4$  because it cannot be written as a semi-direct product  $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$ .

**Proposition 2.5.** Let  $G$  be a group containing a normal subgroup  $N$  and a subgroup  $H$  such that  $N \cap H = \{1\}$  and  $G = NH$ . Then  $G \cong N \rtimes_\phi H$  where  $\phi : H \rightarrow \text{Aut } N$  is given by  $\phi(h)(n) := hnh^{-1}$ .

**Proof.** To see that  $\phi$  is a group homomorphism:  $\phi(a)\phi(b)(n) = a(bnb^{-1})a^{-1} = \phi(ab)(n)$ .  $\square$

### 1.3 The symmetric group

**Definition 3.1.** The  $n^{\text{th}}$  symmetric group, denoted  $S_n$ , is the group of all permutations of  $\{1, 2, \dots, n\}$ .  $\diamond$

We always think of elements of  $S_n$  as acting on  $\{1, 2, \dots, n\}$ .

Let  $\sigma \in S_n$ . The orbit of  $i \in \{1, 2, \dots, n\}$  under the action of  $\sigma \in S_n$  is  $\{i, \sigma(i), \sigma^2(i), \dots\}$ . Obviously  $\{1, 2, \dots, n\}$  is the disjoint union of its orbits under  $\sigma$ .

**Notation.** If  $\sigma, \tau \in S_n$ , the product  $\sigma\tau$  means first do  $\tau$ , then do  $\sigma$ . Thus, we think of permutations as acting on  $\{1, 2, \dots, n\}$  from the left. Not all books adopt this convention (e.g., P.M. Cohn's book uses the opposite convention). The permutation  $\sigma \in S_9$  defined by

$$\begin{aligned}\sigma(1) &= 1, \sigma(2) = 5, \sigma(3) = 7, \sigma(4) = 8, \sigma(5) = 2, \\ \sigma(6) &= 4, \sigma(7) = 6, \sigma(8) = 9, \sigma(9) = 3,\end{aligned}$$

is denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 8 & 2 & 4 & 6 & 9 & 3 \end{pmatrix}.$$

We adopt the notation

$$(abc \dots z) := \begin{pmatrix} abc \dots z \\ bc \dots za \end{pmatrix}.$$

A permutation of this form is called a *cycle*. With our convention that  $\sigma\tau$  means first do  $\tau$  then  $\sigma$ , we have  $(12)(23) = (123)$ . For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 8 & 2 & 4 & 6 & 9 & 3 \end{pmatrix} = (25)(3764893).$$

Two cycles  $\sigma$  and  $\tau$  are *disjoint* if they can be written as  $\sigma = (abc \dots z)$  and  $\tau = (a'b'c' \dots z')$  with  $\{a, b, c, \dots, z\} \cap \{a', b', c', \dots, z'\} = \emptyset$ . Disjoint cycles commute with each other. The **length** of the cycle  $(abc \dots z)$  is the cardinality of  $\{a, b, c, \dots, z\}$ . A cycle of length  $k$  is called a  $k$ -cycle. A 2-cycle is called a *transposition*.

**Lemma 3.2.** Every element of  $S_n$  can be written as a product of disjoint cycles in a unique way up to order.

**Proof.** Let  $\sigma \in S_n$ . Write  $\{1, 2, \dots, n\}$  as the disjoint union of its  $\sigma$ -orbits, say  $O_1 \cup \dots \cup O_m$ . Let  $\tau_i$  be the cycle that is the identity on all  $O_j$  other than  $O_i$  and acts on  $O_i$  as does  $\sigma$ : thus, if  $a \in O_i$ , then  $\tau_i = (a \sigma(a), \sigma^2(a) \dots)$ . Then  $\sigma = \tau_1 \dots \tau_m$ .  $\square$

**Lemma 3.3.** Every permutation can be written as a product of transpositions.

**Proof.** Every cycle is a product of transpositions because, for example,  $(1\ 2\ \dots\ m-1\ m) = (1\ m)(1\ m-1)\cdots(1\ 3)(1\ 2)$ . But every permutation is a product of cycles, so the result follows.  $\square$

The Lemma can be read as saying that  $S_n$  is generated by transpositions. However, one can be efficient and generate it with just  $n-1$  transpositions. Show that  $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle$ .

**Partitions.** A partition of a positive integer  $n$  is a collection of positive integers  $n_1, \dots, n_k$  such that  $n_1 + \dots + n_k = n$ . The order of the integers is not important. It is often convenient to denote a partition by writing, for example,  $(1^3 2^3 5)$  to denote the partition  $1, 1, 1, 2, 3, 3, 5$  of 16. Each element of  $S_n$  determines a partition of  $n$  by taking the size of its orbits.

**Lemma 3.4.** *Two elements of  $S_n$  are conjugate if and only if they determine the same partition of  $n$ ; that is, if and only if they have orbits of the same size.*

**Proof.** Suppose that  $\sigma$  and  $\tau$  yield the same partition of  $n$ . Then, we can write  $\{1, \dots, n\}$  as a disjoint union in two ways, say

$$\{1, \dots, n\} = A_1 \sqcup \dots \sqcup A_r = B_1 \sqcup \dots \sqcup B_r,$$

where  $|A_i| = |B_i|$  for all  $i$ , and the elements of each  $A_i$  (resp., each  $B_i$ ) consist of a single  $\sigma$ -orbit (resp.,  $\tau$ -orbit). Fix elements  $a_i \in A_i$  and  $b_i \in B_i$  for all  $i$ . It is obvious that there is an element  $\eta \in S_n$  such that  $\eta(A_i) = B_i$  for all  $i$ , and even more precisely  $\eta(\sigma^j(a_i)) = \tau^j(b_i)$  for all  $i$  and  $j$ . In particular,  $\eta(a_i) = b_i$ , so  $\tau = \eta\sigma\eta^{-1}$ .

The converse is obvious.  $\square$

The bijection between conjugacy classes and partitions is fundamental to the analysis of the symmetric group.

**Example 3.5.** *The conjugacy classes in  $S_5$  are as follows:*

| Partition     | Element in the conjugacy class | Size of conjugacy class |
|---------------|--------------------------------|-------------------------|
| 5             | (12345)                        | 24                      |
| 1, 4          | (1234)                         | 30                      |
| 2, 3          | (12)(345)                      | 20                      |
| 1, 1, 3       | (123)                          | 20                      |
| 1, 2, 2       | (12)(34)                       | 15                      |
| 1, 1, 1, 2    | (12)                           | 10                      |
| 1, 1, 1, 1, 1 | 1                              | 1.                      |

We will use this list to find the normal subgroups of  $S_5$  in Proposition 3.8.  $\diamond$

The next result is useful for recognizing when a subgroup of the symmetric group is actually the whole group. We will use it when show that certain polynomials do not have a solution in radicals (see ???).

**Proposition 3.6.**  *$S_n$  is generated by  $(12)$  and  $(12\cdots n)$ .*

**Proof.** Let  $H$  be the subgroup generated by  $a = (12)$  and  $b = (12 \cdots n)$ . Then  $H$  contains  $bab^{-1} = (23)$  and hence, by induction,  $(ii+1)$  for all  $i$ . Thus  $H$  contains  $(12)(23)(12) = (13)$  and  $(13)(34)(13) = (14)$ , and so on. That is,  $(1i) \in H$  for all  $i$ . Hence, if  $i \neq j$ ,  $H$  contains  $(1i)(1j)(1i) = (ij)$ . Since every element of  $S_n$  is a product of transpositions we conclude that  $H = S_n$ , as claimed.  $\square$

**Lemma 3.7.** *If  $\sigma$  is written as a product of transpositions in two different ways, say  $\sigma = \alpha_1 \cdots \alpha_m = \beta_1 \cdots \beta_r$ , then  $m \equiv r \pmod{2}$ .*

A permutation is **even** if it is a product of an even number of transpositions, and is **odd** if it is a product of an odd number of transpositions. The previous lemma ensures that this definition is unambiguous. The set of even permutations form a subgroup of  $S_n$  called the **alternating group** and denoted by  $A_n$ .

There is a well-defined group homomorphism

$$\text{sgn} : S_n \rightarrow \{\pm 1\}$$

defined by

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}.$$

The kernel of this homomorphism is obvious  $A_n$ . Hence  $A_n$  is a normal subgroup of  $S_n$  of index 2.

We now use the list of conjugacy classes in Example 3.5 to find the normal subgroups of  $S_5$ .

**Proposition 3.8.** *The only normal subgroups of  $S_5$  are  $A_5$ ,  $S_5$ , and  $\{1\}$ .*

**Proof.** Let  $H$  be a normal subgroup that is neither  $S_5$  nor  $\{1\}$ . Since  $gHg^{-1} \subset H$  for every  $g \in S_5$ ,  $H$  is a union of conjugacy classes. The conjugacy classes have sizes 1, 10, 15, 20, 24, and 30. The class of size one must belong to  $H$  because it consists of the identity element.

