CHAPTER L

GROUPS OF LOW ORDER

In this chapter we shall give tables which give explicit information about several interesting examples of groups which have order less than 100. For the most part we shall not prove the results given in these tables. We strongly suggest that, in each individual case, the reader do the appropriate computations to check the information in these tables, for it is exactly in the computations in examples such as these that the subject of group theory "comes alive".

Notes of Arun Ram aram@unimelb.edu.au, Version: 4 April 2020

Let us begin with a list of the different groups of order $\leqslant 15$. The reader should think about extending this table to include all groups of order, say, $\leqslant 100$. The following beautiful book may be very helpful for such a project:

> H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups*, Series Ergebnisse der Mathematik und ihrer Grenzgebiete **14**, Springer-Verlag, Berlin 1984.

Note also that the finite abelian groups are completely determined by the Fundamental Theorem of Abelian groups, Theorem (?????). In the following table:

Q denotes the quaternion group.
$\mathbb{Z}/k\mathbb{Z}$ denotes the cyclic group of order k.
D_k denotes the dihedral group of order $2k$.
S_k denotes the symmetric group on k letters.
A_k denotes the alternating group on k letters.

Group	Order	Abelian
(1)	1	Yes
$\mathbb{Z}/2\mathbb{Z}$	2	Yes
$\mathbb{Z}/3\mathbb{Z}$	3	Yes
$\mathbb{Z}/4\mathbb{Z}$	4	Yes
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	4	Yes
$\mathbb{Z}/5\mathbb{Z}$	5	Yes
$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	6	Yes
$S_3 \simeq D_3$	6	No
$\mathbb{Z}/7\mathbb{Z}$	7	Yes
$\mathbb{Z}/8\mathbb{Z}$	8	Yes
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8	Yes
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8	Yes
D_4	8	No
Q	8	No
$\mathbb{Z}/9\mathbb{Z}$	9	Yes
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	9	Yes
$\mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	10	Yes
D_5	10	No
$\mathbb{Z}/11\mathbb{Z}$	11	Yes
$\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	12	Yes
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	12	Yes
$D_6 \simeq \mathbb{Z}/2\mathbb{Z} \times D_3$	12	No
A_4	12	No
$\langle S, T \mid S^3 = T^2 = (ST)^2 \rangle$	12	No
$\mathbb{Z}/13\mathbb{Z}$	13	Yes
$\mathbb{Z}/14\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	14	Yes
D_7	14	No
$\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	15	Yes

L.1. The cyclic group $\mathbb{Z}/2\mathbb{Z}$ of order 2, the 2-clock

There are at least two natural ways of defining the 2-clock. The isomorphism which shows that these two definitions are the same is given in the rightmost column of the following table.

Set	Operation	Multiplication Table
$\begin{aligned}\mu_2 &= \{1,-1\}\\ &= \{\pm 1\}\end{aligned}$	ordinary multiplication of integers	$\begin{array}{c\|cc} \times & 1 & \text{-1} \\ \hline 1 & 1 & \text{-1} \\ \text{-1} & \text{-1} & 1 \end{array}$
$\mathbb{Z}/2\mathbb{Z} = \{0,1\}$	addition modulo 2	$\begin{array}{c\|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$

The isomorphism is

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}/2\mathbb{Z} & \to & \mu_2 \\ & 0 & \mapsto & 1 \\ & 1 & \mapsto & -1 \end{array}$$

Elements

Element g	Order $o(g)$	Centralizer Z_g
1	1	$\mathcal{Z}_2$
-1	2	$\mathcal{Z}_2$

Generators and relations

Generators	Relations
g	$g^2 = 1$

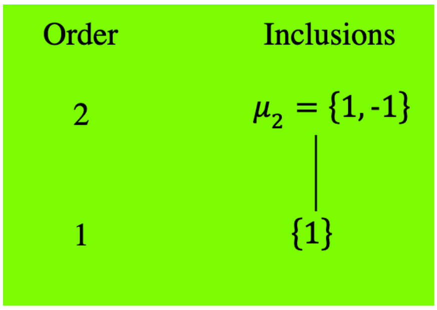
Some Homomorphisms

Homomorphism	Kernel	Image
$\begin{array}{rccc} \phi_0\colon & \mathcal{Z}_2 & \to & \{1\} \\ & 1 & \mapsto & 1 \\ & -1 & \mapsto & 1 \end{array}$	$\ker\phi_0 = \mu_2$	$\operatorname{im}\phi_0 = \{1\}$
$\begin{array}{rccc} \phi_1\colon & \mu_2 & \to & \mu_2 \\ & 1 & \mapsto & 1 \\ & -1 & \mapsto & -1 \end{array}$	$\ker\phi_1 = \{1\}$	$\operatorname{im}\phi_1 = \mu_2$

Center, conjugacy class and subgroups

Center	Abelian	Conjugacy classes	Subgroups
$Z(\mu_2) = \mu_2$	Yes	$\mathcal{C}_1 = \{1\}$ $\mathcal{C}_{-1} = \{-1\}$	$H_0 = \mu_2$ $H_1 = \{1\}$

Subgroup lattice



Subgroups H_i	Structure	Index	Normal	Quotient Group
$H_0 = \mu_2$	$H_0 = \mu_2$	$\mathrm{Card}(\mu_2/\mu_2) = 1$	Yes	$\mu_2/H_0 \simeq \{1\}$
$H_1 = \{1\}$	$H_1 = \{1\}$	$\mathrm{Card}(\mu_2/\{1\}) = 2$	Yes	$\mu_2/\{1\} \simeq \mu_2$

Subgroup H_i	Normalizer	Centralizer
$H_0 = \mu_2$	$N(H_0) = \mu_2$	$Z_{\mu_2}(H_1) = \mu_2$
$H_1 = (1)$	$N(H_1) = \mu_2$	$Z_{\mu_2}(H_1) = \mu_2$

Subgroups	Cosets	Right Cosets
$H_0 = \mu_2$	$\mu_2 = \{1, -1\}$	$\mu_2 = \{1, -1\}$
$H_1 = \{1\}$	$H_1 = \{1\}$ $(-1)H_1 = \{-1\}$	$H_1 = \{1\}$ $H_1(-1) = \{-1\}$

L.2. The Klein 4-group $G = \mu_2 \times \mu_2$

Let us make some shorter notations for the following matrices.

$$(1,1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (-1,1) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (1,-1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (-1,-1) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Klein 4-group is the group of order 4 defined as in the following table.

Set	Operation
$\mu_2 \times \mu_2 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$	matrix multiplication

The complete multiplication table for this group is as follows.

Multiplication Table

	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(-1,1)$	$(1,1)$	$(-1,-1)$	$(1,-1)$
$(-1,1)$	$(1,-1)$	$(-1,-1)$	$(1,1)$	$(-1,1)$
$(-1,-1)$	$(-1,-1)$	$(1,-1)$	$(-1,1)$	$(1,1)$

HW: Show that this group, as defined above, is isomorphic to the direct product of a cyclic group of order 2, μ_2, with another cyclic group of order 2, μ_2.

Center	Abelian	Conjugacy Classes	Subgroups
$Z(G) = \mu_2 \times \mu_2$	Yes	$\mathcal{C}_{(1,1)} = \{(1,1)\}$	$H_0 = \mu_2 \times \mu_2$
		$\mathcal{C}_{(1,-1)} = \{(1,-1)\}$	$H_1 = \{(1,1),(1,-1)\}$
		$\mathcal{C}_{(1,-1)} = \{(1,-1)\}$	$H_3 = \{(1,1),(-1,-1)\}$
		$\mathcal{C}_{(1,-1)} = \{(1,-1)\}$	$H_4 = \{(1,1)\}$

Elements

Element g	Order $o(g)$	Centralizer $Z(g)$	Conjugacy Class $\mathcal{C}_g$
$(1,1)$	1	$\mu_2 \times \mu_2$	$\mathcal{C}_{(1,1)}$
$(1,-1)$	2	$\mu_2 \times \mu_2$	$\mathcal{C}_{(1,-1)}$
$(-1,1)$	2	$\mu_2 \times \mu_2$	$\mathcal{C}_{(-1,1)}$
$(-1,-1)$	2	$\mu_2 \times \mu_2$	$\mathcal{C}_{(-1,-1)}$

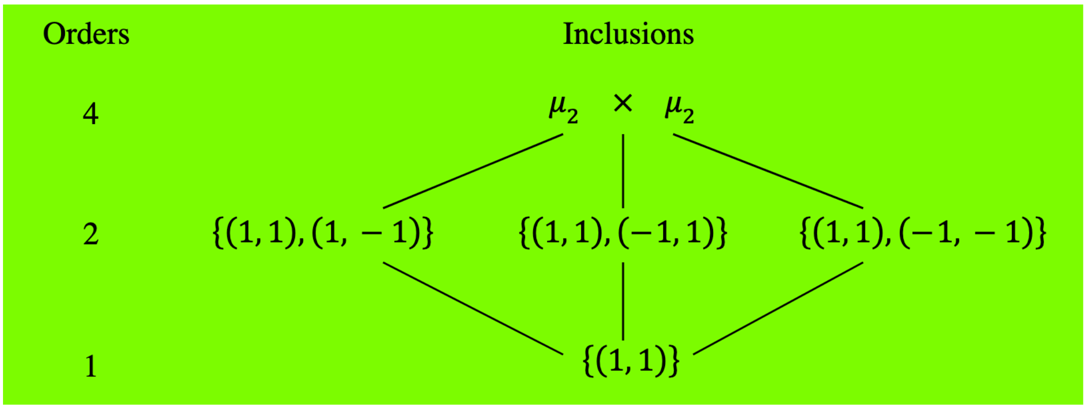
Generators and relations

Generators	Relations
x, y	$x^2 = 1$ $y^2 = 1$ $xy = yx$

Subgroups

Subgroups H_i	Structure	Size	Index	Quotient Group
$H_0 = \mu_2 \times \mu_2$	$\mu_2 \times \mu_2$	4	1	$(\mathcal{Z}_2 \times \mathcal{Z}_2)/H_0 \simeq (1)$
$H_1 = \{(1,1),(1,-1)\}$	μ_2	2	2	$(\mathcal{Z}_2 \times \mu_2)/H_1 \simeq \mu_2$
$H_2 = \{(1,1),(-1,1)\}$	μ_2	2	2	$(\mu_2 \times \mu_2)/H_2 \simeq \mu_2$
$H_3 = \{(1,1),(-1,-1)\}$	μ_2	2	2	$(\mu_2 \times \mu_2)/H_3 \simeq \mu_2$
$H_4 = \{(1,1)\}$	(1)	1	4	$(\mu_2 \times \mu_2)/H_4 \simeq \mu_2 \times \mu_2$

All of the subgroups H_0, H_1, H_2, H_3, H_4 are normal in $G = \mu_2 \times \mu_2$.



Subgroup H_i	Normalizer $N(H_i)$	Centralizer $Z_G(H_i)$
H_0	H_0	H_0
H_1	H_0	H_0
H_2	H_0	H_0
H_3	H_0	H_0
H_4	H_0	H_0

Subgroups	Cosets	Right Cosets
H_0	$H_0 = \{(\pm 1, \pm 1)\}$	$H_0 = \{\pm 1, \pm 1\}$
H_1	$H_1 = \{(1,1),(1,-1)\}$	$H_1 = \{(1,1),(1,-1)\}$
	$(-1,1)H_1 = \{(-1,1),(-1,-1)\}$	$H_1(-1,1) = \{(-1,1),(-1,-1)\}$
H_2	$H_2 = \{(1,1),(-1,1)\}$	$H_2 = \{(1,1),(-1,1)\}$
	$(1,-1)H_2 = \{(1,-1),(-1,-1)\}$	$H_2(1,-1) = \{(1,-1),(-1,-1)\}$
H_3	$H_3 = \{(1,1),(-1,-1)\}$	$H_3 = \{(1,1),(-1,-1)\}$
	$(1,-1)H_3 = \{(1,-1),(-1,1)\}$	$H_3(1,-1) = \{(1,-1),(-1,1)\}$
H_4	$H_4 = \{(1,1)\}$	$H_4 = \{(1,1)\}$
	$(-1,1)H_4 = \{(-1,1)\}$	$H_4(-1,1) = \{(-1,1)\}$
	$(1,-1)H_4 = \{(1,-1)\}$	$H_4(1,-1) = \{(1,-1)\}$
	$(-1,-1)H_4 = \{(-1,-1)\}$	$H_4(-1,-1) = \{(-1,-1)\}$

Some Homomorphisms

Homomorphism	Kernel	Image
$\phi_0\colon \quad \mu_2 \times \mu_2 \to \{1\}$		
$\qquad (-1,1) \mapsto 1$	$\ker \phi_0 = \mu_2 \times \mu_2$	$\operatorname{im} \phi_0 = \{1\}$
$\qquad (1,-1) \mapsto 1$		
$\phi_1\colon \quad \mu_2 \times \mu_2 \to \mu_2$		
$\qquad (-1,1) \mapsto -1$	$\ker \phi_1 = H_1$	$\operatorname{im} \phi_1 = \mu_2$
$\qquad (1,-1) \mapsto 1$		
$\phi_2\colon \quad \mu_2 \times \mu_2 \to \mu_2$		
$\qquad (-1,1) \mapsto 1$	$\ker \phi_2 = H_2$	$\operatorname{im} \phi_2 = \mu_2$
$\qquad (1,-1) \mapsto -1$		
$\phi_3\colon \quad \mu_2 \times \mu_2 \to \mu_2$		
$\qquad (-1,1) \mapsto -1$	$\ker \phi_3 = H_3$	$\operatorname{im} \phi_3 = \mu_2$
$\qquad (1,-1) \mapsto -1$		

L.3. $S_3 \simeq D_3$, the nonabelian group of order 6

Let

$$1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (12) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (23) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$(13) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad (132) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad (123) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

The groups S_3 and D_3 are as in the following table.

Set	Operation
$S_3 = \{1, (12), (23), (13), (132), (123)\}$	matrix multiplication
$D_3 = \{1, x, x^2, y, xy, x^2y\}$	$x^iy^jx^ky^l = x^{(i-k) \bmod 3}y^{(j+l) \bmod 2}$

The complete multiplication tables for these groups are as follows.

Multiplication Tables

S_3	1	(12)	(23)	(13)	(132)	(123)
1	1	(12)	(23)	(13)	(132)	(123)
(12)	(12)	1	(123)	(132)	(13)	(23)
(23)	(23)	(132)	1	(123)	(12)	(13)
(13)	(13)	(123)	(132)	1	(23)	(12)
(132)	(132)	(23)	(13)	(12)	(123)	1
(123)	(123)	(13)	(12)	(23)	1	(132)

D_3	1	y	x^2y	xy	x^2	x
1	1	y	x^2y	xy	x^2	x
y	y	1	x	x^2	xy	x^2y
x^2y	x^2y	x^2	1	x	y	xy
xy	xy	x	x^2	1	x^2y	y
x^2	x^2	x^2y	xy	y	x	1
x	x	xy	y	x^2y	1	x^2

HW: Prove that the group homorphism given as in the following table is an isomorphism.

