Contents

1 Examples in Algebra **1**

1.1 Examples of Groups 1

1.1.1 $\mathbb{Z}/m\mathbb{Z}$ 1

1.1.2 $(\mathbb{Z}/m\mathbb{Z})^*$ 1

1.1.3 Klein four-group 1

1.1.4 Symmetric group S_n 2

1.1.5 Alternating group A_n 3

1.1.6 Dihedral group D_{2n} 3

1.1.7 Quaternion group Q_8 4

1.1.8 General linear group (over a field/ring) GL_n 4

1.1.9 Special linear group SL_n 4

1.1.10 Orthogonal group O_n 4

1.1.11 Special orthogonal group SO_n 4

1.1.12 Unitary group U_n 5

1.1.13 Special unitary group SU_n 5

1 Examples in Algebra

1.1 Examples of Groups

1.1.1 $\mathbb{Z}/m\mathbb{Z}$

The additive group

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$$
$$\overline{a} + \overline{b} = \overline{a+b}$$

has the following properties

1. $\mathbb{Z}/m\mathbb{Z}$ is cyclic.
2. $\overline{a}$, $(a, m) = 1$ is a generator. In particular, $\mathbb{Z}/m\mathbb{Z} = \langle \overline{1} \rangle$.
3. Any subgroup of $\mathbb{Z}/m\mathbb{Z}$ is of the form $\langle \overline{d} \rangle = \overline{d\mathbb{Z}}\,(d \big| n)$.
4. $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$
5. It can be decomposed using CRT.

1.1.2 $(\mathbb{Z}/m\mathbb{Z})^*$

The multiplicative group

$$(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{a} : (a, m) = 1\}$$

$$\overline{a}\overline{b} = \overline{ab}$$

has the following properties

1. $(\mathbb{Z}/p\mathbb{Z})^*$ has order $\varphi(m)$.
2. If $m = p$ is a prime number, then $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p - 1$.

1.1.3 Klein four-group

The group

$$V = \{a, b : a^2 = b^2 = (ab)^2 = 1\}$$

has the following properties

1. Each element is the inverse of itself.
2. The product of two different nonidentity elements is the third.

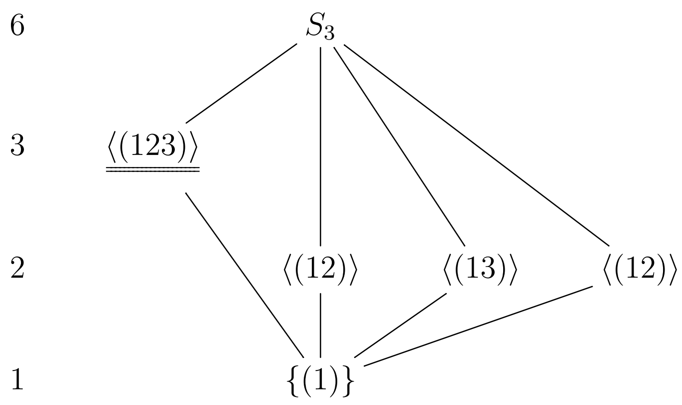
1.1.4 Symmetric group S_n

The group S_n of all permutations of n objects has the following properties

1. S_n has order n.
2. S_n is not abelian when $n \geqslant 3$.
3. $Z(S_n) = \{(1)\}$ for $n \geqslant 3$.
4. The alternating group A_n is a normal subgroup of S_n
5. S_n, A_n are unsolvable for $n \geqslant 5$.
6. The coset decomposition of S_n with respect to $S_{n-1} = \{\sigma \in S_n : \sigma(n) = n\}$ is
7. Any $\sigma \in S_n$ is a product of some nonintersecting cyclic permutations.

The cases $n = 3, 4$ are as follows:

S_3 The group $S_3 = \{(1),(12),(13),(23),(123),(132)\}$ is a nonabelian group of order 6. It is isomorphic to D_6 (See below for its presentation). The lattice of its subgroups is:



S_4 The group S_4 is a nonabelian group of order 24.

$$\begin{aligned}
S_4 &= \{(1),(12),(13),(23),(123),(132),\\
&= (34),(12)(34),(143),(243),(1243),(4321),\\
&= (24),(13)(24),(234),(142),(1342),(1423),\\
&= (14),(14)(23),(134),(124),(1234),(1324)\}
\end{aligned}$$

It is isomorphic to the symmetry group of a regular tetrahedron.

1.1.5 Alternating group A_n

The group A_n of all even permutations of n objects has the following properties

1. A_n is generated by all 3-cycles.
2. For $n \geqslant 5$, all 3-cycles are conjugate in A_n.
3. For $n \geqslant 5$, A_n is a simple group.
4. For $n \geqslant 5$, A_n is unsolvable.