The order of  $H$  is a divisor of  $|S_5| = 120$ . Since 120 is not divisible by  $1+10$ , or  $1+15$ , or  $1+20$ , or  $1+24$ , or  $1+10+15$ , or  $1+30$ , the only possibilities for  $|H|$  are  $40 = 1+15+24$  and  $60 = 1+15+24+20$ .

If  $|H| = 40 = 24+15+1$ , then  $H$  contains every 5-cycle, so contains  $(12345)$ , and contains every element corresponding to the partition  $1, 2, 2$ , so contains  $(12)(34)$ . Hence  $H$  contains their product  $(135)$ . Since  $(135)$  has order 3,  $|H| \neq 40$ .

Thus  $|H| = 60$  and  $H$  contains the conjugacy classes of  $(12345)$ ,  $(12)(34)$ , and  $(135)$ . But the union of these conjugacy classes is  $A_5$ . Hence  $H = A_5$ .  $\square$

**Lemma 3.9.**  *$A_n$  is generated by  $(123), (124), \dots, (12n)$ .*

**Proof.** By its very definition  $A_n$  is generated by the elements  $(ab)(cd) = (cad)(abc)$  and  $(ac)(ab) = (abc)$ . So it suffices to show that each  $(abc)$  belongs to the subgroup generated by  $\{(12m) \mid 3 \leq m \leq n\}$ . If  $\{b, c\} \cap \{1, 2\} = \emptyset$ , then

$(1bc) = (12c)^{-1}(12b)(12c)$  and  $(2bc) = (12b)(12c)(12b)^{-1}$ . If  $\{a, b, c\} \cap \{1, 2\} = \emptyset$ , then  $(abc) = (12a)(2bc)(12a)^{-1}$ . The result now follows.  $\square$

**Proposition 3.10.** *If  $n \geq 5$ , then  $A_n$  is a simple group.*

**Proof.** Let  $H$  be a non-trivial normal subgroup of  $A_5$ .

Suppose that  $H$  contains a 3-cycle, say  $(123)$ . If  $i \notin \{1, 2, 3\}$ , then  $H$  contains  $(12)(3i)(123)(3i)(12) = (1i2)$  and its square  $(12i)$ . It now follows from Lemma 3.9 that  $H = A_n$ .

Choose  $1 \neq \alpha \in H$  fixing as many elements of  $\{1, \dots, n\}$  as possible. Since  $\alpha$  is even it is not a transposition. Write  $\alpha$  as a product of disjoint cycles.

Suppose that only 2-cycles occur in the cycle decomposition of  $\alpha$ . Suppose first that  $\alpha = (12)(34) \cdots$ . If  $\alpha = (12)(34)$ , then  $H$  contains  $(543)\alpha(543)^{-1}\alpha^{-1} = (345)$ . If  $\alpha \neq (12)(34)$ , then  $\alpha = (12)(34)(56)(78) \cdots$ . Hence  $H$  contains  $(543)\alpha(543)^{-1}\alpha^{-1} = (36)(45)$  and applying the previous argument to  $(36)(45)$  in place of  $(12)(34)$  we see that  $H$  contains a 3-cycle.

If  $\alpha$  moves just 3 elements then it must be a 3-cycle.

We may now assume that the cycle decomposition for  $\alpha$  contains a  $d$ -cycle with  $d \geq 3$ , say  $\alpha = (123 \cdots) \cdots$ . If  $\alpha$  moves exactly four elements, then it must be  $(123i)$ ; but this is not even, so  $\alpha$  moves at least 5 elements, say  $1, 2, 3, 4, 5$ . Since  $H$  is normal it contains  $\beta = (543)\alpha(543)^{-1}$ , and hence  $\beta\alpha^{-1}$ . Notice that  $(543)\alpha$  sends 2 to 5 and  $\alpha(543)$  sends 2 to 3, so  $\beta\alpha^{-1} \neq 1$ . Now  $\beta\alpha^{-1}$  fixes every element that  $\alpha$  fixes, and also fixes 2; so  $\beta\alpha^{-1}$  fixes more elements than  $\alpha$ . This contradicts our choice of  $\alpha$ .  $\square$

**Exercise.** Show that  $S_3 \cong \text{GL}_2(\mathbb{F}_2)$ .

## 1.4 Actions

Often a group acts as permutations of a set.

This is typically how groups arise: as certain kinds of permutations of a set with structure, and the group consists of permutations that preserve the structure. This is roughly what we mean when we speak of a symmetry group.

We will exploit this perspective in this section.

A permutation of a set  $X$  is a bijective map  $X \rightarrow X$ . The set  $S(X)$  of all permutations of  $X$  is a group under composition of maps. If  $X$  has  $n$  elements we call the set of all permutations of  $X$  the **symmetric group** on  $n$  letters, and denote it by  $S_n$ .

An action of a group  $G$  on a set  $X$  is a group homomorphism  $G \rightarrow S(X)$ . If  $g \in G$  and  $x \in X$  we write  $g.x$  for the image of  $x$  under the action of  $g$ . Thus  $1.x = x$ , and  $g.(h.x) = (gh).x$  for all  $x \in X$ , and all  $g, h \in G$ .

**Example 4.1. 1.** *The dihedral group  $D_n$  of order  $2n$ , ( $n \geq 3$ ). Let  $V$  be the set of vertices of a regular  $n$ -gon  $P$ . Consider all rigid motions of  $P$  that send  $V$  to  $V$ . Think of  $P$  as a piece of wood that you may pick up, rotate, turn over, and put down again so that it is in its original position, i.e., the vertices are placed*

on top of the original vertices. The set of all such motions is called the **dihedral group**  $D_n$ . If we think of  $D_n$  acting on  $V$  we see that it is a subgroup of  $S_n$ .

Label the vertices  $1, 2, \dots, n$  in a clockwise sequence. The position of the  $P$  after a rigid motion is determined by the new position of 1 after the motion and whether the vertices are now labelled in the clockwise or counter-clockwise order. Hence  $D_n$  has  $2n$  elements.

If clockwise rotation by  $2\pi/n$  radians is denoted by  $\tau$ , and the flip about some fixed axis is denoted by  $\sigma$ , then  $D_n$  is generated by  $\sigma$  and  $\tau$ . Now  $\tau^n = \sigma^2 = 1$ , and  $\sigma\tau\sigma^{-1} = \tau^{-1}$ . It is not hard to convince oneself that  $D_n$  consists of the  $2n$  distinct elements  $\{\tau^i, \sigma\tau^i \mid 0 \leq i \leq n-1\}$ .

For example,  $D_3$  acts on the vertices of an equilateral triangle, and  $D_3 \cong S_3$ .

**2.** The general linear group  $GL_n(k)$  or  $GL(n, k)$  is the group of all invertible  $k$ -linear maps  $k^n \rightarrow k^n$ .

**3.** If  $K/k$  is a Galois extension, then  $\text{Gal}(K/k)$  acts on  $K$ . It also acts on the intermediate fields lying between  $k$  and  $K$ . If  $K = k(\alpha)$ , then  $\text{Gal}(K/k)$  permutes the zeroes of the minimal polynomial of  $\alpha$ .

This is the historical origin of groups: the ancients considered the permutations of the zeroes of a polynomial.

**4.** A group  $G$  acts on itself by left multiplication,  $g.x = gx$ . If  $|G| = n$ , this action gives a homomorphism  $G \rightarrow S_n$ .

Notice that the action of  $G$  on itself by right multiplication is not always an action according to our definition because then  $g.(h.x) = (hg).x$ . (It is an action if  $G$  is commutative.) However, if we define  $g.x = xg^{-1}$ , this is an action of  $G$  on itself.

**5.** A group  $G$  acts on itself by conjugation:  $g.x = gxg^{-1}$ . This action defines a group homomorphism  $G \rightarrow \text{Aut } G$ , the automorphism group of  $G$ . The kernel of this is

$$\{g \in G \mid gx = xg \text{ for all } x \in G\} = Z(G),$$

the center of  $G$ . The image of this homomorphism is called the group of inner automorphisms of  $G$ , and is denoted by  $\text{Inn}(G)$ .

**6.** A group  $G$  acts on the set of its subgroups by conjugation,  $g.H = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ . Subgroups  $H$  and  $H'$  are said to be **conjugate** if  $H' = gHg^{-1}$  for some  $g \in G$ .