Isomorphism

$$\begin{array}{lrcl} \Phi\colon & D_3 & \to & S_3 \\ & x & \mapsto & (123) \\ & y & \mapsto & (12) \end{array}$$

Center	Abelian	Conjugacy Classes	Subgroups
$Z(S_3) = \{1\}$	No	$\mathcal{C}_{(1^3)} = \{1\}$ $\mathcal{C}_{(21)} = \{(12), (23), (13)\}$ $\mathcal{C}_{(3)} = \{(123), (132)\}$	$H_0 = S_3$ $H_1 = \{1, (132), (123)\}$ $H_2 = \{1, (12)\}$ $H_3 = \{1, (13)\}$ $H_4 = \{1, (23)\}$ $H_5 = \{1\}$

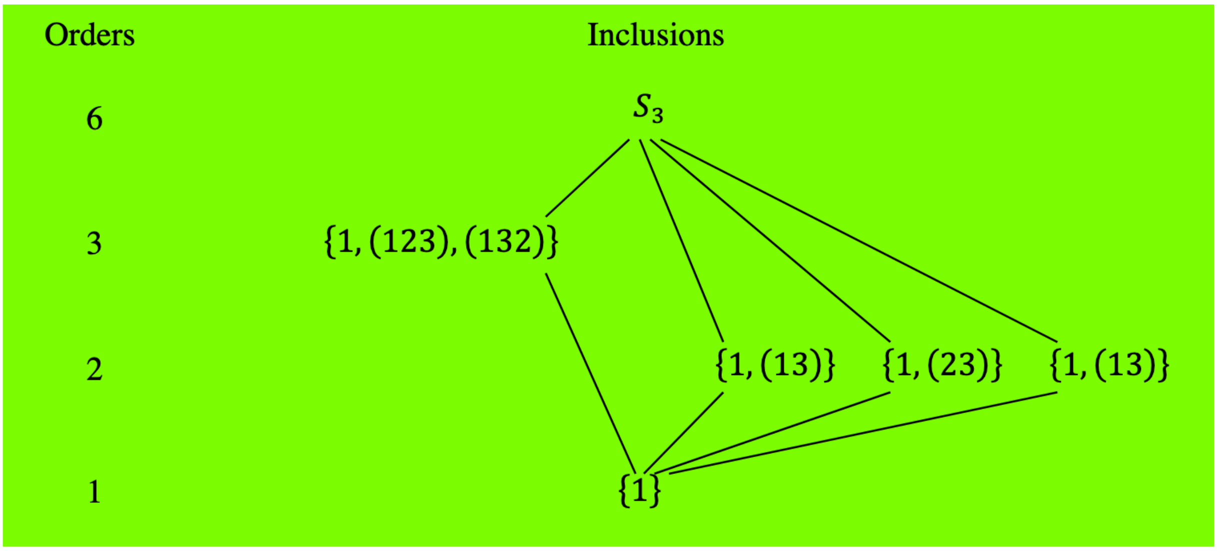
Elements

Element g	Order $o(g)$	Centralizer Z_g	Conjugacy Class $\mathcal{C}_g$
1	1	S_3	$\mathcal{C}_{(1^3)}$
(12)	2	H_2	$\mathcal{C}_{(21)}$
(23)	2	H_4	$\mathcal{C}_{(21)}$
(13)	2	H_3	$\mathcal{C}_{(21)}$
(132)	3	H_1	$\mathcal{C}_{(3)}$
(123)	3	H_1	$\mathcal{C}_{(3)}$

Generators and relations

	Generators	Relations	Realization
D_3	x, y	$x^3 = y^2 = 1$ $(xy)^2 = 1$	$x = (123)$ $y = (12)$
S_3	s_1, s_2	$s_1^2 = s_2^2 = 1$ $s_1 s_2 s_1 = s_2 s_1 s_2$	$s_1 = y = (12)$ $s_2 = x^2 y = (23)$

Subgroups



Subgroups	Structure	Normal
$H_0 = S_3$	$H_0 = S_3$	Yes
$H_1 = \{1,(132),(123)\}$	$H_1 \simeq \mu_3 \simeq A_3$	Yes
$H_2 = \{1,(12)\}$	$H_2 \simeq \mu_2$	No
$H_3 = \{1,(13)\}$	$H_3 \simeq \mu_2$	No
$H_4 = \{1,(23)\}$	$H_4 \simeq \mu_2$	No
$H_5 = \{1\}$	$H_5 = \{1\}$	Yes

Normal Subgroup	Index	Quotient Group
$H_0 = S_3$	$\mathrm{Card}(S_3/S_3) = 1$	$S_3/H_0 \simeq (1)$
$H_1 = \{1,(132),(123)\}$	$\mathrm{Card}(S_3/H_1) = 2$	$S_3/H_1 \simeq \mathbb{Z}/2\mathbb{Z}$
$H_5 = \{1\}$	$\mathrm{Card}(S_3/H_5) = 6$	$S_3/\{1\} \simeq S_3$

Subgroup H_i	Normalizer N_{H_i}	Centralizer Z_{H_i}
$H_0 = S_3$	$H_0 = S_3$	$H_5 = \{1\}$
$H_1 = \{1,(132),(123)\}$	$H_0 = S_3$	$H_1 = \{1,(132),(123)\}$
$H_2 = \{1,(12)\}$	$H_2 = \{1,(12)\}$	$H_2 = \{1,(12)\}$
$H_3 = \{1,(13)\}$	$H_3 = \{1,(13)\}$	$H_3 = \{1,(13)\}$
$H_4 = \{1,(23)\}$	$H_4 = \{1,(23)\}$	$H_4 = \{1,(23)\}$
$H_5 = \{1\}$	$H_0 = S_3$	$H_0 = S_3$

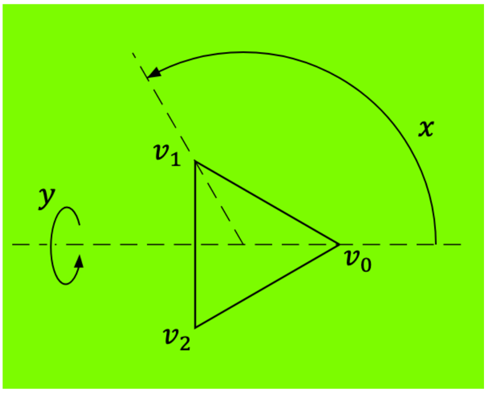
Subgroups	Cosets	Right Cosets
$H_0 = S_3$	S_3	S_3
$H_1 = \{1, (132), (123)\}$	$H_1 = \{1, (132), (123)\}$	$H_1 = \{1, (132), (123)\}$
	$(12)H_1 = \{(12), (13), (23)\}$	$H_1(12) = \{(12), (13), (23)\}$
$H_2 = \{1, (12)\}$	$H_2 = \{1, (12)\}$	$H_2 = \{1, (12)\}$
	$(23)H_2 = \{(23), (132)\}$	$H_2(23) = \{(23), (123)\}$
	$(13)H_2 = \{(13), (123)\}$	$H_2(13) = \{(13), (132)\}$
$H_3 = \{1, (13)\}$	$H_3 = \{1, (13)\}$	$H_3 = \{1, (13)\}$
	$(23)H_3 = \{(23), (123)\}$	$H_3(23) = \{(23), (132)\}$
	$(12)H_3 = \{(12), (132)\}$	$H_3(12) = \{(12), (123)\}$
$H_4 = \{1, (23)\}$	$H_4 = \{1, (23)\}$	$H_4 = \{1, (23)\}$
	$(12)H_4 = \{(12), (123)\}$	$H_4(12) = \{(12), (132)\}$
	$(13)H_4 = \{(13), (132)\}$	$H_4(13) = \{(13), (123)\}$
$H_5 = \{1\}$	$H_5 = \{1\}$	$H_5 = \{1\}$
	$(12)H_5 = \{(12)\}$	$(12)H_5 = \{(12)\}$
	$(23)H_5 = \{(23)\}$	$(23)H_5 = \{(23)\}$
	$(13)H_5 = \{(13)\}$	$(13)H_5 = \{(13)\}$
	$(132)H_5 = \{(132)\}$	$(132)H_5 = \{(132)\}$
	$(123)H_5 = \{(123)\}$	$(123)H_5 = \{(123)\}$

Some Homomorphisms

Homomorphism	Kernel	Image
$\begin{array}{rccc} \varphi_0\colon & S_3 & \to & \{1\} \\ & s_1 & \mapsto & 1 \\ & s_2 & \mapsto & 1 \end{array}$	$\ker\varphi_0 = S_3$	$\operatorname{im}\varphi_0 = \{1\}$
$\begin{array}{rccc} \epsilon\colon & S_3 & \to & \mu_2 \\ & s_1 & \mapsto & -1 \\ & s_2 & \mapsto & -1 \end{array}$	$\ker\epsilon = A_3$	$\operatorname{im}\,\epsilon = \mu_2$
$\begin{array}{rccc} \varphi_2\colon & S_3 & \to & O(3) \\ & (12) & \mapsto & \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix} \\ & (23) & \mapsto & \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix} \end{array}$	$\ker\varphi_2 = \{1\}$	$\left\{\begin{array}{cc} \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, & \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}, \\ \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}, & \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, \\ \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}, & \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix} \end{array}\right\}$
$\begin{array}{rccc} \varphi_3\colon & S_3 & \to & O(2) \\ & (12) & \mapsto & \begin{pmatrix}-1&0\\0&1\end{pmatrix} \\ & (23) & \mapsto & \begin{pmatrix}1/2&1/2\\3/2&-1/2\end{pmatrix} \end{array}$	$\ker\varphi_3 = \{1\}$	$\left\{\begin{array}{cc} \begin{pmatrix}1&0\\0&1\end{pmatrix}, & \begin{pmatrix}-1&0\\0&1\end{pmatrix}, \\ \begin{pmatrix}1/2&1/2\\3/2&-1/2\end{pmatrix}, & \begin{pmatrix}-1/2&-1/2\\3/2&-1/2\end{pmatrix}, \\ \begin{pmatrix}-1/2&1/2\\-3/2&-1/2\end{pmatrix}, & \begin{pmatrix}-1/2&-1/2\\-3/2&-1/2\end{pmatrix} \end{array}\right\}$
$\begin{array}{rccc} \varphi_4\colon & S_3 & \to & D_3 \\ & (12) & \mapsto & y \\ & (132) & \mapsto & x \end{array}$	$\ker\varphi_4 = \{1\}$	$\operatorname{im}\varphi_4 = D_3$

The group action of D_3 as rotations and reflections of an equilateral triangle

D_3 is the group of rotations and reflections of an equilateral triangle. Denote the vertices by v_i, the edge connecting vertex i to vertex j by e_{ij}, $i < j$, and the face f_{012}. Let p_{ij}, for $i, j \in \{0, 1, 2\}$, denote the point on the edge connecting v_i to v_j which is a third of the way from v_i to v_j.



Let x be the $\frac{\pi}{3}$ counterclockwise rotation about the center taking

$$v_0 \to v_1 \to v_2 \to v_0.$$

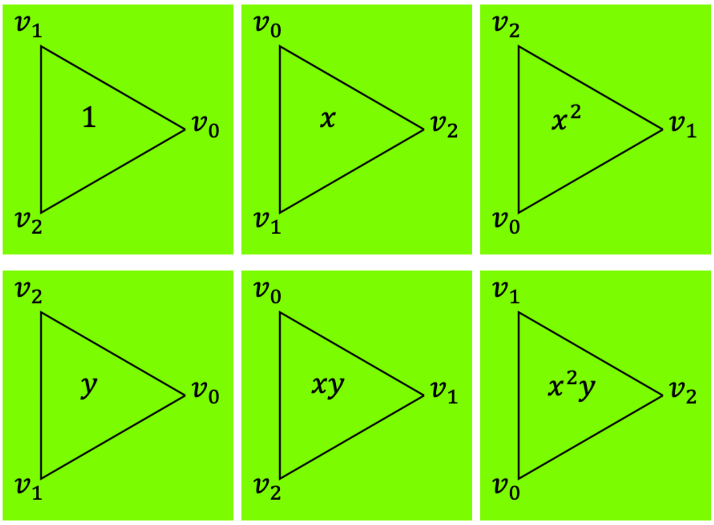
Let y be the reflection about the line connecting vertex v_0 with the midpoint of the edge e_{12}, taking

$$v_1 \to v_2 \quad \text{and fixing } v_0.$$

Note that $x^3 = 1$, $y^2 = 1$, and $yx = x^{-1}y$.
Let

$$\begin{aligned} P &= \{p_{01}, p_{10}, p_{12}, p_{21}, p_{02}, p_{20}\}, \\ V &= \{v_0, v_1, v_2\}, \\ E &= \{e_{01}, e_{12}, e_{02}\}, \qquad \text{and} \\ F &= \{f_{012}\}, \end{aligned}$$

denote the sets of points, vertices, edges, and faces, respectively. Since D_3 acts on the equilateral triangle, D_3 acts on each of these sets.



Stabilizer	Size of Stabilizer	Orbit	Size of Orbit
$(D_3)_{p_{ij}} = (1)$	1	$D_3 p_{ij} = P$	6
$(D_3)_{v_0} = \{1, y\} = H$	2	$D_3 v_0 = V$	3
$(D_3)_{v_1} = \{1, x^2y\} = xHx^{-1}$	2	$D_3 v_1 = V$	3
$(D_3)_{v_2} = \{1, xy\} = x^2Hx^{-2}$	2	$D_3 v_2 = V$	3
$(D_3)_{e_{01}} = \{1, xy\} = x^2Hx^{-2}$	2	$D_3 e_{01} = E$	3
$(D_3)_{e_{12}} = \{1, y\} = H$	2	$D_3 e_{12} = E$	3
$(D_3)_{e_{02}} = \{1, x^2y\} = xHx^{-1}$	2	$D_3 e_{02} = E$	3
$(D_3)_{f_{012}} = D_3$	6	$D_3 f_{012} = F$	1

L.4. The dihedral group D_4 of order 8

The group D_4 is as in the following table.

Set	Operation
$D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$	$x^iy^jx^ky^l = x^{(i-k) \bmod 4}y^{(j+l) \bmod 2}$

The complete multiplication table for D_4 is as follows.