1.1.6 Dihedral group D_{2n}

The group D_{2n} of all symmetries of a n-sided regular polygon has the following properties

1. D_{2n} is of order $2n$. Its elements are n rotations and n reflections.

2. D_{2n} has the group presentation

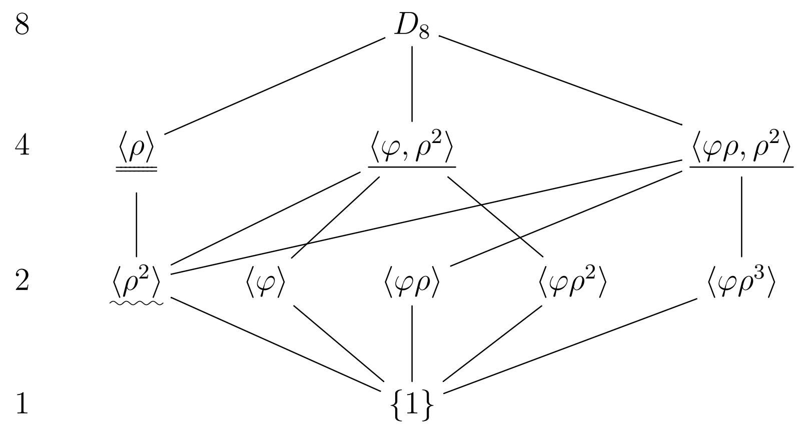
$$D_{2n} = \{\rho, \varphi : \rho^n = 1, \varphi^2 = 1, \rho\varphi = \varphi\rho^{n-1}\}$$

3. The center of D_{2n} is

$$Z(D_{2n}) = \begin{cases} \{1\} & , \quad n \text{ is odd} \\ \{1, r = \rho^{n/2}\} & , \quad n \text{ is even} \end{cases}$$

The case $n = 4$ is as follows:

D_8 The group D_8 of all symmetries of a square is a nonabelian group of order 8. The lattice of its subgroups is:

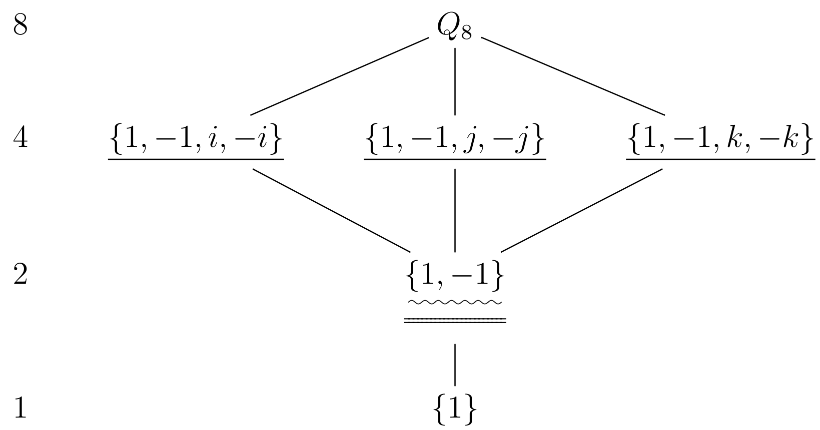


1.1.7 Quaternion group Q_8

The quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is a nonabelian group of order 8. It has the group presentation

$$Q_8 = \langle -1, i, j, k : (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$$

The lattice of its subgroups is:



1.1.8 General linear group (over a field/ring) GL_n

The general linear group of degree n over a field F or a ring R is the set of $n \times n$ invertible matrices with entries from F or R, associated with matrix multiplication. It is denoted $GL_n(F)$ or $GL_n(R)$.

1.1.9 Special linear group SL_n

The special linear group $SL_n(F)$ of degree n over a field F is the subgroup of $GL_n(F)$ in which each matrix has determinant 1.

1.1.10 Orthogonal group O_n

The orthogonal group O_n is a subgroup of GL_n in which each matrix is an orthogonal matrix.

1.1.11 Special orthogonal group SO_n

The special orthogonal group SO_n is a subgroup of O_n of index 2 in which each matrix is an orthogonal matrix with determinant 1. It is also called the rotation group.

1.1.12 Unitary group U_n

The unitary group U_n of degree n is a subgroup of $GL_n(\mathbb{C})$ in which each matrix is a unitary matrix.

1.1.13 Special unitary group SU_n

The special unitary group SU_n of degree n is a subgroup of U_n in which each matrix is a unitary matrix with determinant 1.