**7.** If  $H$  is a subgroup of  $G$ , then  $G$  acts on the set of left cosets of  $H$  by  $g.xH = (gx)H$ .

**8.** Suppose that  $G$  acts on a set  $X$ , and  $R$  is the ring of  $k$ -valued functions on  $X$ . Then there is an action of  $G$  on  $R$  by

$$(g.f)(x) = f(g^{-1}.x) \quad \text{for } g \in G, f \in R, \text{ and } x \in X.$$

It is essential to use  $g^{-1}$  here so one gets a left action of  $G$  on  $R$ . Notice that each  $g$  acts as an automorphism of the ring  $R$ . In fact, the automorphisms of a ring form a group, denoted by  $\text{Aut } R$ , and this action of  $G$  on  $R$  can be interpreted as a group homomorphism  $G \rightarrow \text{Aut } R$ . It is usual for  $X$  to have some additional structure and for the  $G$  action to preserve that structure and  $R$  to consist of functions that are related to that structure. For example,  $X$

may be a topological space and  $R$  might be the ring of all continuous  $\mathbb{R}$ -valued (or  $\mathbb{C}$ -valued) functions on  $X$ ; when  $X$  is a topological space we usually only consider continuous  $G$ -actions on  $X$ ; i.e., the map  $x \mapsto g.x$  is required to be continuous for all  $g \in G$ ; in this case,  $g.f$  is a continuous function whenever  $f$  is continuous so  $g.f$  belongs to  $R$  if  $f$  does.

**9.** Consider the previous example, but now suppose that  $X$  is an irreducible algebraic variety over a field  $k$ . Suppose further that the  $G$  action on  $X$  is such that the map  $x \mapsto g.x$  is a morphism of varieties for each  $g \in G$ . Each morphism corresponds to a homomorphism of rings  $\mathcal{O}(X) \rightarrow \mathcal{O}(X)$ ; explicitly it is  $f \mapsto g^{-1}.f$ . Hence we obtain a  $G$ -action on  $\mathcal{O}(X)$ . We extend this to an action of  $G$  on  $k(X)$  in the natural way  $g.(a/b) = (g.a)/(g.b)$ . It makes sense to consider the invariants  $k(X)^G$  and  $\mathcal{O}(X)^G$ .  
More ..... ◇

**Definition 4.2.** Let  $G$  be a group acting on a set  $X$ . The orbit of  $x \in X$  is  $G.x = \{g.x \mid g \in G\}$ . The stabilizer of  $x$  is  $\text{Stab}_G(x) = \{g \in G \mid g.x = x\}$ .

Notice that the stabilizer of  $x$  is a subgroup of  $G$ .

The orbits partition  $X$ ;  $X$  is the disjoint union of its orbits. This provides an equivalence relation on  $X$ ,

$$x \sim y \Leftrightarrow y \in G.x \Leftrightarrow G.x = G.y.$$

**Example 4.3.** We may view the general linear group  $GL_n(k)$  as the set of invertible  $n \times n$  matrices. It therefore acts on the space of  $n \times n$  matrices  $M_n(k)$  by  $g.A = gAg^{-1}$ . This is an important example and it motivates a lot of mathematics. The finer aspects of it are a topic for current research.

What are the orbits? In each orbit find a “nice” element. Jordan normal form, which we discuss next quarter, gives such a nice element, and is useful in answering other questions about this action.

**Proposition 4.4.** Let  $G$  be a finite group acting on a set  $X$ . If  $x \in X$ , then

1.  $|G| = |G.x| \times |\text{Stab}_G x|$ ;
2.  $|G.x| = |G : \text{Stab}_G x|$ ;
3.  $|G.x|$  divides  $|G|$ .

**Proof.** Let  $g, h \in G$ , and set  $S = \text{Stab}_G x$ . Then

$$g.x = h.x \Leftrightarrow g^{-1}h.x = x \Leftrightarrow g^{-1}h \in S \Leftrightarrow gS = hS.$$

Therefore the map

$$\phi : \{\text{left cosets of } S \text{ in } G\} \longrightarrow Gx, \quad \phi(gS) := gx$$

is a well-defined bijection. Thus  $|G.x|$  is equal to the number of left cosets of  $S$  in  $G$ ; that number is  $|G : S| = |G|/|S|$ . □

The following is a trivial consequence, but its triviality belies its significance.

**Lemma 4.5** (The Orbit Formula). *Let  $G$  be a finite group acting on a finite set  $X$ . Let  $X_1, \dots, X_n$  be the distinct  $G$ -orbits in  $X$ , and for each  $i$  choose  $x_i \in X_i$ . Then*

$$|X| = \sum_{i=1}^n |X_i| = \sum_{i=1}^n |G : \text{Stab}_G(x_i)|.$$

Notice that if  $G$  acts on  $X$  and  $x$  and  $y$  belong to the same orbit, then their stabilizers are conjugate: if  $y = g.x$  and  $S = \text{Stab}_G(x)$ , then  $\text{Stab}_G(y) = gSg^{-1}$ . Conversely, if two subgroups of  $G$  are conjugate to one another, then one is a stabilizer if and only if the other is.

**Definition 4.6.** *The conjugacy class of  $x \in G$  is*

$$C_G(x) = \{gxg^{-1} \mid g \in G\},$$

*and the centralizer of  $x \in G$  is*

$$Z_G(x) = \{g \in G \mid gx = xg\}.$$

*These are, respectively, the orbit and the stabilizer of  $x$  under the action of  $G$  on itself by conjugation.*

The center of a group is denoted by  $Z(G)$ ; by definition it consists of those elements  $z$  such that  $zg = gz$  for all  $g \in G$ . Notice that the center of a group consists of exactly those elements whose conjugacy classes have size one.

The next result follows at once from the definition and Proposition 4.4.

**Lemma 4.7.** *Let  $x$  be an element of a finite group  $G$ . Then*

$$|G| = |Z_G(x)| \times |C_G(x)|.$$

*In particular, the number of conjugates of  $x$  equals  $|G : Z_G(x)|$ , which divides  $|G|$ .*

**Proposition 4.8** (The Class Formula). *Let  $G$  be a finite group and let  $C_1, \dots, C_n$  be the distinct conjugacy classes in  $G$ . Then*

$$1. \quad |G| = \sum_{i=1}^n |C_i|;$$

2. *If  $Z(G)$  denotes the center of  $G$ , then*

$$|G| = |Z(G)| + \sum_{|C_i| > 1} |C_i|. \quad (4-2)$$

**Proof.** Since  $G$  is the disjoint union of its orbits,  $|G| = \sum_{i=1}^n |C_i|$  and this can be written as

$$|G| = \sum_{|C_i|=1} |C_i| + \sum_{|C_i|>1} |C_i|.$$

However,  $Z(G)$  is the disjoint union of those  $C_i$  having cardinality one.  $\square$

**Theorem 4.9** (Cauchy's Theorem). *Let  $p$  be a prime. If  $p$  divides the order of  $G$ , then  $G$  has an element of order  $p$ .*

**Proof.** Let  $\mathbb{Z}/p$  act on

$$X := \{(x_1, \dots, x_p) \mid x_i \in G, x_1 \cdots x_p = 1\} \subseteq G^p$$

by cyclic permutations, i.e., fix a generator  $\xi$  for  $\mathbb{Z}/p$  and define

$$\xi \cdot (x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1}).$$

The stabilizer of a point in  $X$  is a subgroup of  $\mathbb{Z}/p$  so is either  $\mathbb{Z}/p$  or the trivial subgroup. The number of elements in an orbit is therefore either 1 or  $p$ . An element in  $X$  is completely determined by its first  $p-1$  terms, which can be anything, so  $|X| = |G|^{p-1}$ . In particular,  $|X|$  is divisible by  $p$ . Since  $|X|$  is the sum of sizes of the distinct orbits, and non-trivial orbits have  $p$  elements, the number of orbits of size 1 is divisible by  $p$ . There is at least one orbits of size 1, namely  $(1, \dots, 1)$ , so there are at least  $p$  orbits of size 1. Every orbit of size 1 is of the form  $(a, \dots, a)$  for some  $a \in G$ . Hence there is  $a \in G - \{1\}$  such that  $a^p = 1$ .  $\square$

**Another proof of Cauchy's Theorem.** (This proof uses the classification of finite abelian groups.)

We argue by induction on the order of  $G$ . If  $G$  has a proper subgroup whose order is divisible by  $p$ , we may apply the induction hypothesis to that subgroup to obtain the result. So, we may assume  $G$  has no such subgroup.

If  $x \in G - Z(G)$ , then  $p$  does not divide the order of the proper subgroup  $Z_G(x)$ , so divides  $|C_G(x)|$ . It follows from (4-2) that  $p$  divides  $|Z(G)|$ . Hence  $Z(G) = G$ ; thus  $G$  is abelian.

Suppose that  $G$  and  $\{1\}$  are the only subgroups of  $G$ . Let  $x \in G - \{1\}$ . Then  $G = \langle x \rangle$ , the subgroup generated by  $x$ ; hence the order of  $x$  is  $|G|$ , which equals  $pn$ , so  $x^n$  has order  $p$ .