Multiplication Table

	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	1	x^3	x^2	x
xy	xy	y	x^3y	x^2y	x	1	x^3	x^2
x^2y	x^2y	xy	y	x^3y	x^2	x	1	x^3
x^3y	x^3y	x^2y	xy	y	x^3	x^2	x	1

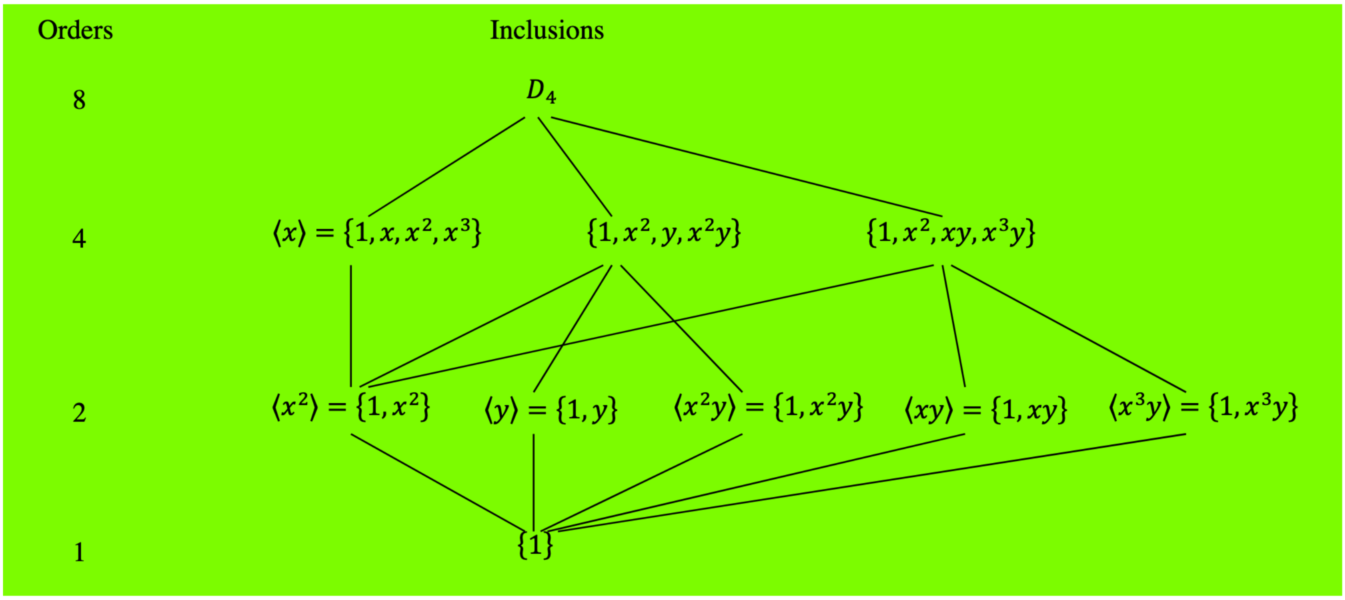
Center	Abelian	Conjugacy Classes	Subgroups
$Z(D_4) = \{1, x^2\}$	No	$\mathcal{C}_1 = \{1\}$	$H_0 = D_4$
		$\mathcal{C}_{x^2} = \{x^2\}$	$H_1 = \{1, x, x^2, x^3\}$
		$\mathcal{C}_y = \{y, x^2y\}$	$H_2 = \{1, x^2, y, x^2y\}$
		$\mathcal{C}_{xy} = \{xy, x^3y\}$	$H_3 = \{1, x^2, xy, x^3y\}$
		$\mathcal{C}_x = \{x, x^3\}$	$H_4 = \{1, x^2\}$
			$H_5 = \{1, y\}$
			$H_6 = \{1, xy\}$
			$H_7 = \{1, x^2y\}$
			$H_8 = \{1, x^3y\}$
			$H_9 = \{1\}$

Elements

Element g	Order $o(g)$	Centralizer Z_g	Conjugacy Class $\mathcal{C}_g$
1	1	D_4	$\mathcal{C}_1$
x	4	H_1	$\mathcal{C}_x$
x^2	2	D_4	$\mathcal{C}_{x^2}$
x^3	4	H_1	$\mathcal{C}_x$
y	2	H_2	$\mathcal{C}_y$
xy	2	H_3	$\mathcal{C}_{xy}$
x^2y	2	H_2	$\mathcal{C}_y$
x^3y	2	H_3	$\mathcal{C}_{xy}$

Subgroups

Subgroup Lattice


Orders
Inclusions
8
D_4
4
$\langle x\rangle = \{1, x, x^2, x^3\}$
$\{1, x^2, y, x^2y\}$
$\{1, x^2, xy, x^3y\}$
2
$\langle x^2\rangle = \{1, x^2\}$
$\langle y\rangle = \{1, y\}$
$\langle x^2y\rangle = \{1, x^2y\}$
$\langle xy\rangle = \{1, xy\}$
$\langle x^3y\rangle = \{1, x^3y\}$
1
$\{1\}$

Subgroups	Structure	Normal
$H_0 = D_4$	$H_0 = D_4$	Yes
$H_1 = \{1, x, x^2, x^3\}$	$H_1 \simeq \mu_4$	Yes
$H_2 = \{1, x^2, y, x^2y\}$	$H_2 \simeq \mu_2 \times \mu_2$	Yes
$H_3 = \{1, x^2, y, x^2y\}$	$H_3 \simeq \mu_2 \times \mu_2$	Yes
$H_4 = \{1, x^2\}$	$H_4 \simeq \mu_2$	Yes
$H_5 = \{1, y\}$	$H_5 \simeq \mu_2$	No
$H_6 = \{1, xy\}$	$H_6 \simeq \mu_2$	No
$H_7 = \{1, x^2y\}$	$H_7 \simeq \mu_2$	No
$H_8 = \{1, x^3y\}$	$H_8 \simeq \mu_2$	No
$H_9 = \{1\}$	$H_9 = \{1\}$	Yes

Normal Subgroup	Index	Quotient Group
$H_0 = D_4$	$\mathrm{Card}(D_4/D_4) = 1$	$D_4/H_0 \simeq \{1\}$
$H_1 = \{1, x, x^2, x^3\}$	$\mathrm{Card}(D_4/H_1) = 2$	$D_4/H_0 \simeq \mu_2$
$H_2 = \{1, x^2, y, x^2y\}$	$\mathrm{Card}(D_4/H_2) = 2$	$D_4/H_2 \simeq \mu_2$
$H_3 = \{1, x^2, y, x^2y\}$	$\mathrm{Card}(D_4/H_3) = 2$	$D_4/H_3 \simeq \mu_2$
$H_4 = \{1, x^2\}$	$\mathrm{Card}(D_4/H_4) = 4$	$D_4/H_4 \simeq \mu_2 \times \mu_2$
$H_9 = \{1\}$	$\mathrm{Card}(D_4/\{1\}) = 8$	$D_4/\{1\} \simeq D_4$

Subgroup H_i	Normalizer $N(H_i)$	Centralizer $Z_G(H_i)$
$H_0 = D_4$	D_4	$Z(D_4) = H_4 = \langle x^2 \rangle$
$H_1 = \langle x \rangle$	D_4	$H_1 = \langle x \rangle$
$H_2 = \langle x^2, y \rangle$	D_4	$H_2 = \langle x^2, y \rangle$
$H_3 = \langle x^2, xy \rangle$	D_4	$H_3 = \langle x^2, xy \rangle$
$H_4 = \langle x^2 \rangle$	D_4	D_4
$H_5 = \langle y \rangle$	$H_2 = \langle x^2, y \rangle$	$H_2 = \langle x^2, y \rangle$
$H_6 = \langle xy \rangle$	$H_3 = \langle x^2, xy \rangle$	$H_3 = \langle x^2, xy \rangle$
$H_7 = \langle x^2y \rangle$	$H_2 = \langle x^2, y \rangle$	$H_2 = \langle x^2, y \rangle$
$H_8 = \langle x^3y \rangle$	$H_3 = \langle x^2, xy \rangle$	$H_3 = \langle x^2, xy \rangle$
$H_9 = (1)$	D_4	D_4

Subgroups	Cosets	Right Cosets
$H_0 = D_4$	$D_4 = xD_4 = x^3D_4 = yD_4$ $= xyD_4 = x^2yD_4 = x^3yD_4$	$D_4 = D_4x = D_4x^2 = D_4x^3$ $= D_4y = D_4xy = D_4x^2y = D_4x^3y$
$H_1 = \{1, x, x^2, x^3\}$	$H_1 = xH_1 = x^2H_1 = x^3H_1$ $= \{1, x, x^2, x^3\}$ $yH_1 = xyH_1 = x^2yH_1 = x^3yH_1$ $= \{y, xy, x^2y, x^3y\}$	$H_1 = H_1x = H_1x^2 = H_1x^3$ $= \{1, x, x^2, x^3\}$ $H_1y = H_1xy = H_1x^2y = H_1x^3y$ $= \{y, xy, x^2y, x^3y\}$
$H_2 = \{1, x^2, y, x^2y\}$	$H_2 = x^2H_2 = yH_2 = x^2yH_2$ $= \{1, x^2, y, x^2y\}$ $xH_2 = x^3H_2 = xyH_2 = x^3yH_2$ $= \{x, x^3, xy, x^3y\}$	$H_2 = H_2x^2 = H_2y = H_2x^2y$ $= \{1, x^2, y, x^2y\}$ $H_2x = H_2x^3 = H_2xy = H_2x^3y$ $= \{x, x^3, xy, x^3y\}$
$H_3 = \{1, x^2, xy, x^3y\}$	$H_3 = x^2H_3 = xyH_3 = x^3yH_3$ $= \{1, x^2, xy, x^3y\}$ $xH_3 = x^3H_3 = yH_3 = x^2yH_3$ $= \{x, x^3, y, x^2y\}$	$H_3 = H_3x^2 = H_3xy = H_3x^3y$ $= \{1, x^2, xy, x^3y\}$ $H_3x = H_3x^3 = H_3y = H_3x^2y$ $= \{x, x^3, y, x^2y\}$
$H_4 = \{1, x^2\}$	$H_4 = x^2H_4 = \{1, x^2\}$ $xH_4 = x^3H_4 = \{x, x^3\}$ $yH_4 = x^2yH_4 = \{y, x^2y\}$ $xyH_4 = x^3yH_4 = \{xy, x^3y\}$	$H_4 = H_4x^2 = \{1, x^2\}$ $H_4x = H_4x^3 = \{x, x^3\}$ $H_4y = H_4x^2y = \{y, x^2y\}$ $H_4xy = H_4x^3y = \{xy, x^3y\}$
$H_5 = \{1, y\}$	$H_5 = yH_5 = \{1, y\}$ $xH_5 = xyH_5 = \{x, xy\}$ $x^2H_5 = x^2yH_5 = \{x^2, x^2y\}$ $x^3H_5 = x^3yH_5 = \{x^3, x^3y\}$	$H_5 = H_5y = \{1, y\}$ $H_5x = H_5x^3y = \{x, x^3y\}$ $H_5x^2 = H_5x^2y = \{x^2, x^2y\}$ $H_5x^3 = H_5xy = \{x^3, xy\}$
$H_6 = \{1, xy\}$	$H_6 = xyH_6 = \{1, xy\}$ $xH_6 = x^2yH_6 = \{x, x^2y\}$ $x^2H_6 = x^3yH_6 = \{x^2, x^3y\}$ $x^3H_6 = yH_6 = \{x^3, y\}$	$H_6 = H_6xy = \{1, xy\}$ $H_6x = H_6x^2y = \{x, y\}$ $H_6x^2 = H_6x^3y = \{x^2, x^3y\}$ $H_6x^3 = H_6x^2y = \{x^3, x^2y\}$
$H_7 = \{1, x^2y\}$	$H_7 = x^2yH_7 = \{1, x^2y\}$ $xH_7 = x^3yH_7 = \{x, x^3y\}$ $x^2H_7 = yH_7 = \{x^2, y\}$ $x^3H_7 = xyH_7 = \{x^3, xy\}$	$H_7 = H_7x^2y = \{1, x^2y\}$ $H_7x = H_7xy = \{x, xy\}$ $H_7x^2 = H_7y = \{x^2, y\}$ $H_7x^3 = H_7x^3y = \{x^3, x^3y\}$
$H_8 = \{1, x^3y\}$	$H_8 = x^3yH_8 = \{1, x^3y\}$ $xH_8 = yH_8 = \{x, y\}$ $x^2H_8 = xyH_8 = \{x^2, xy\}$ $x^3H_8 = x^2yH_8 = \{x^3, x^2y\}$	$H_8 = H_8x^3y = \{1, x^3y\}$ $H_8x = H_8x^2y = \{x, x^2y\}$ $H_8x^2 = H_8xy = \{x^2, xy\}$ $H_8x^3 = H_8y = \{x^3, y\}$
$H_9 = \{1\}$	$H_9 = \{1\}, xH_9 = \{x\},$ $x^2H_9 = \{x^2\}, x^3H_9 = \{x^3\}$ $yH_9 = \{y\}, xyH_9 = \{xy\},$ $x^2yH_9 = \{x^2y\}, x^3yH_9 = \{x^3y\}$	$H_9 = \{1\}, H_9x = \{x\},$ $H_9x^2 = \{x^2\}, H_9x^3 = \{x^3\}$ $H_9y = \{y\}, H_9xy = \{xy\},$ $H_9x^2y = \{x^2y\}, H_9x^3y = \{x^3y\}$

Some Homomorphisms

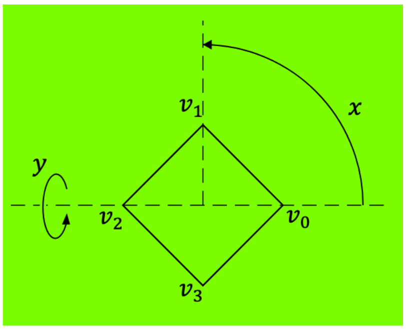
Homomorphism	Kernel	Image
$\begin{array}{rrcl} \varphi_0\colon & D_4 & \to & \{1\} \\ & x & \mapsto & 1 \\ & y & \mapsto & 1 \end{array}$	$\ker\varphi_0 = D_4$	$\operatorname{im}\varphi_0 = \{1\}$
$\begin{array}{rrcl} \varphi_1\colon & D_4 & \to & \mu_2 \\ & x & \mapsto & 1 \\ & y & \mapsto & -1 \end{array}$	$\ker\varphi_1 = H_1$	$\operatorname{im}\varphi_1 = \mu_2$
$\begin{array}{rrcl} \varphi_2\colon & D_4 & \to & \mu_2 \\ & x & \mapsto & -1 \\ & y & \mapsto & 1 \end{array}$	$\ker\varphi_2 = \{1, x^2, y, x^2y\} = H_2$	$\operatorname{im}\varphi_2 = \mu_2$
$\begin{array}{rrcl} \varphi_3\colon & D_4 & \to & \mu_2 \\ & x & \mapsto & -1 \\ & y & \mapsto & -1 \end{array}$	$\ker\varphi_3 = \{1, x^2, xy, x^3y\} = H_3$	$\operatorname{im}\varphi_3 = \mu_2$
$\begin{array}{rrcl} \varphi_4\colon & D_4 & \to & \mu_2\times\mu_2 \\ & x & \mapsto & (-1,1) \\ & y & \mapsto & (1,-1) \end{array}$	$\ker\varphi_4 = \{1, x^2\} = H_4$	$\operatorname{im}\varphi_4 = \mu_2\times\mu_2$
$\begin{array}{rrcl} \varphi_9\colon & D_4 & \to & D_4 \\ & x & \mapsto & x \\ & y & \mapsto & y \end{array}$	$\ker\varphi_9 = \{1\} = H_9$	$\operatorname{im}\varphi_9 = D_4$

Generators and relations

Generators	Relations
x, y	$x^4 = y^2 = 1$ $yx = x^{-1}y$

The group action of D_4 as rotations and reflections of a square

D_4 is the group of rotations and reflections of the square. We shall denote the vertices by v_i, the edge connecting vertex i to vertex j by e_{ij}, $i < j$, and the face f_{0123}. For all v_i and v_j connected by an edge, let p_{ij} denote the point on the edge connecting v_i to v_j which is a third of the way from v_i to v_j.