Now suppose that  $G$  and  $\{1\}$  are not the only subgroups of  $G$ . We can choose a proper subgroup  $H$  of largest possible order. Then  $H$  must be a maximal subgroup and, if  $|H| = m$ , then  $(p, m) = 1$ . By the induction hypothesis applied to  $G/H$ , there is an element  $x \in G - H$  such that  $x^p \in H$ . Since  $H$  is maximal,  $G = \langle H, x \rangle$ , and  $|G| = pm$ . If  $x^m = 1$ , choose  $a, b \in \mathbb{Z}$  such that  $ap + bm = 1$ . Then

$$x = x^{ap+bm} = (x^m)^a (x^p)^b \in H,$$

contradicting our choice of  $x$ . Hence  $x^m \neq 1$ , and

$$(x^m)^p = x^{mp} = x^{|G|} = 1,$$

so  $x^m$  has order  $p$ .

### 1.4.1 Small groups

A fundamental problem that has driven the development of finite group theory since its infancy is that of classification: classify all finite groups.

Here “small” does not mean that  $|G|$  is small, though that is a reasonable place to begin, but that  $|G|$  is a product of a small number of primes. For example, if  $p$  is prime and  $|G| = p$ , then  $G \cong \mathbb{Z}_p$ . The next result is the first step towards classifying groups of order  $p^n$ . I believe the classification of groups of order  $p^n$  is still not solved; I don’t even know if it is reasonable to hope for some sort of classification.

**Proposition 4.10.** *If the order of a group is a power of a prime, then its center is non-trivial; i.e., it contains a non-identity element.*

**Proof.** Suppose that  $|G| = p^r$ . If  $C_1, \dots, C_m$  are the conjugacy classes with more than one element, then  $|C_i| = p^{r_i}$  for some  $r_i > 1$ . It therefore follows from (4-2) that  $p$  divides  $|Z(G)|$ .  $\square$

**Proposition 4.11.** *If  $p$  is prime and  $|G| = p^2$ , then  $G$  is isomorphic to either  $\mathbb{Z}_p \times \mathbb{Z}_p$  or  $\mathbb{Z}/p^2$ .*

**Proof.** Let  $G$  be a group with  $p^2$  elements. If  $G$  is abelian, then  $G$  is isomorphic to either  $\mathbb{Z}_p \times \mathbb{Z}_p$  or  $\mathbb{Z}/p^2$ . We will show that  $G$  *must* be abelian. By Proposition 4.10,  $Z(G) \neq \{1\}$ . If  $Z(G) = G$ , then  $G$  is abelian. The remaining alternative is that  $|Z(G)| = p$ . However, in that case  $G/Z(G)$  has size  $p$  so is isomorphic to  $\mathbb{Z}_p$  and is there generated by a single element. It follows that  $G$  is generated by two elements, say  $z$  which generates  $Z(G)$  and  $y \in G - Z(G)$ . But  $x$  commutes with  $y$  so the group  $\langle x, y \rangle$  is abelian, i.e.,  $G$  is abelian.  $\square$

A group of order  $p^3$  need not be abelian. The quaternion group,

$$Q := \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}^\times,$$

where  $\mathbb{H}^\times$  is Hamilton’s group of non-zero quaternions, has size 8 and is not abelian.

There is another non-abelian group with 8 elements? What is it? Show it is not isomorphic to the quaternion group.

You might like to think of the next two cases, groups of size  $p^3$  for  $p = 3$  and  $p = 5$ . Can you classify them.

The next case is  $|G| = pq$  where  $p$  and  $q$  are distinct primes.

**Proposition 4.12.** *Let  $p$  and  $q$  be primes with  $p > q$ . If  $G$  is a group with  $pq$  elements, then  $G$  has a unique subgroup of order  $p$  and that subgroup is normal.*

**Proof.** By Cauchy’s Theorem,  $G$  has an element of order  $p$ . Let  $N$  be the subgroup it generates.

Suppose  $N$  is not normal. Then  $G$  has another subgroup of order  $p$ ,  $M = gNg^{-1}$  for some  $g \in G$ . Both  $G$  and  $M$  act on  $X := \{gNg^{-1} \mid g \in G\}$  by conjugation,  $g \cdot N = gNg^{-1}$ . We have  $|G| = |\text{Orb}_G(N)| \times |\text{Stab}_G(N)|$ . But  $N \subseteq$

$\text{Stab}_G(N) = N_G(N) \subsetneq G$  so  $\text{Stab}_G(N) = N$ . Therefore  $|\text{Orb}_G(N)| = q$ . Hence  $|\text{Orb}_M(N)| \leq q < p = |M|$ . But  $|\text{Orb}_M(N)|$  divides  $|M|$  so  $|\text{Orb}_M(N)| = 1$ . Hence  $M \subseteq \text{Stab}_G(N) = N$ . It follows that  $M = N$ . This contradiction implies that  $N$  is a normal subgroup of  $G$ .

Suppose  $M$  is another subgroup of order  $p$ . Let  $x \in M - \{1\}$ . Then  $x$  has order  $p$ . If  $x$  were in  $N$  it would generate both  $N$  and  $M$  which is absurd. Hence  $x \notin N$ . The image of  $x$  in  $G/N$ , which is isomorphic to  $\mathbb{Z}/q$ , is not the identity element so its order must be  $q$ . But the order of the image of  $x$  in  $G/N$  divides the order of  $x$ ; i.e.,  $q$  divides  $p$ . That is absurd so we conclude that  $N$  is the only subgroup of  $G$  having  $p$  elements.  $\square$

**Theorem 4.13.** *Let  $p$  and  $q$  be primes such that  $q$  divides  $p - 1$ . Then there is a unique non-abelian group of order  $pq$ , namely the semi-direct product*

$$\langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^s \text{ where } s^q \equiv 1 \pmod{p} \rangle. \quad (4-3)$$

**Proof.** By Proposition 1.2,  $\text{Aut } \mathbb{Z}_p \cong \mathbb{Z}_{p-1}$ . By Cauchy's Theorem,  $\mathbb{Z}_{p-1}$  has an element of order  $q$ . Hence there is a non-trivial homomorphism  $\phi : \mathbb{Z}_q \rightarrow \text{Aut}(\mathbb{Z}_p)$  and therefore a non-abelian group  $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$  having  $pq$  elements.

Let  $G$  be a non-abelian group of order  $pq$ . Let  $N$  be the normal subgroup of  $G$  having  $p$  elements. Then  $G \cong N \rtimes (G/N) \cong \mathbb{Z}_p \rtimes_\psi \mathbb{Z}_q$  for some non-trivial homomorphism  $\psi : \mathbb{Z}_q \rightarrow \text{Aut}(\mathbb{Z}_p)$ .

Since  $\mathbb{Z}_{p-1}$  is cyclic it has a *unique* subgroup with  $q$  elements. Therefore  $\psi = \phi\beta$  for some  $\beta \in \text{Aut}(\mathbb{Z}_q)$ . By Proposition 2.2,

$$\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q \cong \mathbb{Z}_p \rtimes_{\phi\beta} \mathbb{Z}_q = \mathbb{Z}_p \rtimes_\psi \mathbb{Z}_q.$$

Define the elements  $\sigma := (1, 0)$  and  $\tau := (0, 1)$  in  $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$ . We will use multiplicative notation for the product in  $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$ ; this might be a little confusing because we use additive notation for  $\mathbb{Z}_p$  and  $\mathbb{Z}_q$ ; thus, the product  $(a, b)(c, d)$  of two elements in  $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$  is  $(a + \phi(c)(b), b + d)$ . Now  $\sigma^p = \tau^q = 1$  and

$$\tau\sigma\tau^{-1} = (0, 1)(1, 0)(0, -1) = (\phi(1)(1), 0) = (s, 0) = \sigma^s$$

for some integer  $s$ . However,  $\tau^q = 1$  so  $\sigma = \tau^q\sigma\tau^{-q} = \sigma^{s^q}$ . Therefore  $s^q$  is equal to 1 modulo  $p$ .  $\square$

Theorem 4.13 is quite useful for classifying groups of small order. For example, making a table of small primes  $p$ , and primes  $q$  dividing  $p - 1$ , we obtain the following

| $p$ | $q$   | $pq$    |
|-----|-------|---------|
| 3   | 2     | 6       |
| 5   | 2     | 10      |
| 7   | 2, 3  | 14, 21  |
| 11  | 2, 5  | 22, 55  |
| 13  | 2, 3  | 26, 39  |
| 17  | 2,    | 34      |
| 19  | 2, 3  | 38, 57  |
| 23  | 2, 11 | 46, 253 |
| 29  | 2, 7  | 58, 206 |

Hence we have described the unique non-abelian group of the orders appearing in the right-hand column. We now know the structure of all groups of order  $n \leq 30$  except for  $n \in \{8, 12, 16, 18, 20, 24, 27, 28, 30\}$ .