Let x be the $\frac{\pi}{2}$ counterclockwise rotation about the center taking

$$v_0 \to v_1 \to v_2 \to v_3 \to v_0.$$

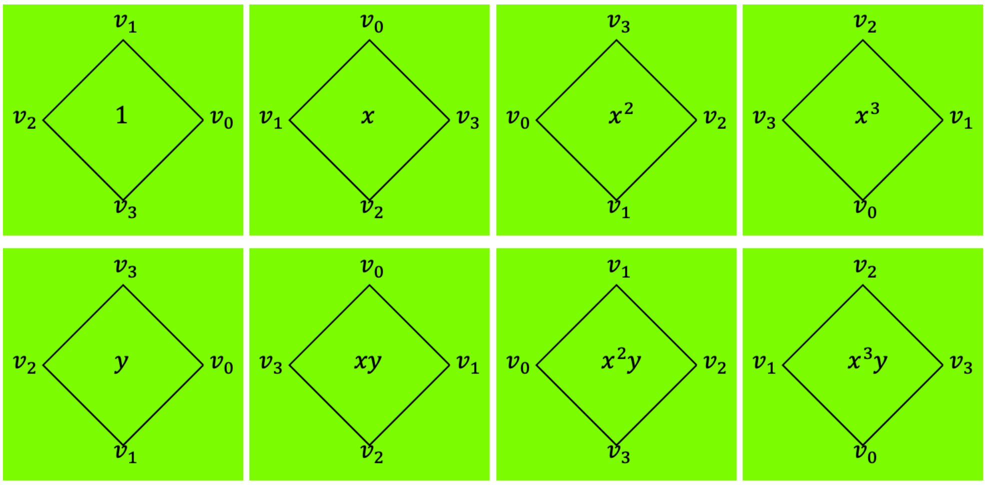
Let y be the reflection about the line connecting vertex v_0 with vertex v_2, taking

$$v_1 \to v_3 \quad \text{and fixing } v_0 \text{ and } v_2.$$

Note that $x^4 = 1$, $y^2 = 1$, and $yx = x^{-1}y$.
Let

$$\begin{aligned} P &= \{p_{01}, p_{10}, p_{12}, p_{21}, p_{23}, p_{32}, p_{03}, p_{30}\}, \\ V &= \{v_0, v_1, v_2, v_3\}, \\ E &= \{e_{01}, e_{12}, e_{23}, e_{03}\}, \qquad \text{and} \\ F &= \{f_{0123}\}, \end{aligned}$$

denote the sets of points, vertices, edges, and faces, respectively. Since D_4 acts on the square, D_4 acts on each of these sets.


v_1 v_2 1 v_0 v_3
v_0 v_1 x v_3 v_2
v_3 v_0 x^2 v_2 v_1
v_2 v_3 x^3 v_1 v_0
v_3 v_2 y v_0 v_1
v_0 v_3 xy v_1 v_2
v_1 v_0 x^2y v_2 v_3
v_2 v_1 x^3y v_3 v_0

	Size of		Size of
Stabilizer	Stabilizer	Orbit	Orbit
$(D_4)_{p_{ij}} = (1)$	1	$D_4 p_{ij} = P$	8
$(D_4)_{v_0} = \{1, y\} = H$	2	$D_4 v_0 = V$	4
$(D_4)_{v_1} = \{1, x^2 y\} = xHx^{-1}$	2	$D_4 v_1 = V$	4
$(D_4)_{v_2} = \{1, y\} = H$	2	$D_4 v_2 = V$	4
$(D_4)_{v_3} = \{1, x^2 y\} = xHx^{-1}$	2	$D_4 v_3 = V$	4
$(D_4)_{e_{01}} = \{1, xy\} = J$	2	$D_4 e_{01} = E$	4
$(D_4)_{e_{23}} = \{1, xy\} = J$	2	$D_4 e_{23} = E$	4
$(D_4)_{e_{12}} = \{1, x^3 y\} = xJx^{-1}$	2	$D_4 e_{12} = E$	4
$(D_4)_{e_{03}} = \{1, x^3 y\} = xJx^{-1}$	2	$D_4 e_{03} = E$	4
$(D_4)_{f_{0123}} = D_4$	8	$D_4 f_{0123} = F$	1

L.5. The quaternion group Q

The quaternion group Q is as in the following table. The element -1 acts like -1 in the complex numbers, it takes everything to its negative, and the negative of a negative is a positive.

Set	Operation
$Q = \{1, -1, i, -i, j, -j, k, -k\}$	$i^2 = j^2 = k^2 = ijk = -1$

The complete multiplication table for Q is as follows.

Multiplication Table

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Center	Abelian	Conjugacy Classes	Subgroups
$Z(Q) = \{1, -1\}$	No	$\mathcal{C}_1 = \{1\}$	$H_0 = Q$
		$\mathcal{C}_{-1} = \{-1\}$	$H_1 = \{\pm 1, \pm i\}$
		$\mathcal{C}_i = \{\pm i\}$	$H_2 = \{\pm 1, \pm j\}$
		$\mathcal{C}_j = \{\pm j\}$	$H_3 = \{\pm 1, \pm k\}$
		$\mathcal{C}_k = \{\pm k\}$	$H_4 = \{\pm 1\}$
			$H_5 = \{1\}$

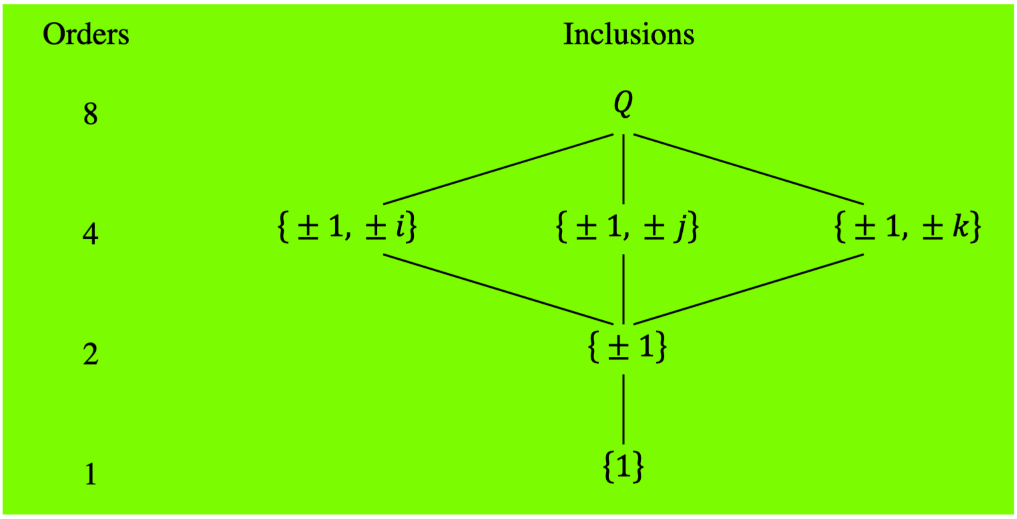
Elements

Element g	Order $o(g)$	Centralizer $Z_Q(g)$	Conjugacy Class $\mathcal{C}_g$
1	1	Q	$\mathcal{C}_1$
-1	2	Q	$\mathcal{C}_{-1}$
i	4	H_1	$\mathcal{C}_i$
$-i$	4	H_1	$\mathcal{C}_i$
j	4	H_2	$\mathcal{C}_j$
$-j$	4	H_2	$\mathcal{C}_j$
k	4	H_3	$\mathcal{C}_k$
$-k$	4	H_3	$\mathcal{C}_k$

Subgroups

Subgroups	Structure	Index	Normal	Quotient Group
$H_0 = Q$	$H_0 = Q$	$\mathrm{Card}(Q/Q) = 1$	Yes	$Q/H_0 \simeq (1)$
$H_1 = \{\pm 1, \pm i\}$	$H_1 \simeq \mu_4$	$\mathrm{Card}(Q/H_1) = 2$	Yes	$Q/H_1 \simeq Z_2$
$H_2 = \{\pm 1, \pm j\}$	$H_2 \simeq \mu_4$	$\mathrm{Card}(Q/H_2) = 2$	Yes	$Q/H_2 \simeq \mu_2$
$H_3 = \{\pm 1, \pm k\}$	$H_3 \simeq \mu_4$	$\mathrm{Card}(Q/H_3) = 2$	Yes	$Q/H_3 \simeq \mu_2$
$H_4 = \{\pm 1\}$	$H_4 \simeq \mu_2$	$\mathrm{Card}(Q/H_4) = 4$	Yes	$Q/H_4 \simeq \mu_2 \times \mu_2$
$H_5 = \{1\}$	$H_5 = \{1\}$	$\mathrm{Card}(Q/H_5) = 8$	Yes	$Q/(1) \simeq Q$

Subgroup Lattice



Subgroup H_i	Normalizer $N(H_i)$	Centralizer $Z_G(H_i)$
$H_0 = Q$	Q	$H_4 = \{\pm 1\}$
$H_1 = \langle i \rangle$	Q	$H_1 = \langle i \rangle$
$H_2 = \langle j \rangle$	Q	$H_2 = \langle j \rangle$
$H_3 = \langle k \rangle$	Q	$H_3 = \langle k \rangle$
$H_4 = \{\pm 1\}$	Q	Q
$H_5 = (1)$	Q	Q

Subgroups	Cosets	Right Cosets
$H_0 = Q$	Q	Q
$H_1 = \{\pm 1, \pm i\}$	$H_1 = \{\pm 1, \pm i\}$	$H_1 = \{\pm 1, \pm i\}$
	$jH_1 = \{\pm j, \pm k\}$	$H_1 j = \{\pm j, \pm k\}$
$H_2 = \{\pm 1, \pm j\}$	$H_2 = \{\pm 1, \pm j\}$	$H_2 = \{\pm 1, \pm j\}$
	$iH_2 = \{\pm i, \pm k\}$	$H_2 i = \{\pm i, \pm k\}$
$H_3 = \{\pm 1, \pm k\}$	$H_3 = \{\pm 1, \pm k\}$	$H_3 = \{\pm 1, \pm k\}$
	$iH_3 = \{\pm i, \pm j\}$	$H_3 i = \{\pm i, \pm j\}$
$H_4 = \{\pm 1\}$	$H_4 = \{\pm 1\}$	$H_4 = \{\pm 1\}$
	$iH_4 = \{\pm i\}$	$H_4 i = \{\pm i\}$
	$jH_4 = \{\pm j\}$	$H_4 j = \{\pm j\}$
	$kH_4 = \{\pm k\}$	$H_4 k = \{\pm k\}$
$H_5 = \{1\}$	$H_5 = \{1\}$	$H_5 = \{1\}$
	$(-1)H_5 = \{-1\}$	$H_5(-1) = \{-1\}$
	$iH_5 = \{i\}$	$H_5 i = \{i\}$
	$-iH_5 = \{-i\}$	$H_5(-i) = \{-i\}$
	$jH_5 = \{j\}$	$H_5 j = \{j\}$
	$-jH_5 = \{-j\}$	$H_5(-j) = \{-j\}$
	$kH_5 = \{k\}$	$H_5 k = \{k\}$
	$-kH_5 = \{-k\}$	$H_5(-k) = \{-k\}$

Generators and relations

Generators	Relations	Realization
S, T	$S^2 = T^2 = (ST)^2$	$S = i, T = j, ST = k$

Some Homomorphisms

Homomorphism	Kernel	Image
$\begin{array}{rrcl} \varphi_0\colon & Q & \to & (1) \\ & i & \mapsto & 1 \\ & j & \mapsto & 1 \end{array}$	$\ker\varphi_0 = Q$	$\mathrm{im}\varphi_0 = (1)$
$\begin{array}{rrcl} \varphi_1\colon & Q & \to & Z_2 \\ & i & \mapsto & 1 \\ & j & \mapsto & -1 \end{array}$	$\ker\varphi_1 = H_1 = \{\pm 1, \pm i\}$	$\mathrm{im}\varphi_1 = Z_2$
$\begin{array}{rrcl} \varphi_2\colon & Q & \to & Z_2 \\ & i & \mapsto & -1 \\ & j & \mapsto & 1 \end{array}$	$\ker\varphi_2 = H_2 = \{\pm 1, \pm j\}$	$\mathrm{im}\ \varphi_2 = Z_2$
$\begin{array}{rrcl} \varphi_3\colon & Q & \to & Z_2 \\ & i & \mapsto & -1 \\ & j & \mapsto & -1 \end{array}$	$\ker\varphi_3 = H_3 = \{\pm 1, \pm k\}$	$\mathrm{im}\varphi_3 = Z_2$
$\begin{array}{rrcc} \varphi_4\colon & Q & \to & Gl_2(\mathbb{C}) \\ & i & \mapsto & \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ & j & \mapsto & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ & k & \mapsto & \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \end{array}$	$\ker\varphi_4 = H_5 = (1)$	$\mathrm{im}\ \varphi_4 = \left\{ \begin{matrix} \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix}, \\ \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix} \end{matrix} \right\}$
$\begin{array}{rrcl} \varphi_5\colon & Q & \to & Z_2 \times Z_2 \\ & i & \mapsto & (-1, 1) \\ & j & \mapsto & (1, -1) \end{array}$	$\ker\varphi_5 = H_4 = \{\pm 1\}$	$\mathrm{im}\ \varphi_5 = Z_2 \times Z_2$

L.6. The tetrahedral group A_4

The group A_4 can be given in at least two natural ways. In the following tables we shall use one-line notation to represent the permutations in A_4.

Set	Operation
even permutations in S_4	composition of permutations
rotations preserving a tetrahedron	composition of rotations

Center	Abelian	Conjugacy Classes
$Z(A_4) = \{(1234)\}$	No	$\mathcal{C}_{(1^4)} = \{(1234)\}$ $\mathcal{C}_{(2^2)} = \{(2143), (3412), (4321)\}$ $\mathcal{C}_{(31)^+} = \{(3124), (4213), (2431), (1342)\}$ $\mathcal{C}_{(31)^-} = \{(2314), (3241), (4132), (1423)\}$

Elements

Element g	Order $o(g)$	Centralizer $Z(g)$	Conjugacy Class $\mathcal{C}_g$
(1234)	1	A_4	$\mathcal{C}_{(1^4)}$
(2143)	2	H_1	$\mathcal{C}_{2^2}$
(3412)	2	H_1	$\mathcal{C}_{2^2}$
(4321)	2	H_1	$\mathcal{C}_{2^2}$
(3124)	3	H_2	$\mathcal{C}_{(31)^+}$
(4213)	3	H_4	$\mathcal{C}_{(31)^+}$
(2431)	3	H_3	$\mathcal{C}_{(31)^+}$
(1342)	3	H_5	$\mathcal{C}_{(31)^+}$
(2314)	3	H_2	$\mathcal{C}_{(31)^-}$
(3241)	3	H_4	$\mathcal{C}_{(31)^-}$
(4132)	3	H_3	$\mathcal{C}_{(31)^-}$
(1423)	3	H_5	$\mathcal{C}_{(31)^-}$

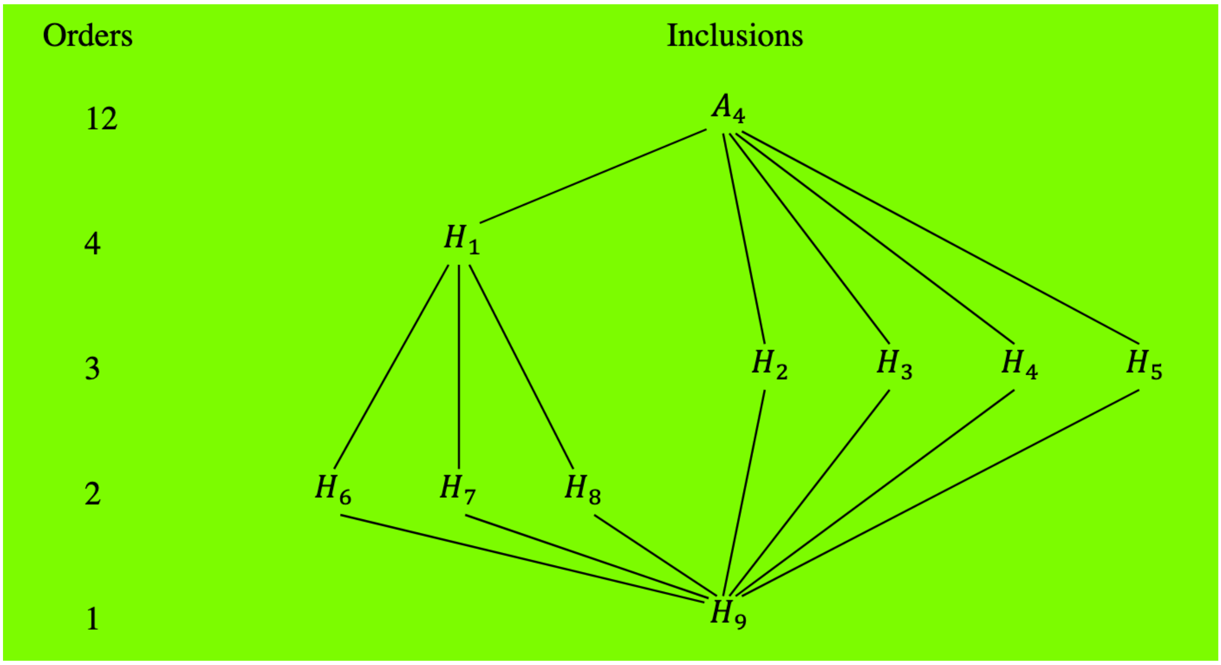
Generators and relations

Generators	Relations	Realization
S, T	$S^3 = T^2 = (ST)^3 = 1$	$S = (2314), T = (2143)$

Subgroups

Subgroups	Structure	Index	Normal
$H_0 = A_4$	$H_0 = A_4$	$\mathrm{Card}(A_4/A_4) = 1$	Yes
$H_1 = \{(1234), (2143), (3412), (4321)\}$	$H_1 \simeq \mu_2 \times \mu_2$	$\mathrm{Card}(A_4/H_1) = 3$	Yes
$H_2 = \{(1234), (3124), (2314)\}$	$H_2 \simeq \mu_3$	$\mathrm{Card}(A_4/H_2) = 4$	No
$H_3 = \{(1234), (4132), (2431)\}$	$H_3 \simeq \mu_3$	$\mathrm{Card}(A_4/H_3) = 4$	No
$H_4 = \{(1234), (4213), (3241)\}$	$H_4 \simeq \mu_3$	$\mathrm{Card}(A_4/H_4) = 4$	No
$H_5 = \{(1234), (1423), (1342)\}$	$H_5 \simeq \mu_3$	$\mathrm{Card}(A_4/H_5) = 4$	No
$H_6 = \{(1234), (3412)\}$	$H_6 \simeq \mu_2$	$\mathrm{Card}(A_4/H_6) = 6$	No
$H_7 = \{(1234), (2143)\}$	$H_7 \simeq \mu_2$	$\mathrm{Card}(A_4/H_7) = 6$	No
$H_8 = \{(1234), (4321)\}$	$H_8 \simeq \mu_2$	$\mathrm{Card}(A_4/H_8) = 6$	No
$H_9 = \{(1234)\}$	$H_9 \simeq (1)$	$[A_4 : H_9] = 12$	Yes

Subgroup Lattice



Normal Subgroup	Index	Quotient Group
$H_0 = A_4$	$\mathrm{Card}(A4/A_4) = 1$	$A_4/A_4 \simeq \{1\}$
$H_1 = \{(1234), (2143), (3412), (4321)\}$	$\mathrm{Card}(A_4/H_1) = 3$	$A_4/H_1 \simeq \mu_3$
$H_9 = \{(1234)\}$	$\mathrm{Card}(A_4/H_9) = 12$	$A_4/\{1\} \simeq A_4$

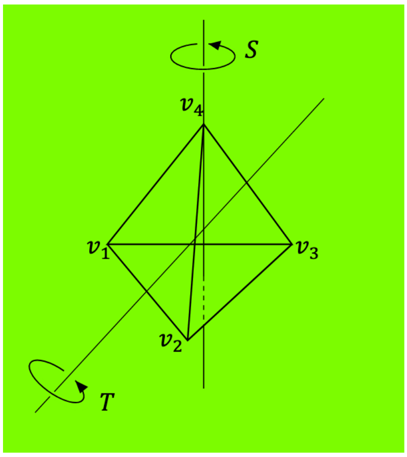
Some Homomorphisms

Let ξ be the primitive cube root of 1 given by $\xi = e^{2\pi i/3} \in \mathbb{C}$.

Homomorphism	Kernel
$\begin{array}{lccc} \varphi_0\colon & A_4 & \to & (1) \\ & S & \mapsto & 1 \\ & T & \mapsto & 1 \end{array}$	$\ker\varphi_0 = A_4$
$\begin{array}{lccc} \varphi_1\colon & A_4 & \to & \mu_3 \\ & S & \mapsto & \xi \\ & T & \mapsto & 1 \end{array}$	$\ker\varphi_1 = H_1$
$\begin{array}{lccc} \varphi_2\colon & A_4 & \to & \mu_3 \\ & S & \mapsto & \xi^2 \\ & T & \mapsto & 1 \end{array}$	$\ker\varphi_2 = H_1$
$\begin{array}{lccc} \varphi_3\colon & A_4 & \to & GL(3) \\ & S & \mapsto & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & -3/2 \\ 0 & 1/2 & -1/2 \end{pmatrix} \\ r & T & \mapsto & \begin{pmatrix} -1/3 & -4/3 & 0 \\ -2/3 & 1/3 & 0 \\ 0 & 0 & -1 \end{pmatrix} \end{array}$	$\ker\varphi_3 = (1)$

The group action of A_4 as rotations of a tetrahedron

A_4 is the group of rotations of the tetrahedron. We shall denote the vertices by v_i, the edge connecting vertex i to vertex j by e_{ij}, $i < j$, and the face adjacent to the three vertices v_i, v_j, v_k, by f_{ijk}, $i < j < k$. Let r_{1234} denote the region determined by the inside of the tetrahedron. Let p_{ij}, $1 \leqslant i, j \leqslant 4$ denote the point on the edge connecting v_i to v_j which is a third of the way from v_i to v_j.



Let S be the 60° rotation about the bottom face taking

$$v_1 \to v_2 \to v_3 \to v_1 \quad \text{and fixing } v_4.$$

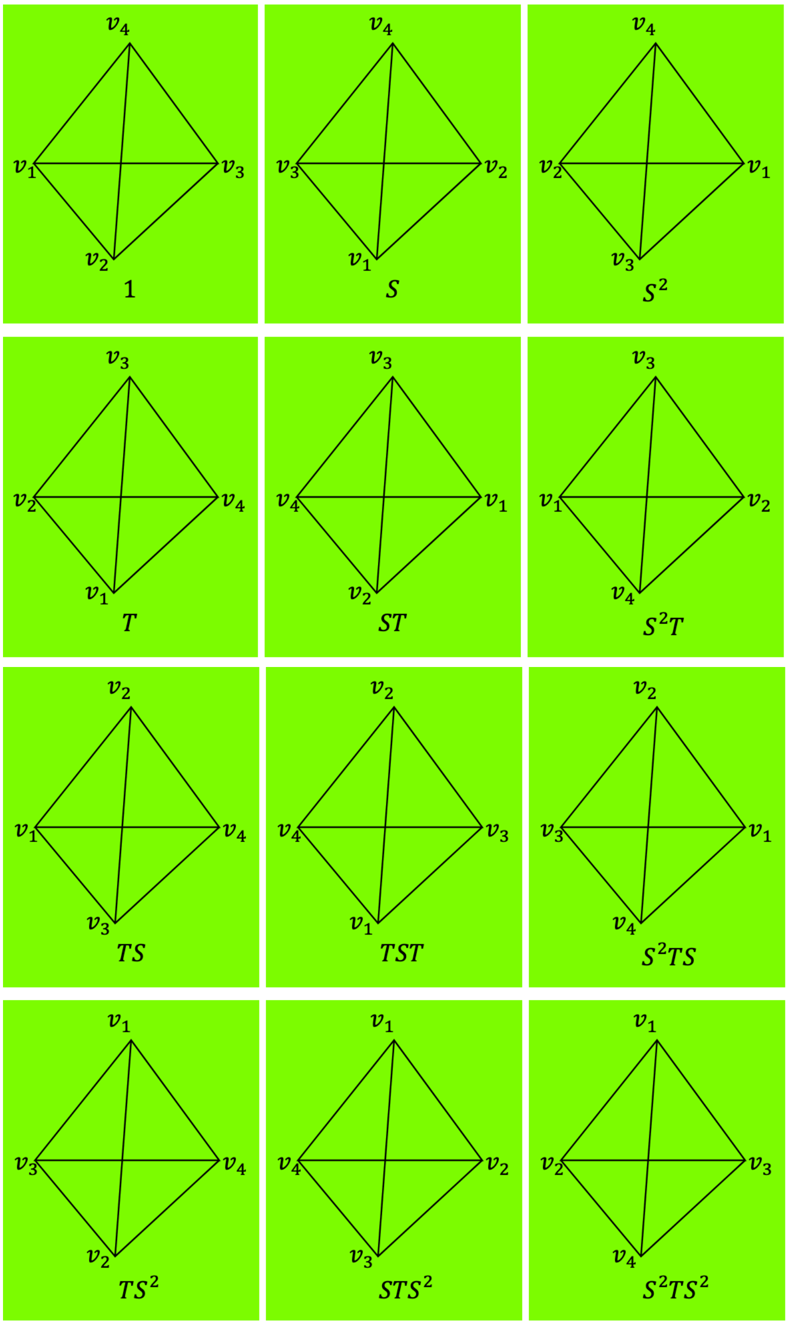
Let T be the 180° rotation about the line connecting the midpoint of edge e_{34} with the midpoint of edge e_{12}, taking

$$v_1 \to v_2 \quad \text{and} \quad v_3 \to v_4.$$

Note that $S^3 = 1$, $T^2 = 1$, and $(ST)^3 = 1$.
Let

$$\begin{aligned} P &= \{p_{ij} \mid 1 \leqslant i, j \leqslant 4\}, \\ V &= \{v_1, v_2, v_3, v_4\}, \\ E &= \{e_{12}, e_{13}, e_{14}, e_{23}, e_{24}, e_{34}\}, \\ F &= \{f_{123}, f_{124}, f_{134}, f_{234}\}, \qquad \text{and} \\ R &= \{r_{1234}\}, \end{aligned}$$

denote the sets of points, vertices, edges, faces, and regions, respectively. Since A_4 acts on the tetrahedron, A_4 acts on each of these sets.


v_4 v_1 v_3 v_2
1
v_4 v_3 v_2 v_1
S
v_4 v_2 v_1 v_3
S^2
v_3 v_2 v_4 v_1
T
v_3 v_4 v_1 v_2
ST
v_3 v_1 v_2 v_4
S^2T
v_2 v_1 v_4 v_3
TS
v_2 v_4 v_3 v_1
TST
v_2 v_3 v_1 v_4
S^2TS
v_1 v_3 v_4 v_2
TS^2
v_1 v_4 v_2 v_3
STS^2
v_1 v_2 v_3 v_4
S^2TS^2

Stabilizer	Size of Stabilizer	Orbit	Size of Orbit
$(A_4)_{p_{ij}} = (1)$	1	$A_4 p_{ij} = P$	12
$(A_4)_{v_4} = \{1, S, S^2\} = H$	3	$A_4 v_4 = V$	4
$(A_4)_{v_3} = \{1, TST^{-1}, TS^2T^{-1}\} = THT^{-1}$	3	$A_4 v_3 = V$	4
$(A_4)_{v_1} = \{1, TS, S^2T\} = (ST)H(ST)^{-1}$	3	$A_4 v_1 = V$	4
$(A_4)_{v_2} = \{1, ST, (ST)^2\} = (S^2T)H(S^2T)^{-1}$	3	$A_4 v_2 = V$	4
$(A_4)_{e_{12}} = \{1, T\}$	2	$A_4 e_{12} = E$	6
$(A_4)_{e_{34}} = \{1, T\}$	2	$A_4 e_{34} = E$	6
$(A_4)_{e_{14}} = \{1, STS^{-1}\}$	2	$A_4 e_{14} = E$	6
$(A_4)_{e_{23}} = \{1, STS^{-1}\}$	2	$A_4 e_{23} = E$	6
$(A_4)_{e_{13}} = \{1, S^2TS^{-2}\}$	2	$A_4 e_{13} = E$	6
$(A_4)_{e_{24}} = \{1, S^2TS^{-2}\}$	2	$A_4 e_{24} = E$	6
$(A_4)_{f_{123}} = \{1, S, S^2\}$	3	$A_4 f_{123} = F$	4
$(A_4)_{f_{124}} = \{1, TST^{-1}, TS^2T^{-1}\}$	3	$A_4 f_{124} = F$	4
$(A_4)_{f_{234}} = \{1, (ST)S(ST)^{-1}, (ST)S^2(ST)^{-1}\}$	3	$A_4 f_{234} = F$	4
$(A_4)_{f_{134}} = \{1, (S^2T)S(S^2T)^{-1}, (S^2T)S^2(S^2T)^{-1}\}$	3	$A_4 f_{134} = F$	4
$(A_4)_{r_{1234}} = A_4$	12	$A_4 r_{1234} = R$	1

L.7. The octahedral group S_4

The group S_4 can be represented in several different ways. Some of these are given in the following table.

Set	Operation
permutations of 4 elements	composition of permutations
rotations preserving a cube	composition of rotations
rotations preserving an octahedron	composition of rotations

The complete multiplication table for S_4 is a 24 × 24 matrix. This matrix is too big to include here.

In the following tables we shall use one-line notation to represent the permutations in S_4.

Center	Conjugacy classes
$Z(S_4) = \{1, -1\}$	$\mathcal{C}_{(1^4)} = \{(1234)\}$ $\mathcal{C}_{(21^2)} = \{(2134), (3214), (4231)(1324), (1432), (1243)\}$ $\mathcal{C}_{(2^2)} = \{(2143), (3412), (4321)\}$ $\mathcal{C}_{(31)} = \{(3124), (4132), (4213), (1423)(2314), (2431), (3241), (1342)\}$ $\mathcal{C}_{(4)} = \{(4123), (3142), (2413), (4312), (2341), (3421)\}$

Subgroups

There are more than 30 subgroups of the group S_4. We shall not give a list of all of the subgroups and we shall not give a subgroup lattice here. The following table lists only the normal subgroups of S_4.

Normal subgroup	Structure	Quotient Group
$N_0 = S_4$	$N_0 = S_4$	$S_4/S_4 \simeq (1)$
$N_1 = A_4$	$N_1 = A_4$	$S_4/A_4 \simeq \mu_2$
$N_2 = \left\{ \begin{array}{c} (1234), (2143), \\ (3412), (4321) \end{array} \right\}$	$N_2 \simeq \mu_2 \times \mu_2$	$S_4/N_2 \simeq S_3$
$N_3 = \{(1234)\}$	$N_3 \simeq \{1\}$	$S_4/\{1\} \simeq S_4$

Generators and relations

The following table gives two useful presentations of the octahedral group S_4.