Classifying those groups is a nice problem.

## 1.5 The Sylow Theorems

Let  $p$  be a prime. A  $p$ -group is a group in which the order of every element is a power of  $p$ .  $p$ -groups are of great importance, and it is an interesting problem to describe their structure. By Cauchy's Theorem, the order of a finite  $p$ -group is a power of  $p$  so has a non-trivial center by Proposition 4.10.

Finite  $p$ -groups are the building blocks for finite groups.

**Definition 5.1.** Let  $G$  be a finite group. If the order of  $G$  is  $p^n t$  where  $(p, t) = 1$ , a  $p$ -Sylow subgroup of  $G$  is a subgroup of order  $p^n$ .

Let  $H$  be a subgroup of  $G$ . Its normalizer in  $G$ , denoted  $N_G(H)$ , is largest subgroup of  $G$  that contains  $H$  as a normal subgroup.

If we let  $G$  act on its subgroups by conjugation, then  $N_G(H) = \text{Stab}_G H$ . Hence the number of conjugates of  $H$  in  $G$  is  $|G : N_G(H)| = |G|/|N_G(H)|$ .

**Theorem 5.2** (Sylow's First Theorem, 1872). Let  $G$  be a finite group of order  $p^n t$ , where  $(p, t) = 1$ . Let  $H$  be a subgroup of  $G$  of order  $p^i$  with  $i < n$ . Then there exists a subgroup  $K$  of  $G$  such that

1.  $H$  is normal in  $K$ , and
2.  $|K| = p^{i+1}$ .

In particular,  $p$ -Sylow subgroups exist, and every  $p$ -subgroup of  $G$  is contained in a  $p$ -Sylow subgroup.

**Proof.** We will show that  $p$  divides the order of the group  $N_G(H)/H$ ; Cauchy's Theorem will then provide an element  $x \in N_G(H) - H$  such that  $x^p \in H$ , whence  $\langle H, x \rangle$  will be the desired  $K$ .

Let  $H$  act on  $X = \{aH \mid a \in G\}$  by left multiplication. Since  $|X| = |G|/|H|$ ,  $p$  divides  $|X|$ . But

$$|X| = \sum_{\text{distinct orbits}} |H.x| = \sum_{\text{distinct orbits}} |H.(aH)|$$

and  $|H.aH| = |H : \text{Stab}_H(aH)| = p^j$  for some  $j \leq i$ . Therefore the number of orbits of size one is divisible by  $p$ .

Notice that  $|H.aH| = 1$  if and only if  $h.aH = aH$  for all  $h \in H$ , if and only if  $a^{-1}ha \in H$  for all  $h \in H$ , if and only if  $a \in N_G(H)$ , if and only if  $aH \in N_G(H)/H$ . Therefore the number of orbits of size one is  $|N_G(H)/H|$ ; so this is divisible by  $p$  as claimed.  $\square$

**Lemma 5.3.** *Let  $P$  be a  $p$ -Sylow subgroup of  $G$ , and suppose that  $x \in G$  has order  $p^i$ . If  $xPx^{-1} = P$ , then  $x \in P$ . In particular, if  $P$  is normal in  $G$ , then it is the only  $p$ -Sylow subgroup.*

**Proof.** Suppose to the contrary that  $x \notin P$ . Then  $P$  is normal in the strictly larger group  $\langle P, x \rangle$ . But  $\langle P, x \rangle / P$  is a cyclic group generated by  $\bar{x}$ , the image of  $x$ , so its order is equal to the order of  $\bar{x}$ , which must divide the order of  $x$ , and so is equal to  $p^m$  for some  $m \geq 1$ . But this implies that  $p^m$  divides  $|G|/|P|$  which is false since  $P$  is a  $p$ -Sylow subgroup. Hence  $x$  belongs to  $P$ , as claimed.

Now suppose that  $P$  is normal in  $G$ . If  $Q$  is another  $p$ -Sylow subgroup, pick  $x \in Q$ . The order of  $x$  is a power of  $p$ , so the first part of the lemma applies, showing that  $x \in P$ . Hence  $Q \subset P$ . But  $|Q| = |P|$ , so  $Q = P$ .  $\square$

**Theorem 5.4** (Sylow's Second and Third Theorems). *Let  $G$  be a finite group.*

1. *Any two  $p$ -Sylow subgroups of  $G$  are conjugate.*
2. *The number of  $p$ -Sylow subgroups is of the form  $np + 1$ .*
3. *The number of  $p$ -Sylow subgroups divides  $|G|$ .*

**Proof.** Let  $P$  be a  $p$ -Sylow subgroup of  $G$ , and let  $X = \{P = P_0, P_1, \dots, P_t\}$  be the distinct conjugates of  $P$  in  $G$ .

Let  $P$  act on  $X$  by conjugation; that is,  $x.P_i = xP_i x^{-1}$  for  $x \in P$ . One orbit is  $P = P_0$  and, by Lemma 5.3, this is the only orbit consisting of one element. The orbit of  $P_i$  has size  $|P : \text{Stab}_P(P_i)|$ , so is divisible by  $p$  if  $i \neq 0$ . But  $|X| = \sum |\text{distinct orbits}|$ , so  $|X| = np + 1$  for some  $n \in \mathbb{N}$ .

Suppose  $Q$  is a  $p$ -Sylow subgroup of  $G$  that does not belong to  $X$ . Let  $Q$  act on  $X$  by conjugation. There is no orbit of size one because  $xP_i x^{-1} = P_i$  for all  $x \in Q$ , then  $Q \subset P_i$  by Lemma 5.3. Hence, by the same argument as in the previous paragraph,  $p$  divides  $|X|$ ; this contradicts the previous paragraph, so we conclude that  $X$  consists of all  $p$ -Sylow subgroups. This proves (1) and (2).

Let  $G$  act on  $X$  by conjugation. There is only one orbit, so  $|X| = |G : \text{Stab}_G(P)|$  which divides  $|G|$ , so (3) holds.  $\square$

## 1.6 Using Sylow's Theorems

Sylow's theorems are the rock on which all deeper analysis of finite groups is built. This section contains some illustrative examples.

**Theorem 6.1.** *Let  $p$  and  $q$  be primes such that  $q|p-1$ . Then there is a unique non-abelian group of order  $pq$ , namely*

$$\langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^s \text{ where } s^q \equiv 1 \pmod{p} \rangle. \quad (6-4)$$

**Proof.** Suppose that  $G$  is a non-abelian group of order  $pq$ . The number of  $p$ -Sylow subgroups is congruent to  $1 \pmod{p}$  and divides  $pq$ , so there is a unique

$p$ -Sylow subgroup, say  $N$ , and it is therefore normal in  $G$ . Let  $H$  be any  $q$ -Sylow subgroup of  $G$ . Then  $H \cap N = \{1\}$  and  $NH = G$ . Hence  $G \cong N \rtimes H$ . The result now follows from Proposition 2.5 and Corollary ??.

**Example 6.2.** If  $|G| = 28$ , then  $G$  is not simple. Since  $28 = 2^2 \cdot 7$ , and the number of 7-Sylow subgroups is  $\equiv 1 \pmod{7}$  and divides 28, there is exactly one 7-Sylow subgroup. Since all 7-Sylow subgroups are conjugate, that 7-Sylow subgroup must be normal.

**Example 6.3.** If  $|G| = 56 = 2^3 \cdot 7$ , then  $G$  is not simple. The number of 7-Sylow subgroups divides 56 and is congruent to 1 (mod 7), so is either 1 or 8. If there were only one 7-Sylow subgroup it would be a normal subgroup, so  $G$  would not be simple.

Suppose there were eight 7-Sylow subgroups. Since a 7-Sylow subgroup is isomorphic to  $\mathbb{Z}_7$ , the intersection of two distinct 7-Sylow subgroups would equal  $\{1\}$ . Hence the union, say  $V$ , of the eight distinct 7-Sylow subgroups contains  $1 + 8 \times 6 = 49$  elements. Now let  $P$  be a 2-Sylow subgroup. None of the eight elements in  $P$  has order 7, so  $P \cap V = \{1\}$ , whence  $V \cup P = G$ . It follows that  $P$  is the unique 2-Sylow subgroup, and is therefore normal in  $G$ .

**Lemma 6.4.** If  $|G| = p^n q$  where  $p$  and  $q$  are distinct primes with  $q < p$ , then  $G$  is not simple.

**Proof.** The number of  $p$ -Sylow subgroups is  $\equiv 1 \pmod{p}$  and divides  $q$ , so must be one. That  $p$ -Sylow subgroup is therefore normal.