Generators	Relations	Realization
S, T	$S^4 = T^2 = (ST)^3 = 1$	$S = (4123), T = 4231$
s_1, s_2, s_3	$s_1^2 = s_2^2 = s_3^2 = 1$ $s_1 s_2 s_1 = s_2 s_1 s_2$ $s_2 s_3 s_2 = s_3 s_2 s_3$	$s_1 = (2134)$ $s_2 = (1324)$ $s_3 = (1243)$

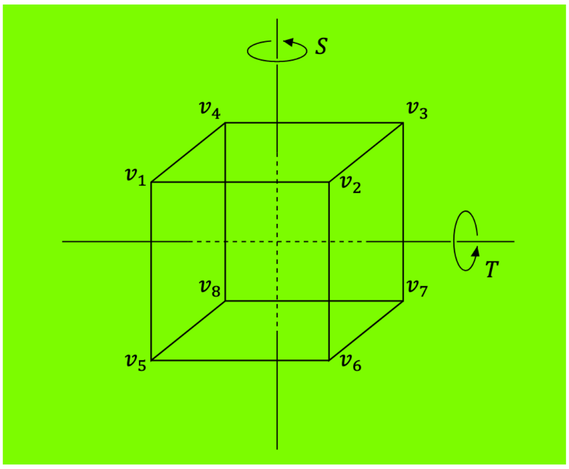
Some Homomorphisms

In the following table $s_1 = (2134)$, $s_2 = (1324)$, $s_3 = (1243)$ denote the simple transpositions in the group S_4. These simple transpositions generate S_4. Note also that the homomorphism labeled $\phi_{(1^4)}$ is the sign homomorphism ε of the symmetric group S_4.

Homomorphism	Kernel
$\begin{array}{llcl} \varphi\colon & S_4 & \to & S_3 \\ & s_1 & \mapsto & (213) \\ & s_2 & \mapsto & (132) \\ & s_3 & \mapsto & (213) \end{array}$	$\ker\varphi = N_2$
$\begin{array}{llcl} \varphi_{(4)}\colon & S_4 & \to & (1) \\ & s_1 & \mapsto & 1 \\ & s_2 & \mapsto & 1 \\ & s_3 & \mapsto & 1 \end{array}$	$\ker\varphi_{(4)} = S_4$
$\begin{array}{llcl} \varphi_{(1^4)}\colon & S_4 & \to & Z_2 \\ & s_1 & \mapsto & -1 \\ & s_2 & \mapsto & -1 \\ & s_3 & \mapsto & -1 \end{array}$	$\ker\varphi_{(1^4)} = A_4$
$\begin{array}{llcc} \varphi_{(21^2)}\colon & S_4 & \to & GL_3 \\ & s_1 & \mapsto & \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ & s_2 & \mapsto & \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1/2 & 3/2 \\ 0 & 1/2 & -1/2 \end{pmatrix} \\ & s_3 & \mapsto & \begin{pmatrix} 1/3 & 4/3 & 0 \\ 2/3 & -1/3 & 0 \\ 0 & 0 & -1 \end{pmatrix} \end{array}$	$\ker\varphi_{(21^2)} = (1)$
$\begin{array}{llcc} \varphi_{31}\colon & S_4 & \to & GL_3 \\ & s_1 & \mapsto & \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ & s_2 & \mapsto & \begin{pmatrix} 1/2 & 3/2 & 0 \\ 1/2 & -1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ & s_3 & \mapsto & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/3 & 4/3 \\ 0 & 2/3 & -1/3 \end{pmatrix} \end{array}$	$\ker\varphi_{(31)} = (1)$
$\begin{array}{llcc} \varphi_{(22)}\colon & S_4 & \to & GL(2) \\ & s_1 & \mapsto & \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ & s_2 & \mapsto & \begin{pmatrix} 1/2 & 3/2 \\ 1/2 & -1/2 \end{pmatrix} \\ & s_3 & \mapsto & \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \end{array}$	$\ker\varphi_{(22)} = N_2$

The group action of S_4 as rotations of a cube

S_4 is the group of rotations of the cube. We shall denote the vertices by v_i, the edge connecting vertex i to vertex j by e_{ij}, $i < j$, and the face adjacent to the four vertices v_i, v_j, v_k, v_l, by f_{ijkl}, $i < j < k < l$. Let $r_{12345678}$ denote the region determined by the inside of the cube. For all v_i and v_j connected by an edge, let p_{ij}, denote the point on the edge connecting v_i to v_j which is a third of the way from v_i to v_j.



Let S be the 90° rotation about the top face taking

$$v_1 \to v_2 \to v_3 \to v_4 \to v_1 \quad \text{and} \quad v_5 \to v_6 \to v_7 \to v_8 \to v_5.$$

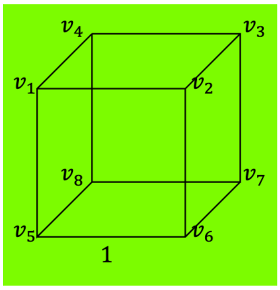
Let T be the rotation 90° about the right face taking

$$v_4 \to v_1 \to v_5 \to v_8 \quad \text{and} \quad v_3 \to v_2 \to v_6 \to v_7.$$

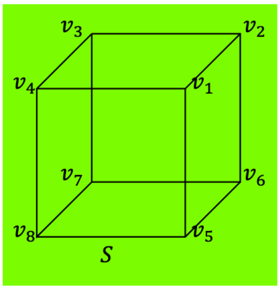
Let

$$\begin{aligned} P &= \{p_{ij} \mid 1 \leqslant i, j \leqslant 8\}, \\ V &= \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}, \\ E &= \{e_{12}, e_{23}, e_{34}, e_{14}, e_{15}, e_{48}, e_{26}, e_{37}, e_{56}, e_{67}, e_{78}, e_{58}\}, \\ F &= \{f_{1234}, f_{5678}, f_{1256}, f_{3478}, f_{1458}, f_{2367}\}, \qquad \text{and} \\ R &= \{r_{12345678}\}, \end{aligned}$$

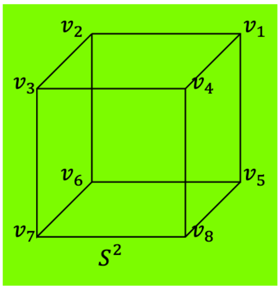
denote the sets of points, vertices, edges, faces, and regions, respectively. Since S_4 acts on the cube, S_4 acts on each of these sets.



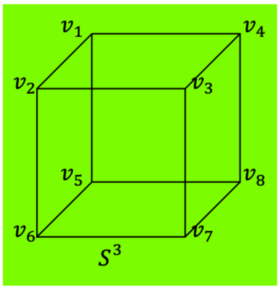
1



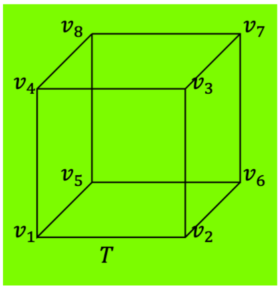
S



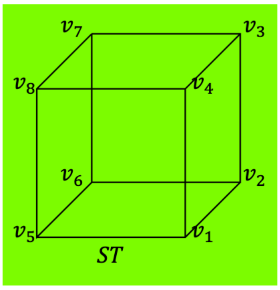
S^2



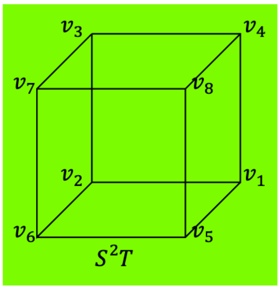
S^3



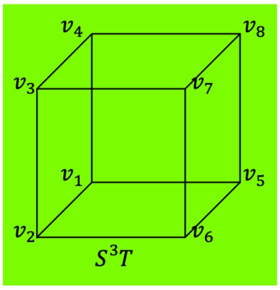
T



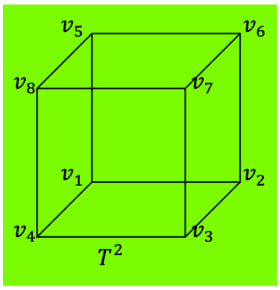
ST



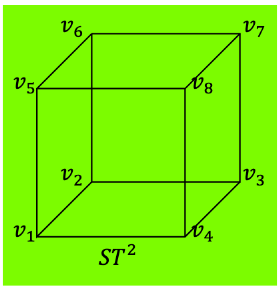
S^2T



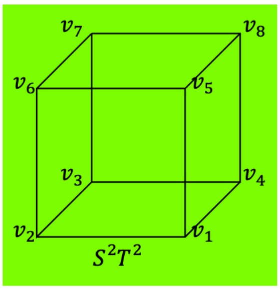
S^3T



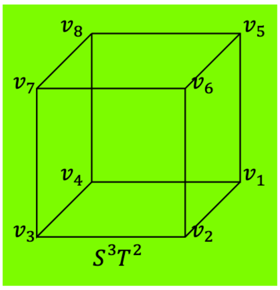
T^2



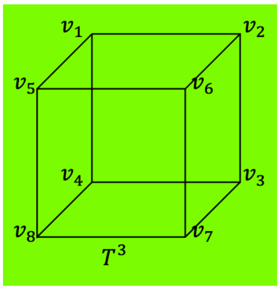
ST^2



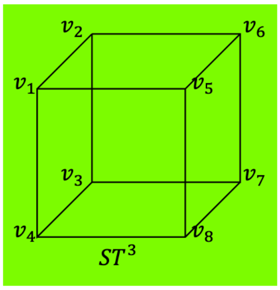
S^2T^2



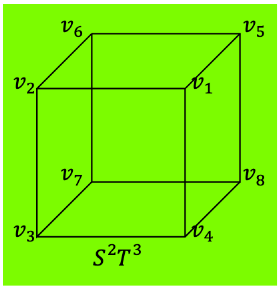
S^3T^2



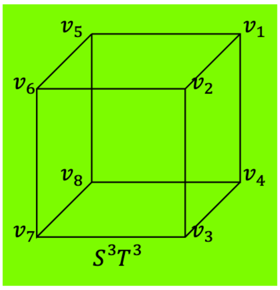
T^3



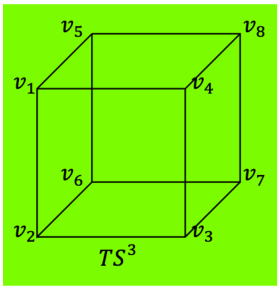
ST^3



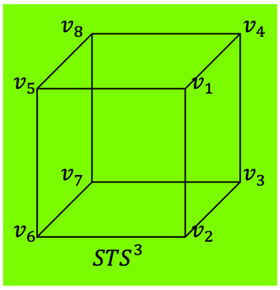
S^2T^3



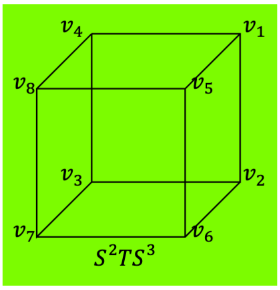
S^3T^3



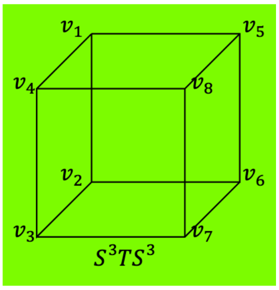
TS^3



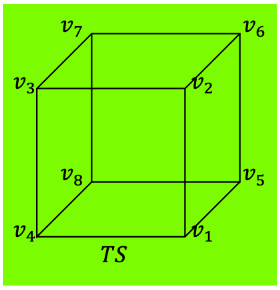
STS^3



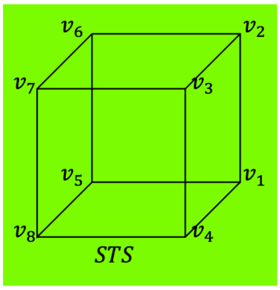
S^2TS^3



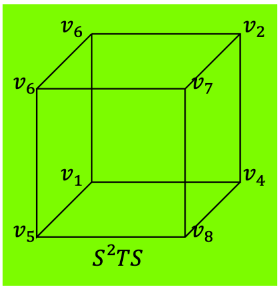
S^3TS^3



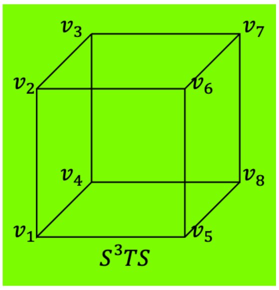
TS



STS



S^2TS



S^3TS

Stabilizer	Size of Stabilizer	Orbit	Size of Orbit
$(S_4)_{p_{ij}} = (1)$	1	$S_4 p_{ij} = P$	24
$(S_4)_{v_1} = \{1, T^3S, TS^3\} = H$	3	$S_4 v_1 = V$	8
$(S_4)_{v_7} = \{1, T^3S, TS^3\} = H$	3	$S_4 v_7 = V$	8
$(S_4)_{v_2} = \{1, S^3T^3, TS\} = SHS^{-1}$	3	$S_4 v_2 = V$	8
$(S_4)_{v_8} = \{1, S^3T^3, TS\} = SHS^{-1}$	3	$S_4 v_8 = V$	8
$(S_4)_{v_3} = \{1, ST, S^2TS\} = S^2HS^{-2}$	3	$S_4 v_3 = V$	8
$(S_4)_{v_5} = \{1, ST, S^2TS\} = S^2HS^{-2}$	3	$S_4 v_5 = V$	8
$(S_4)_{v_4} = \{1, S^3T, S^2TS^3\} = S^3HS^{-3}$	3	$S_4 v_4 = V$	8
$(S_4)_{v_6} = \{1, S^3T, S^2TS^3\} = S^3HS^{-3}$	3	$S_4 v_6 = V$	8
$(S_4)_{e_{12}} = \{1, TS^2\} = J$	2	$S_4 e_{12} = E$	12
$(S_4)_{e_{78}} = \{1, TS^2\} = J$	2	$S_4 e_{78} = E$	12
$(S_4)_{e_{23}} = \{1, STS\} = SJS^{-1}$	2	$S_4 e_{23} = E$	12
$(S_4)_{e_{58}} = \{1, STS\} = SJS^{-1}$	2	$S_4 e_{58} = E$	12
$(S_4)_{e_{34}} = \{1, S^2T\} = S^2JS^{-2}$	2	$S_4 e_{34} = E$	12
$(S_4)_{e_{56}} = \{1, S^2T\} = S^2JS^{-2}$	2	$S_4 e_{56} = E$	12
$(S_4)_{e_{14}} = \{1, S^3TS^3\} = S^3JS^{-3}$	2	$S_4 e_{14} = E$	12
$(S_4)_{e_{67}} = \{1, S^3TS^3\} = S^3JS^{-3}$	2	$S_4 e_{67} = E$	12
$(S_4)_{e_{15}} = \{1, ST^2\} = (ST^3)J(ST^3)^{-1}$	2	$S_4 e_{15} = E$	12
$(S_4)_{e_{37}} = \{1, ST^2\} = (ST^3)J(ST^3)^{-1}$	2	$S_4 e_{37} = E$	12
$(S_4)_{e_{48}} = \{1, S^3T^2\} = (S^3TS)J(S^3TS)^{-1}$	2	$S_4 e_{48} = E$	12
$(S_4)_{e_{26}} = \{1, S^3T^2\} = (S^3TS)J(S^3TS)^{-1}$	2	$S_4 e_{26} = E$	12
$(S_4)_{f_{1234}} = \{1, S, S^2, S^3\} = K$	4	$S_4 f_{1234} = F$	6
$(S_4)_{f_{5678}} = \{1, S, S^2, S^3\} = K$	4	$S_4 f_{5678} = F$	6
$(S_4)_{f_{1256}} = \{1, S^2T^2, S^3TS, STS^3\} = TKT^{-1}$	4	$S_4 f_{1256} = F$	6
$(S_4)_{f_{3478}} = \{1, S^2T^2, S^3TS, STS^3\} = TKT^{-1}$	4	$S_4 f_{3478} = F$	6
$(S_4)_{f_{1458}} = \{1, T, T^2, T^3\} = (ST^3)K(ST^3)^{-1}$	4	$S_4 f_{1458} = F$	6
$(S_4)_{f_{2367}} = \{1, T, T^2, T^3\} = (ST^3)K(ST^3)^{-1}$	4	$S_4 f_{2367} = F$	6
$(S_4)_{r_{12345678}} = S_4$	24	$S_4 r_{12345678} = R$	1

CHAPTER C

COMMUTATIVE RINGS

C.1. Euclidean Domains, PIDs and UFDs

C.1.1. R is a Euclidean domain $\Longrightarrow$ R is a PID. —

Definition C.1.1. — Let $\mathbb{Z}_{\geqslant 0} = \{0, 1, 2, \ldots\}$ be the set of nonnegative integers.