A possible project in a first course on group theory is to find all simple groups of order  $\leq 100$ . The previous lemma allows one to exclude quite a lot of the possibilities

| $q$ | $p$       | there is no simple group of order      |
|-----|-----------|----------------------------------------|
| 2   | 3         | 6, 18, 54                              |
| 2   | 5         | 10, 50                                 |
| 2   | 7         | 14, 98                                 |
| 2   | $\geq 11$ | 22, 26, 34, 38, 46, 58, 62, 74, 86, 94 |
| 3   | 5         | 15, 75                                 |
| 3   | $\geq 7$  | 21, 33, 39, 51, 57, 69, 87, 93         |
| 5   | $\geq 7$  | 35, 55, 65, 85, 95                     |

**Lemma 6.5.** If  $H$  is a subgroup of  $G$  of index two, then  $H$  is normal in  $G$ .

**Proof.** Because  $G$  is the disjoint union of the cosets of  $H$  we have

$$G = H \sqcup Hx = H \sqcup xH,$$

where  $x \notin H$ . Thus  $xH = xH$  and  $xHx^{-1} = H$ .

We now use Sylow's theorems to prove that  $\mathbb{C}$  is the algebraic closure of  $\mathbb{R}$ . Our proof will use two facts:

1. if the degree of  $f \in \mathbb{C}[x]$  is two, then  $f$  splits in  $\mathbb{C}$ ;
2. if the degree of  $f \in \mathbb{R}[x]$  is odd, then  $f$  has a zero in  $\mathbb{R}$ .

**Theorem 6.6** (The Fundamental Theorem of Algebra). *Every polynomial in  $\mathbb{C}[x]$  is a product of linear polynomials. That is,  $\mathbb{C}$  is algebraically closed.*

**Proof.** It is enough to show that if  $\mathbb{R} \subset \mathbb{C} \subset K$  is a finite normal extension of  $\mathbb{R}$ , then  $K = \mathbb{C}$ .

Write  $G = \text{Gal}(K/\mathbb{R})$ , and  $|G| = [K : \mathbb{R}] = 2^n s$  with  $s$  odd.

Let  $P$  be a 2-Sylow subgroup of  $G$ , and let  $K^P$  be the fixed field of  $P$ . Then  $[K^P : \mathbb{R}] = |G|/|P| = s$ . Since  $s$  is odd,  $[\mathbb{R}(\alpha) : \mathbb{R}]$  is odd for all  $\alpha \in K^P$ . Hence the minimal polynomial of  $\alpha$  over  $\mathbb{R}$  has odd degree, and therefore has a zero in  $\mathbb{R}$ . But the minimal polynomial is also irreducible, so it has degree one. Hence  $\alpha \in \mathbb{R}$ , and therefore  $K^P = \mathbb{R}$ , and  $s = 1$ .

It follows that  $[K : \mathbb{C}] = 2^{n-1}$ . Because  $K$  is normal over  $\mathbb{R}$  it is normal, and hence Galois, over  $\mathbb{C}$ . Write  $G' = \text{Gal}(K/\mathbb{C})$ . Thus  $|G'| = 2^{n-1}$ . If  $K \neq \mathbb{C}$ , then Sylow's First Theorem provides a subgroup  $H$  of  $G'$  of index two. Hence  $[K^H : \mathbb{C}] = |G'|/|H| = 2$ . But this contradicts the fact (1).  $\square$

**Theorem 6.7.** *Let  $(A, +)$  be a finite abelian group of order  $n = p_1^{r_1} \cdots p_n^{r_n}$  where the  $p_i$ s are distinct primes and each  $r_i$  is  $\geq 1$ . For each prime  $p$ ,  $A$  has a unique  $p$ -Sylow subgroup, namely*

$$A_p := \{a \in A \mid \text{the order of } a \text{ is } p^j \text{ for some } j\},$$

and  $A = A_{p_1} \oplus \cdots \oplus A_{p_n}$ .

**Proof.** Since  $A$  is an abelian all its subgroups are normal, so for each prime  $p$  dividing  $n$  there is a unique  $p$ -Sylow subgroup. Each element of that  $p$ -Sylow subgroup has order a power of  $p$  and, conversely, every element of  $A$  having order a power of  $p$  belongs to a  $p$ -Sylow (Sylow's First Theorem). Hence the  $p$ -Sylow subgroups are the subgroups  $A_p$ .

To see that the sum of the  $A_p$ s is direct suppose that  $0 = a_1 + \cdots + a_n$  with each  $a_i \in A_{p_i}$ . If some  $a_i \neq 0$ , we can assume after relabelling that  $a_1 \neq 0$ . Write  $m = n/p_1^{r_1}$ . Then  $0 = m \cdot 0 = m a_1$ ; but this implies that  $m$  divides  $p_1^{r_1}$  which is absurd.

It remains to show that the sum of all the  $A_p$ s is  $A$ . Let  $0 \neq a \in A$ . The order of  $a$  is of the form  $m = p_1^{s_1} \cdots p_n^{s_n}$  for suitable integers  $s_i$ . Set  $d_i = m/p^{s_i}$ . Then  $\gcd(d_1, \dots, d_n) = 1$ . Hence there exist integers  $t_1, \dots, t_n$  such that  $t_1 d_1 + \cdots + t_n d_n = 1$ . Thus  $a = (t_1 d_1)a + \cdots + (t_n d_n)a$ . The order of  $(t_i d_i)a = (t_i m/p^{s_i})a$  is a power of  $p_i$ , so  $(t_i d_i)a \in A_{p_i}$ . Hence  $a \in A_{p_1} + \cdots + A_{p_n}$ .  $\square$

## 1.7 Simple Groups

One of the outstanding algebraic achievements of the 20<sup>th</sup> century is the classification of finite simple groups. Recall that a group is **simple** if its only normal

subgroups are itself and  $\{1\}$ . If  $G$  is any finite group there is a chain of subgroups

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

such that each  $G_{i+1}$  is normal in  $G_i$  and  $G_i/G_{i+1}$  is simple. To construct such a chain start by choosing  $G_1$  to be a maximal normal subgroup of  $G$ , and take  $G_2$  to be a maximal normal subgroup of  $G_1$ , and so on. Thus one sees that simple groups are the building blocks of all finite groups and a classification of all finite groups might proceed by finding all the simple ones and then understanding how a simple group can be glued on top of another group.

The precise problem that encapsulates the last step is as follows: Fix two finite groups  $N$  and  $H$  and classify the groups  $G$  that contain a copy of  $N$  as a normal subgroup such that  $G/N \cong H$ . This is a hard problem. It contains, at the very least, the problem of classifying semi-direct products  $N \rtimes H$ .

Let's think look for small simple groups. First there are the cyclic groups  $\mathbb{Z}_p$ ,  $p$  prime. Then we can run through the integers starting at 4 and try to use the results in the previous section to eliminate various numbers  $n$ , i.e., find  $n$  such that there is not a simple group of size  $n$ .

**Proposition 7.1.** *If  $G$  is a simple group with 60 elements, then  $G \cong A_5$ .*

**Proof.** Let  $G$  be a simple group of size 60. Notice first that  $60 = 2^2 \cdot 3 \cdot 5$ .

Claim: If  $G$  has a subgroup of index 5, then  $G \cong A_5$ . Proof: If  $H$  is a subgroup of index 5, then  $G$  acts on the set of left cosets of  $H$  and they form a single orbit; the action of  $G$  on this set of 5 cosets provides a non-trivial group homomorphism  $G \rightarrow S_5$  which is injective because  $G$  is simple. So we can think of  $G$  as a subgroup of  $S_5$ , and since  $|S_5| = 120$ ,  $G$  is of index two and hence normal in  $S_5$ . By Proposition 3.8,  $G = A_5$ .  $\diamond$

Now we will prove  $G$  has a subgroup of index 5.

Consider first the 5-sylow subgroups. There must be six of them and the intersection of any two of these is  $\{1\}$ . Their union consists of  $6 \times (5 - 1) = 24$  elements of order 5.

Now consider the 2-sylow subgroups. The possibilities for their number is 1, 3, 5, and 15. There can't be just one because it would then be a normal subgroup. Neither can there be just three of them because then the action of  $G$  by conjugation on the set of 2-Sylow subgroups would provide a non-trivial homomorphism  $G \rightarrow S_3$  and, because  $|G| > |S_3|$ , the kernel of this map would be a proper normal subgroup of  $G$ . Hence there are either 5 or 15 2-sylow subgroups.

If there are five 2-sylow subgroups they form a single orbit under  $G$  acting by conjugation and hence we obtain a homomorphism  $G \rightarrow S_5$ . Now argue as before that the image of this map is  $A_5$ .

Now suppose there are 15 2-sylow subgroups. If the intersection of any two of these is  $\{1\}$ , then the union of the 2-sylow subgroups contains  $15 \times (2^2 - 1) = 45$  elements of order either two or four. But  $45 + 24 > 60$ , so this cannot be the case. Hence there are two 2-sylow subgroups, say  $H$  and  $K$  such that  $H \cap K \neq \{1\}$ . Now  $H \cap K$  is central in  $H$  and  $K$  and hence in the subgroup they generate,

$\langle H, K \rangle$ . The center of a group is always a normal subgroup, so the simplicity of  $G$  implies that  $\langle H, K \rangle \neq G$ . Since  $H$  is a proper subgroup of  $\langle H, K \rangle$ , and  $4 = |H|$  divides  $|\langle H, K \rangle|$ , we conclude that  $|\langle H, K \rangle| \geq 8$ ; of course it can't be 8 because 8 does not divide 60, so  $|\langle H, K \rangle| \geq 12$ . If the order of this were  $> 12$  its index would be  $d < 5$  and the action of  $G$  on the cosets of  $\langle H, K \rangle$  would provide a homomorphism  $G \rightarrow S_d$  which would have a kernel. That can't happen, so we conclude that  $|\langle H, K \rangle| = 12$ , and hence  $G$  has a subgroup of index 5.  $\square$

The next smallest simple group (apart from the cyclic ones) has order 168. It is  $\text{PSL}(2, 7)$  the projective special linear group of  $2 \times 2$  matrices over  $\mathbb{F}_7$ .

**Definition 7.2.** For any field  $k$  and integer  $n \geq 1$ , the special linear group  $\text{SL}(n, k)$  consists of the  $n \times n$  matrices over  $k$  of determinant one. The projective special linear group is

$$\text{PSL}(n, k) := \text{SL}(n, k) / \text{center}$$

$\diamond$

If  $n > 1$ ,  $\text{SL}(n, k)$  is never simple because it has non-trivial center: its center consists of those matrices  $\xi I$  where  $\xi \in k$  is an  $n^{\text{th}}$  root of unity.

The center of  $\text{SL}(2, 7)$  is  $\{\pm 1\}$  so  $|\text{PSL}(2, 7)| = \frac{1}{2}|\text{SL}(2, 7)|$ . Let's count: there are  $7^2 - 1 = 48$  choices for the first column of  $g \in \text{GL}(2, 7)$ ; then there are  $7^2 - 7$  choices for the second column. Hence  $|\text{GL}(2, 7)| = (7^2 - 1)(7^2 - 7)$ . Now, multiplying the first column of  $g \in \text{GL}(2, 7)$  by a non-zero  $\xi \in \mathbb{F}_7$  produces a new element of  $\text{GL}(2, 7)$  whose determinant is  $\xi$  times  $\det g$ . Hence, there is a unique  $\xi$  such that the new matrix has determinant one. Hence

$$|\text{SL}(2, 7)| = \frac{|\text{GL}(2, 7)|}{|\mathbb{F}_7 - \{0\}|} = (7^2 - 1) \times 7.$$

It follows at once that  $|\text{PSL}(2, 7)| = 168$ .

**Theorem 7.3.** If  $p > 4$ , then  $\text{PSL}(2, p)$  is simple.

## 1.8 Solvable groups

**Definition 8.1.** A group  $G$  is solvable if there exists a finite chain of subgroups

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

such that each  $G_{i+1}$  is a normal subgroup of  $G_i$  and  $G_i/G_{i+1}$  is abelian. We call such a chain of subgroups a solvable chain.  $\diamond$

If  $H$  is a finitely generated abelian group, then there is a finite chain of subgroups  $H = H_0 \supset H_1 \supset \cdots \supset H_m = \{0\}$  such that each  $H_i/H_{i+1}$  is cyclic: if  $H = \mathbb{Z}h_1 + \cdots + \mathbb{Z}h_m$ , the chain of submodules  $0 \subset \mathbb{Z}h_1 \subset \mathbb{Z}h_1 + \mathbb{Z}h_2 \subset \cdots$  has cyclic slices.

Hence, in the definition of a solvable group we can insist that the quotients  $G_i/G_{i+1}$  are cyclic.

**Proposition 8.2.** *Let  $N$  be a normal subgroup of a group  $G$ . Then  $G$  is solvable if and only if  $N$  and  $G/N$  are solvable.*

**Proof.** ( $\Rightarrow$ ) Let  $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$  be a solvable chain.

Claim: the chain  $N = N \cap G_0 \supset N \cap G_1 \supset \cdots \supset N \cap G_n = \{1\}$  is a solvable chain. Let  $\pi_i : G_i \rightarrow G_i/G_{i+1}$  be the natural map. The restriction of  $\pi_i$  to  $N \cap G_i$  has kernel  $N \cap G_{i+1}$ , so  $N \cap G_{i+1}$  is a normal subgroup of  $N \cap G_i$ , and the quotient  $N \cap G_i / N \cap G_{i+1}$  is isomorphic to a subgroup of  $G_i/G_{i+1}$ , so is abelian.

Let  $\psi : G \rightarrow G/N$  be the natural map. To show that  $G/N$  is solvable, we show that the chain  $G/N = \psi(G_0) \supset \psi(G_1) \supset \cdots \supset \psi(G_n) = \{1\}$  is a solvable chain. Because  $G_{i+1}$  is a normal subgroup of  $G_i$ ,  $\psi(G_{i+1})$  is a normal subgroup of  $\psi(G_i)$ . The map  $G_i \rightarrow \psi(G_i) \rightarrow \psi(G_i)/\psi(G_{i+1})$  is surjective and sends  $G_{i+1}$  to zero, so induces a surjective map  $G_i/G_{i+1} \rightarrow \psi(G_i)/\psi(G_{i+1})$ . Therefore  $\psi(G_i)/\psi(G_{i+1})$  is abelian.

( $\Leftarrow$ ) The map  $H \mapsto H/N$  from subgroups of  $G$  containing  $N$  to subgroups of  $G/N$  is a bijection. Furthermore,  $H$  is normal in  $G$  if and only if  $H/N$  is normal in  $G/N$ , and if  $H \supset K \supset N$ , then  $H/K \cong (H/N)/(K/N)$ .

Thus, a solvable chain in  $G/N$  corresponds to a chain  $G = G_0 \supset G_1 \supset \cdots \supset G_n = N$  of subgroups in  $G$ .

If  $N = N_0 \supset N_1 \supset \cdots \supset N_m = \{1\}$  is a solvable chain in  $N$ , then

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = N \supset N_1 \supset \cdots \supset N_m = \{1\}$$

is a solvable chain in  $G$ . □

The proof that  $G$  solvable implies  $N$  solvable did not use the fact that  $N$  is normal. In fact, every subgroup of a solvable group is solvable.

## 1.9 Some important groups

$\mathrm{GL}(n)$ ,  $SL(n)$ ,  $O(n)$ ,  $SO(n)$ ,  $SP(n)$ , Spin groups,  $PGL(n)$ ,  $PGL(2, \mathbb{F}_7)$ ,  $U(n)$  etc...

Tori, ...

**Example 9.1.** *Let  $p$  be a prime and  $q = p^r$ . We want to consider the finite general linear group*

$$G = \mathrm{GL}_n(\mathbb{F}_q).$$

*First let's compute its order.*

*By its very construction  $\mathrm{GL}_n(\mathbb{F}_q)$  acts on the  $n$ -dimensional vector space  $V = \mathbb{F}_q^n$ . We view elements of  $V$  as column vectors so that  $\mathrm{GL}_n(\mathbb{F}_q)$  acts from the left by multiplication.*

*Fix an ordered basis  $\mathcal{B} = \{v_1, \dots, v_n\}$  for  $V$ . Each  $g \in \mathrm{GL}_n(\mathbb{F}_q)$  sends  $\mathcal{B}$  to a new ordered basis  $g.\mathcal{B} = \{g.v_1, \dots, g.v_n\}$ . Every ordered basis is of the form  $g.\mathcal{B}$  for some  $g$ , and  $g.\mathcal{B} = g'.\mathcal{B}$  if and only if  $g = g'$ . Thus the ordered bases form a*

single orbit under the action of  $\mathrm{GL}_n(\mathbb{F}_q)$  and the stabilizer of each ordered basis is trivial. Hence

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \text{the number of ordered bases.}$$

Let's count the ordered bases. Choose  $0 \neq v_1 \in V$ . Since  $|V| = q^n$  there are  $q^n - 1$  possible choices for  $v_1$ . Having chosen  $v_1$ , choose  $v_2$  such that  $\{v_1, v_2\}$  is linearly independent. Since  $v_2$  may be any element of  $V - \mathbb{F}_q v_1$ , there are  $q^n - q$  choices for  $v_2$ . Now choose  $v_3$  such that  $\{v_1, v_2, v_3\}$  is linearly independent; since  $v_3$  may be any element in  $V - \mathbb{F}_q v_1 - \mathbb{F}_q v_2$ , there are  $q^n - q^2$  choices for  $v_3$ . Continuing in this way we see that the number of possible ordered bases is

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{\frac{1}{2}n(n-1)}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1) = |\mathrm{GL}_n(\mathbb{F}_q)|.$$

It follows from this that the order of a  $p$ -Sylow subgroup of  $\mathrm{GL}_n(\mathbb{F}_q)$  is  $q^{\frac{1}{2}n(n-1)}$ . The order of the upper triangular subgroup

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

is obviously  $q^{n-1}q^{n-2} \cdots q^2 \cdot q = q^{\frac{1}{2}n(n-1)}$ , so this is a  $p$ -Sylow subgroup. All other  $p$ -Sylow subgroups are conjugate to this one, so if  $N$  is another  $p$ -Sylow subgroup, there is a choice of basis for  $V$  in which  $N$  is this upper triangular subgroup.  $\diamond$

## 1.10 Representation theory

Fix a group  $G$  and a field  $k$ .