- A **Euclidean domain** is an integral domain R with a function
$$\sigma\colon R - \{0\} \to \mathbb{Z}_{\geqslant 0}, \qquad \text{a } \textbf{size function}$$
such that if $a, b \in R$ and $a \neq 0$ then there exist $q, r \in R$ such that
$$b = aq + r, \qquad \text{where either } r = 0 \text{ or } \sigma(r) < \sigma(a).$$
- Let R be a commutative ring. A **principal ideal** is an ideal generated by a single element.
- A **principal ideal domain** (or **PID**) is an integral domain for which every ideal is principal.

Theorem C.1.1. — *A Euclidean domain is a principal ideal domain.*

C.1.2. R is a PID $\Longrightarrow$ R is a UFD. —

Definition C.1.2. — Let R be an integral domain.

- A **unit** is an element $a \in R$ such that there exists an element $b \in R$ such that $ab = 1$.
- Let $p, q \in R$. The element p **divides** q if there exists $a \in R$ such that $q = ap$.
- Let $p, q \in R$. The element p is a **proper divisor** of q if p is not a unit and there exists a nonunit $a \in R$ such that $q = ap$.
- Let $p, q \in R$. The elements p and q are **associates** if there exists a unit $a \in R$ such that $p = aq$.
- An element $p \in R$ is **irreducible** if
  (a) $p \neq 0$,
  (b) p is not a unit, and
  (c) p has no proper divisor.

The following proposition shows that every property of divisors can be written in terms of containments of ideals and vice versa.

Proposition C.1.2. — *Let $p, q \in R$ and let (p) and (q) denote the ideals generated by the elements p and q respectively. Then*

(a) p is a unit $\Longleftrightarrow (p) = R$.

(b) p divides $q \Longleftrightarrow (q) \subseteq (p)$.

(c) p is a proper divisor of $q \Longleftrightarrow (q) \subsetneq (p) \subsetneq R$.

[d) p is an associate of $q \Longleftrightarrow (p) = (q)$.

(e) $$\begin{array}{lcl} p \textit{ is irreducible} & \Longleftrightarrow & (p) \neq 0 \textit{ and } (p) \neq R \textit{ and} \\ & & \textit{if } (q) \in R \textit{ and } (q) \supsetneq (p) \textit{ then } (q) = R. \end{array}$$

HW: Show that if R is a PID and $p \in R$ then p is irreduicible if and only if (p) is a maximal ideal.

Definition C.1.3. —

- A **unique factorization domain** (or **UFD**) is an integral domain R such that
  (a) If $x \in R$ then there exist irreducible $p_1, \ldots, p_n \in R$ such that $x = p_1 \cdots p_n$.
  (b) If $x \in R$ and $x = p_1 \cdots p_n = uq_1 \cdots q_m$ where $u \in R$ is a unit and $p_1, \ldots, p_n,\ q_1, \ldots, q_m \in R$ are irreducible then $m = n$ and there exists a permutation $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ and units $u_1, \ldots, u_n \in R$ such that
$$\text{if } i \in \{1, \ldots, n\} \text{ then } q_i = u_i p_{\sigma(i)}.$$

The following theorem says that PID $\Longrightarrow$ UFD.

Theorem C.1.3. — *A principal ideal domain is a unique factorization domain.*

The proof of Theorem C.1.3 will require the following lemmas.

Lemma C.1.4. — *If R is a principal ideal domain and $p \in R$ is an irreducible element of R then (p) is a prime ideal. REALLY? IS THIS NOT TRIVIAL??*

The following Proposition says that a PID is Noetherian or, synonymically, satisfies the ascending chain condition (ACC).?????.

Proposition C.1.5. — *Let R be a principal ideal domain. There does not exist an infinite sequence of elements $a_1, a_2, \ldots \in R$ such that*
$$(0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots .$$

C.1.3. Greatest common divisors. —

Definition C.1.4. — Let R be a unique factorization domain.

- Let $a_0, a_1, \ldots, a_n \in R$. A **greatest common divisor**, $\gcd(a_0, a_1, \ldots, a_n)$, of $a_0, a_1, \ldots, a_n$ is an element $d \in R$ such that
  (a) d divides a_i for all $i = 0, 1, \ldots, n$,
  (b) If d' divides a_i for all $i = 0, 1, \ldots, n$ then $d' \in R$ divides d.

Proposition C.1.6. — *Let R be a unique factorization domain and let $a_0, a_1, \ldots, a_n \in R$. Then*
(a) $\gcd(a_0, a_1, \ldots, a_n)$ *exists.*
(b) $\gcd(a_0, a_1, \ldots, a_n)$ *is unique up to multiplication by a unit.*

C.2. Fields, Integral Domains, Fields of Fractions

C.2.1. R/M is a field $\iff$ M is a maximal ideal.—

Definition C.2.1. —

- A **field** is a commutative ring F such that if $x \in F$ and $x \neq 0$ then there exists an element $x^{-1} \in F$ such that $xx^{-1} = 1$.
- A **proper ideal** is an ideal of R that is not the zero ideal (0) and not the whole ring R.
- A **maximal ideal** is an ideal M of a ring R such that
  (a) $M \neq R$,
  (b) If M' is an ideal of R and $M \subseteq M' \neq R$ then $M = M'$.

Lemma C.2.1. — *Let F be a commutative ring. Then F is a field if and only if the only ideals of F are (0) and F.*

Theorem C.2.2. — *Let R be a commutative ring and let M be an ideal of R. Then*

$$R/M \text{ is a field} \quad \text{if and only if} \quad M \text{ is a maximal ideal.}$$

C.2.2. R/P is an integral domain $\iff$ P is a prime ideal.—

Definition C.2.2. —

- An **integral domain** is a commutative ring R such that if $a, b \in R$ and $ab = 0$ then either $a = 0$ or $b = 0$.
- A **zero divisor** in a ring R is an element $a \in R$ such that there exists $b \in R$ with $\neq 0$ and $ab = 0$.
- A **prime ideal** is an ideal P in a commutative ring R such that if $a, b \in R$ and $ab \in P$ then either $a \in P$ or $b \in P$.

HW: Show that an integral domain is a commutative ring with no zero divisors except 0.

Proposition C.2.3. — (Cancellation Law) *Let R be an integral domain. If $a, b, c \in R$ and $c \neq 0$ and $ac = bc$ then $a = b$.*

Theorem C.2.4. — *Let R be a commutative ring and let P be an ideal of R. Then*

$$R/P \text{ is an integral domain} \quad \text{if and only if} \quad P \text{ is a prime ideal.}$$

C.2.3. Fields of fractions. —

Definition C.2.3. — Let R be an integral domain.

- A **fraction** is an expression $\dfrac{a}{b}$ with $a \in R$, $b \in R$ and $b \neq 0$.

Proposition C.2.5. — *Let R be an integral domain. Let $F_R = \left\{\dfrac{a}{b} \mid a, b \in R, b \neq 0\right\}$ be the set of fractions. Define two fractions $\frac{a}{b}$, $\frac{c}{d}$ to be equal if $ad = bc$, i.e.*

$$\frac{a}{b} = \frac{c}{d} \quad \text{if } ad = bc.$$

Then equality of fractions is an equivalence relation on F_R.

Proposition C.2.6. — *Let R be an integral domain. Let $F_R = \left\{\frac{a}{b} \mid a, b \in R, b \neq 0\right\}$ be its set of fractions with equality of fractions be as defined in Proposition C.2.5. Then the operations $+\colon F_R \times F_R \to F$ and $\times\colon F_R \times F_R \to F_R$ given by*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \textit{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \qquad \textit{are well defined.}$$

Theorem C.2.7. — *Let R be an integral domain and let $F_R = \left\{\frac{a}{b} \mid a \in R, b \in R - \{0\}\right\}$ be the set of fractions with equality of fractions be as defined in Proposition C.2.5 and let operations $+\colon F_R \times F_R \to F_R$ and $\times\colon F_R \times F_R \to F_R$ be as given in Proposition C.2.6. Then F_R is a field.*

Definition C.2.4. — Let R be an integral domain.

- The **field of fractions** of R is the set $F_R = \{\frac{m}{n} \mid m, n \in R, n \neq 0\}$ of fractions with **equality of fractions** defined by
$$\frac{m}{n} = \frac{p}{q} \quad \text{if } mq = np$$
and operations of **addition** $+\colon F_R \times F_R \to F_R$ and **multiplication** $\times\colon F_R \times F_R \to F_R$ defined by
$$\frac{m}{n} + \frac{p}{q} = \frac{mq+np}{pq} \qquad \text{and} \qquad \frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}.$$

HW: Give an example of an integral domain R and its field of fractions.

Proposition C.2.8. — *Let R be an integral domain with identity* 1 *and let F_R be its field of fractions. Then the map $\varphi\colon R \to F_R$ given by*

$$\begin{array}{rccc} \varphi\colon & R & \to & F_R \\ & r & \mapsto & \frac{r}{1} \end{array}$$

is an injective ring homomorphism.

C.3. Polynomial Rings

Definition C.3.1. — Let R be a commutative ring and for $i \in \mathbb{Z}_{>0}$ let x^i be a formal symbol.

- A **polynomial with coefficients in** R is an expression of the form
$$f(x) = r_0 + r_1x + r_2x^2 + \cdots$$
such that
  (a) if $i \in \mathbb{Z}_{\geqslant 0}$ then $r_i \in R$,
  (b) There exists $N \in \mathbb{Z}_{>0}$ such that if $i \in \mathbb{Z}_{>N}$ then $r_i = 0$.
- Polynomials $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = s_0 + s_1x + s_2x^2 + \cdots$ with coefficients in R are
$$\textbf{equal} \text{ if } \quad r_i = s_i \text{ for } i \in \mathbb{Z}_{\geqslant 0}.$$
- The **zero polynomial** is the polynomial $0 = 0 + 0x + 0x^2 + \cdots$.
- The **degree** $\deg\big(f(x)\big)$ of a polynomial $f(x) = r_0+r_1x+r_2x^2+\cdots$ with coefficients in R is
$$\text{the smallest } N \in \mathbb{Z}_{\geqslant 0} \text{ such that } \quad r_N \neq 0 \text{ and } r_k = 0 \text{ for } k \in \mathbb{Z}_{>N}.$$
If $f(x) = 0 + 0x + 0x^2 + \cdots$ then define $\deg\big(f(x)\big) = 0$.
- Let R be a commutative ring. The **ring of polynomials with coefficients in** R is the set $R[x]$ of polynomials with coefficients in R with the operations of addition and multiplication defined as follows:
If $f(x), g(x) \in R[x]$ with
$$f(x) = r_0 + r_1x + r_2x^2 + \cdots \quad \text{and} \quad g(x) = s_0 + s_1x + s_2x^2 + \cdots ,$$
then
$$f(x) + g(x) = (r_0 + s_0) + (r_1 + s_1)x + (r_2 + s_2)x^2 + \cdots , \quad \text{and}$$
$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots , \quad \text{where} \quad c_k = \sum_{i+j=k} r_is_j.$$

Proposition C.3.1. — *Let R be a commutative ring. Then $R[x]$ is a commutative ring.*

Proposition C.3.2. — *Let R be an integral domain. Then $R[x]$ is an integral domain.*

Theorem C.3.3. — *Let R be a unique factorization domain. Then $R[x]$ is a unique factorization domain.*

Theorem C.3.4. — *Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ with size function*
$$\begin{array}{rcc} \deg\colon F[x] - \{0\} & \longrightarrow & \mathbb{Z}_{\geqslant 0} \\ f(x) & \longmapsto & \deg\big(f(x)\big) \end{array} \quad \textit{is a Euclidean domain.}$$

Corollary C.3.5. — *Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a principal ideal domain.*

HW: Show that $\mathbb{Z}$ is a PID and $\mathbb{Z}[x]$ is not a PID.

The following Proposition says that the process of constructing the polynomial ring is “functorial”.

Proposition C.3.6. — *Let R, S be commutative rings and let $\varphi\colon R \to S$ be a ring homomorphism. Then the function*

$$\begin{array}{rcc} \psi\colon R[x] & \longrightarrow & S[x] \\ r_0 + r_1x + r_2x^2 + \cdots & \longmapsto & \varphi(r_0) + \varphi(r_1)x + \varphi(r_2)x^2 + \cdots \end{array}$$

is a ring homomorphism.

C.3.1. Adjoining elements to R, the rings $R[\alpha]$. —

Definition C.3.2. — Let S be a commutative ring and let $\alpha \in S$.

- The **evaluation homomorphism** is the function

$$\begin{array}{rccc} \mathrm{ev}_a\colon & S[x] & \to & S \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

where if $f(x) = s_0 + s_1x + s_2x^2 + \cdots$ then $f(\alpha) = s_0 + s_1\alpha + s_2\alpha^2 + \cdots$.

Proposition C.3.7. — *Let S be a commutative ring and let $\alpha \in S$. Then the evaluation homomorphism $\mathrm{ev}_\alpha\colon S[x] \to S$ is a ring homomorphism.*

Definition C.3.3. — Let S be a commutative ring.
Let $R \subseteq S$ be a subring and let $\alpha \in S$.

- The ring R **adjoined** α is the subring $R[\alpha]$ of S given by
(THIS IS CLUMSY WITH THE DEPENDENCE ON S)

$$R[\alpha] = \mathrm{ev}_\alpha\big(R[x]\big), \qquad \text{where} \quad \begin{array}{rccc} \mathrm{ev}_\alpha\colon & S[x] & \to & S \\ & f(x) & \mapsto & f(\alpha). \end{array}$$

HW: Prove that $R[\alpha] = \mathrm{ev}_\alpha\big(R[x]\big)$ is a subring of S.

HW: Let S be a commutative ring. Let $R \subseteq S$ be a subring and let $\alpha \in S$. Show that

$$R[\alpha] = \{r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_d\alpha^d \in S \mid d \in \mathbb{Z}_{\geqslant 0} \text{ and } r_i \in R\}.$$

C.3.2. Executing the proof of Theorem C.3.3. —

Definition C.3.4. — Let R be a unique factorization domain.

- A polynomial $f(x) = c_0 + c_1x + \cdots + c_kx^k \in R[x]$ is **primitive** if there does not exist $p \in R$ such that $c_0, c_1, \ldots, c_k \in Rp$.