A  $k$ -linear representation of  $G$  is a  $k$ -vector space  $V$  together with a left action of  $G$  on  $V$  by  $k$ -linear maps. We may denote the action of  $g \in G$  on  $v \in V$  either by  $g.v$  or, more formally, as  $\rho(g)(v)$  where  $\rho : G \rightarrow \mathrm{GL}(V)$  is the group homomorphism determined by the action. Thus, we sometimes denote a representation by a pair  $(V, \rho)$ .

Usually,  $k$  is understood so we simply speak of representations of  $G$  or, more briefly, of  $G$ -modules.

If  $U$  and  $V$  are  $G$ -modules, a linear map  $\phi : U \rightarrow V$  is said to be a  $G$ -module homomorphism or  $G$ -equivariant if

$$\phi(g.u) = g.\phi(u)$$

for all  $u \in U$  and  $g \in G$ .

### 1.11 $G$ -actions and orbit spaces

There are some other aspects of  $G$ -actions that should be discussed briefly although they are not purely algebraic matters.

The basic point is that group actions abound, and one often wishes to describe the orbit spaces. Moreover, if the space  $X$  being acted on has some structure beyond being a set and the group  $G$  acts on  $X$  so as to preserve that structure (for example,  $X$  is a manifold and elements of  $G$  act as diffeomorphisms) one wants to put such a structure on the orbit space  $X/G$  too. That is not always possible, but one would still like to do the best possible.

For example, consider the group  $\mathbb{Z}_2 = \{\pm 1\}$  acting on  $\mathbb{R}^2$  with  $-1$  acting as multiplication by  $-1$ . Is there a way to give the orbit space  $\mathbb{R}^2/\mathbb{Z}_2$  the structure of a manifold so that the map  $\mathbb{R}^2 \rightarrow \mathbb{R}^2/\mathbb{Z}_2$  sending each point to its orbit is smooth? The simplest realization of the orbit space is as the cone  $Q := \{(u, v, w) \in \mathbb{R}^3 \mid uw = v^2\}$ , and the map  $\mathbb{R}^2 \rightarrow Q$  defined by  $(x, y) \mapsto (x^2, xy, y^2)$  is the quotient map. Of course the cone is not a submanifold of  $\mathbb{R}^3$  because of the singularity at the cone.

**Projective spaces.** Perhaps the most important orbit spaces in geometry are the projective spaces,  $\mathbb{RP}^n$  and  $\mathbb{CP}^n$ . We outline a construction of these as orbit spaces.

Consider a field  $k$ , and the action of the multiplicative group  $(k^\times, \cdot)$  on the punctured vector space  $k^{n+1} - \{0\}$  according to the rule

$$\lambda \cdot (x_0, \dots, x_n) = (\lambda x_0, \dots, \lambda x_n).$$

The orbits are the punctured lines through the origin; they are in bijection with the 1-dimensional subspaces of  $k^{n+1}$ . The space of orbits is called the  $n$ -dimensional projective space over  $k$ , and is denoted by  $\mathbb{P}_k^n$ . Let's write  $[x_0, \dots, x_n]$  for the point in  $\mathbb{P}_k^n$  that represents the orbit that is the line through  $(x_0, \dots, x_n)$ .

Here is one motivation for introducing  $\mathbb{P}^n$ . You already know that the set of simultaneous solutions to some system of polynomial equations  $f_1 = \dots = f_r = 0$ , where each  $f_i \in k[x_0, \dots, x_n]$ , is an affine algebraic subvariety of  $\mathbb{A}^{n+1} = k^{n+1}$ . Let's write  $X$  for this subvariety. If each of the  $f_i$ s is homogeneous in  $x_0, \dots, x_n$ , then it is clear that  $f_i(\lambda x_0, \dots, \lambda x_n) = \lambda^{\deg f_i} f_i(x_0, \dots, x_n)$ , so that  $X$  is a union of lines through the origin. Hence, we might as well understand the image of  $X$  in  $\mathbb{P}_k^n$ . The images of such  $X$ s are called projective algebraic varieties and their study forms the subject matter of algebraic geometry.

There is a reason for preferring  $\mathbb{P}^n$  to  $\mathbb{A}^n$ : it is compact. Compactness is a finiteness property and one always has better results for compact than for non-compact spaces. A paradigmatic example of this is Poincaré duality, a result for compact connected manifolds that has no suitable analogue without the compactness hypothesis.

If you want a little practice consider the action of  $U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$  on the unit 3-sphere  $S^3$ , realized as  $\{(z_1, z_2) \in \mathbb{C}^2 \mid |z_1|^2 + |z_2|^2 = 1\}$  in  $\mathbb{C}^2$ , defined by  $\lambda \cdot (z_1, z_2) = (\lambda z_1, \lambda z_2)$ . Show that the map  $\pi : S^3 \rightarrow \mathbb{CP}^1$ , the complex projective line, defined by  $\pi(z_1, z_2) = [z_1, z_2]$  has fibers the  $U(1)$ -orbits, and

hence that  $\mathbb{CP}^1 \cong SS^3/U(1)$ . You can view  $\pi$  as being a fibration over  $\mathbb{CP}^1$  with fibers isomorphic to  $U(1) \cong S^1$ . Show that  $\mathbb{CP}^2 \cong S^2$ , the 2-sphere. This is the first example of a Hopf fibration; there are similar ones  $S^7 \rightarrow S^4$  and  $S^{15} \rightarrow S^8$  arising from Hamilton's quaternions and Cayley's octonions.

**Conjugacy classes of matrices.** A standard result in a graduate algebra course is to classify  $n \times n$  matrices up to conjugation over an algebraically closed field  $k$ . This is equivalent to classifying finite dimensional modules over  $k[x]$ . You can think of this as classifying the orbits when  $GL(n)$  acts by conjugation on  $M_n(k)$  the set of  $n \times n$  matrices. The result is encapsulated in the famous Jordan normal form.

A similar sounding problem is to classify pairs of commuting  $n \times n$  matrices  $\{(A, B) \mid AB = BA\}$  up to simultaneous conjugation  $g.(A, B) = (gAg^{-1}, gBg^{-1})$ . This is an unsolved problem. Get the message that classifying orbits is an important but generally hard problem.

**Exercises.**

1. Let  $\beta$  be an element of  $\mathbb{F}_4$  that is not in  $\mathbb{F}_2$ .
  - (a) Find the minimal polynomial of  $\beta$  over  $\mathbb{F}_2$ .
  - (b) Show that  $x^2 + (\beta + 1)x + 1$  is irreducible in  $\mathbb{F}_4[x]$ .
  - (c) Is the cubic  $x^3 + x^2 + \beta \in \mathbb{F}_4[x]$  irreducible? If not, find its factors.
  - (d) Show that  $\mathbb{F}_{16}$  contains an element  $\alpha$  that is a primitive fifth root of one over  $\mathbb{F}_2$ , and that  $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ . Find the minimal polynomial of  $\alpha$  over  $\mathbb{F}_4$ , and show that  $\alpha^4$  is the other zero of this polynomial.
  - (e) Show that  $\alpha$  is a zero of  $x^3 + x^2 + \beta \in \mathbb{F}_4[x]$ .
  - (f) Show that the Galois group of  $x^5 - 1$  over  $\mathbb{F}_4$  is  $\mathbb{Z}_2$ .
  - (g) Factor  $x^4 + x^3 + x^2 + x + 1$  over  $\mathbb{F}_4$ .
  - (h) You have shown above that  $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$  where  $\alpha$  is a primitive fifth root of 1. Does there exist an element  $\alpha \in \text{Gal}(x^5 - 1/\mathbb{F}_4)$  such that  $\sigma(\alpha) = \alpha^2$ ?