Lemma C.3.8. — (Gauss' Lemma) *Let R be a unique factorization domain. Let $f(x), g(x) \in R[x]$ be primitive polynomials. Then $f(x)g(x)$ is a primitive polynomial.*

Proposition C.3.9. — *Let R be a unique factorization domain. Let $\mathbb{F}$ be the field of fractions of R and let $f(x) \in \mathbb{F}[x]$. Then*

(a) There exists $c \in \mathbb{F}$ and a primitive polynomial $g(x) \in R[x]$ such that

$$f(x) = cg(x).$$

(b) The factors c and $g(x)$ are unique up to multiplication by a unit (A UNIT IN WHAT???).

(c) $f(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $g(x)$ is irreducible in $R[x]$.

Theorem C.3.10. — *Let R be a unique factorization domain. Then $R[x]$ is a unique factorization domain.*

C.4. Proofs: Polynomial Rings

Proposition C.4.1. — *Let R be a commutative ring. Then $R[x]$ is a commutative ring.*

Proof. —
To show: (a) If $f(x), g(x) \in R[x]$ then $f(x) + g(x) = g(x) + f(x)$.
(b) If $f(x), g(x), h(x) \in R[x]$ then $\big(f(x)+g(x)\big)+h(x) = f(x)+\big(g(x)+h(x)\big)$.
(c) $0 \in R[x]$ such that if $f(x) \in R[x]$ then $0 + f(x) = f(x)$.
(d) If $f(x) \in R[x]$ then there exists $-f(x) \in R[x]$ such that $f(x)+\big(-f(x)\big) = 0$.
(e) If $f(x), g(x), h(x) \in R[x]$ then $\big(f(x)g(x)\big)h(x) = f(x)\big(g(x)h(x)\big)$.
(f) There exists $1 \in R[x]$ such that $1 \cdot f(x) = f(x) \cdot 1 = f(x)$.
(g) If $f(x), g(x), h(x) \in R[x]$ then $f(x)\big(g(x) + h(x)\big) = f(x)g(x) + f(x)h(x)$ and $\big(g(x) + h(x)\big)f(x) = g(x)f(x) + h(x)f(x)$.
(h) If $f(x), g(x) \in R[x]$ then $f(x)g(x) = g(x)f(x)$.

(a) Let $f(x), g(x) \in R[x]$ such that $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = s_0 + s_1x + s_2x^2 + \cdots$.
Then
$$f(x) + g(x) = (r_0 + s_0) + (r_1 + s_1)x + (r_2 + s_2)x^2 + \cdots \quad \text{and}$$
$$g(x) + f(x) = (s_0 + r_0) + (s_1 + r_1)x + (s_2 + r_2)x^2 + \cdots .$$
Since addition in R is a commutative operation then
$$r_i + s_i = s_i + r_i \quad \text{for } i \in \mathbb{Z}_{\geqslant 0}.$$
So $f(x) + g(x) = g(x) + f(x)$.

(b) Let $f(x), g(x), h(x) \in R[x]$ and let $f(x) = r_0 + r_1x + r_2x^2 + \cdots$, $g(x) = s_0 + s_1x + s_2x^2 + \cdots$, and $h(x) = t_0 + t_1x + t_2x^2 + \cdots$.
Then
$$\big(f(x) + g(x)\big) + h(x) = \big((r_0 + s_0) + t_0\big) + \big((r_1 + s_1) + t_1\big)x + \big((r_2 + s_2) + t_2\big)x^2 + \cdots \quad \text{and}$$
$$f(x) + \big(g(x) + h(x)\big) = \big(r_0 + (s_0 + t_0)\big) + \big(r_1 + (s_1 + t_1)\big)x + \big(r_2 + (s_2 + t_2)\big)x^2 + \cdots .$$
Since addition in R is an associative operation then
$$(r_i + s_i) + t_i = r_i + (s_i + t_i) \quad \text{for } i \in \mathbb{Z}_{\geqslant 0}.$$
So $\big(f(x) + g(x)\big) + h(x) = f(x) + \big(g(x) + h(x)\big)$.

(c) Let 0 denote the polynomial
$$0 = 0 + 0x + 0x^2 + \cdots .$$
Let $f(x) \in R[x]$ and let
$$f(x) = r_0 + r_1x + r_2x^2 + \cdots .$$
Then
$$0 + f(x) = (0 + r_0) + (0 + r_1)x + (0 + r_2)x^2 + \cdots .$$
If $i \in \mathbb{Z}_{\geqslant 0}$ then $0 + r_i = r_i$, and so
$$0 + f(x) = f(x).$$
Since addition of polynomials is commutative by (a) then $f(x)+0 = 0+f(x) = f(x)$.

(d) Let $f(x) \in R[x]$ such that $f(x) = r_0 + r_1x + r_2x^2 + \cdots$.
Then let $-f(x) = -r_0 + (-r_1)x + (-r_2)x^2 + \cdots$.
If $i \in \mathbb{Z}_{\geqslant 0}$ then $r_i \in R$ and so $-r_i \in R$ and $-f(x) \in R[x]$.

Then

$$f(x) + \big(-f(x)\big) = (r_0 - r_0) + (r_1 - r_1)x + (r_2 - r_2)x^2 + \cdots .$$

So

$$f(x) + \big(-f(x)\big) = 0 + 0x + 0x^2 + \cdots = 0.$$

Since addition of polynomials is commutative by (a), $f(x) + \big(-f(x)\big) = -f(x) + f(x) = 0$.

(e) Let $f(x), g(x), h(x) \in R[x]$ and $f(x) = r_0 + r_1x + r_2x^2 + \cdots$, $g(x) = s_0 + s_1x + s_2x^2 + \cdots$, and $h(x) = t_0 + t_1x + t_2x^2 + \cdots$.
Then

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots, \quad \text{where} \quad c_k = \sum_{i+j=k} r_is_j, \quad \text{and}$$

$$\big(f(x)g(x)\big)\big(h(x)\big) = d_0 + d_1x + d_2x^2 + \cdots, \quad \text{where} \quad d_n = \sum_{k+l=n} c_kt_l.$$

So, by the distributive law in R,

$$d_n = \sum_{k+l=n} \Big(\sum_{i+j=k} r_is_j\Big)t_l = \sum_{i+j+l=n} r_is_jt_l,$$

Also

$$g(x)h(x) = e_0 + e_1x + e_2x^2 + \cdots, \quad \text{where} \quad e_q = \sum_{a+b=q} s_at_b, \quad \text{and}$$

$$\big(f(x)\big)\big(g(x)h(x)\big) = d'_0 + d'_1x + d'_2x^2 + \cdots, \quad \text{where} \quad d'_n = \sum_{p+q=n} r_pe_q.$$

Then, by the distributive law in R,

$$d'_n = \sum_{p+q=n} r_p\Big(\sum_{a+b=q} s_at_b\Big) = \sum_{p+a+b=n} r_ps_at_b,$$

So, if $n \in \mathbb{Z}_{\geqslant 0}$ then $d_n = d'_n$.
So $\big(f(x)g(x)\big)\big(h(x)\big) = \big(f(x)\big)\big(g(x)h(x)\big)$.

(h) Let $f(x), g(x) \in R[x]$ and let $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = s_0 + s_1x + s_2x^2 + \cdots$.
Then

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots, \quad \text{where} \quad c_k = \sum_{i+j=k} r_is_j, \quad \text{and}$$

$$g(x)f(x) = c'_0 + c'_1x + c'_2x^2 + \cdots, \quad \text{where} \quad c'_k = \sum_{i+j=k} s_jr_i.$$

Since R is a commutative ring then

$$c_k = \sum_{i+j=k} r_is_j = \sum_{i+j=k} s_jr_i = c'_k \quad \text{for } k \in \mathbb{Z}_{\geqslant 0}.$$

So $f(x)g(x) = g(x)f(x)$.

(f) Let $1 \in R[x]$ be the polynomial given by

$$1 = 1 + 0x + 0x^2 + \cdots .$$

Let $f(x) \in R[x]$ and $f(x) = r_0 + r_1x + r_2x^2 + \cdots$.

Then

$$1 \cdot f(x) = c_0 + c_1x + c_2x^2 + \cdots, \quad \text{where} \quad c_k = \sum_{i+j=k} a_i r_j, \quad \text{and}$$

$$a_0 = 1 \quad \text{and} \quad a_i = 0 \quad \text{for } i \in \mathbb{Z}_{>1}.$$

So $c_k = a_0r_k + 0 + 0 + \cdots + 0 = r_k$ for $k \in \mathbb{Z}_{\geqslant 0}$.
So $1 \cdot f(x) = f(x)$.
Since multiplication in $R[x]$ is commutative by (h) then $1 \cdot f(x) = f(x) \cdot 1 = f(x)$.

(g) Let $f(x), g(x), h(x) \in R[x]$ and suppose $f(x) = r_0 + r_1x + r_2x^2 + \cdots$, $g(x) = s_0 + s_1x + s_2x^2 + \cdots$ and $h(x) = t_0 + t_1x + t_2x^2 + \cdots$.
Then

$$f(x)\big(g(x)h(x)\big) = c_0 + c_1x + c_2x^2 + \cdots \quad \text{where} \quad c_k = \sum_{i+j=k} r_i(s_j + t_j).$$

By the distributive law in R, $c_k = \sum_{i+j=k} r_is_j + r_it_j$.
Also $f(x)g(x) + f(x)h(x) = c'_0 + c'_1x + c'_2x^2 + \cdots$, where

$$c'_k = \sum_{m+n=k} r_ms_n + \sum_{m+n=k} r_mt_n = \sum_{m+n=k} r_ms_n + r_mt_n.$$

So $c_k = c'_k$ for $k \in \mathbb{Z}_{>0}$.
Thus

$$f(x)\big(g(x)h(x)\big) = f(x)g(x) + f(x)h(x).$$

Since multiplication in $R[x]$ is commutative by (h),

$$\begin{aligned}\big(g(x) + h(x)\big)f(x) &= f(x)\big(g(x) + h(x)\big) \\ &= f(x)g(x) + f(x)h(x) \\ &= g(x)f(x) + h(x)f(x).\end{aligned}$$

So $R[x]$ is a commutative ring. □

Proposition C.4.2. — *Let R be an integral domain. Then $R[x]$ is an integral domain.*

Proof. —
To show: If $a(x), b(x) \in R[x]$ and $a(x)b(x) = 0$ then either $a(x) = 0$ or $b(x) = 0$.
Let $a(x) = a_0 + a_1x + a_2x^2 + \cdots$ and let $b(x) = b_0 + b_1x + b_2x^2 + \cdots$.
Let $c(x) = a(x)b(x) = c_0 + c_1x + c_2x^2 + \cdots$.
Assume $a(x) \neq 0$.
Then there exists $i \in \mathbb{Z}_{\geqslant 0}$ such that $a_l \neq 0$.
Let k be the smallest $k \in \mathbb{Z}_{\geqslant 0}$ such that $a_k \neq 0$.
To show: $b(x) = 0$.
To show: if $n \in \mathbb{Z}_{\geqslant 0}$ then $b_N = 0$.
Proof by induction on N.

Base case: $N = 0$.
Since $c(x) = a(x)b(x) = 0$ then $c_k = 0$ for $k \in \mathbb{Z}_{\geqslant 0}$.
So

$$\sum_{i+j=k} a_ib_j = 0.$$

If $i \in \{0, \ldots, k-1\}$ then $a_i = 0$ so that

$$0 = \sum_{i+j=k} a_ib_j = a_kb_0.$$

Since R is an integral domain and $a_k, b_0 \in R$ and $a_k \neq 0$, then $b_0 = 0$.

Induction assumption: Assume if $n \in \mathbb{Z}_{[0,N)}$ then $b_n = 0$.
Since $c(x) = a(x)b(x) = 0$ then $c_{k+N} = 0$,
So

$$\sum_{i+j=k+N} a_i b_j = 0.$$

Since $a_i = 0$ for $i \in \{0, \dots, k\}$ and $b_n = 0$ for $n \in \{0, \dots, N\}$ then

$$0 = \sum_{i+j=k+N} a_i b_j = a_k b_N.$$

Since R is an integral domain and $a_k, b_N \in R$ and $a_k \neq 0$, then $b_N = 0$.

So $b_N = 0$ for $N \in \mathbb{Z}_{\geqslant 0}$.
So $b(x) = 0$.
So $R[x]$ is an integral domain. □

Theorem C.4.3. — *Let $\mathbb{F}$ be a field. The ring $\mathbb{F}[x]$ is a Euclidean domain with size function*

$$\begin{array}{rcl} \deg\colon F[x]-\{0\} & \to & \mathbb{Z}_{\geqslant 0} \\ f(x) & \mapsto & \deg\big(f(x)\big). \end{array}$$

Proof. — To show: If $a(x), b(x) \in F[x]$ and $a(x) \neq 0$ then there exist $q(x), r(x) \in F[x]$ such that

$$b(x) = a(x)q(x) + r(x)$$

where either $r(x) = 0$ or $\deg\big(r(x)\big) < \deg\big(a(x)\big)$.
Assume $a(x), b(x) \in F[x]$ and $a(x) \neq 0$.

Case 1: $b(x) = 0$.
Then $b(x) = a(x) \cdot 0 + 0$.
So $q(x) = 0$ and $r(x) = 0$ satisfies the condition.

Case 2: $\deg\big(b(x)\big) < \deg\big(a(x)\big)$.
Then, since

$$b(x) = a(x) \cdot 0 + b(x) \text{ and } \deg\big(b(x)\big) < \deg\big(a(x)\big)$$

then $q(x) = 0$ and $r(x) = b(x)$ satisfies the condition.

Case 3: $\deg\big(b(x)\big) \geqslant \deg\big(a(x)\big)$.
Let $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_s x^s$ and let $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_t x^t$, where $a_s, b_t \in \mathbb{F}$, $a_s \neq 0$ and $b_t \neq 0$.
Proof by induction on $\deg\big(b(x)\big)$.

Base case: $\deg\big(b(x)\big) = 0$.
Then $\deg\big(a(x)\big) = 0$, since $\deg\big(a(x)\big) \leqslant \deg\big(b(x)\big)$.
So $b(x) = b_0 \in \mathbb{F}$ and $a(x) = a_0$.
So $b(x) = \left(\frac{b_0}{a_0}\right) \cdot a(x) + 0$.
So $q(x) = b_0 a_0^{-1}$ and $r(x) = 0$ satisfies the condition.

Induction assumption: Assume that if $b_1(x) \in \mathbb{F}[x]$ and $\deg\big(b_1(x)\big) < t$ then there exist $q_1(x), r_1(x) \in F[x]$ such that

$$b_1(x) = q_1(x)a(x) + r_1(x)$$

where either $r_1(x) = 0$ or $\deg\big(r_1(x)\big) < \deg\big(a(x)\big)$.

(a) Assume that $\deg\big(b(x)\big) = t$.
Let $b_1(x) = b(x) - (b_t a_s^{-1} x^{t-s})a(x)$.
Then $\deg\big(b_1(x)\big) \leqslant \deg\big(b(x)\big)$.
Note that the coefficient of x^t in $b_1(x)$ is $-b_t + b_t = 0$.
So $\deg\big(b_1(x)\big) < t = \deg\big(b(x)\big)$.
Thus, by the induction assumption, there exist $q_1(x), r_1(x) \in F[x]$ such that

$$b_1(x) = q_1(x)a(x) + r_1(x)$$

where either $r_1(x) = 0$ or $\deg\big(r_1(x)\big) < \deg\big(a(x)\big)$.
Then

$$\begin{aligned} b(x) &= b_1(x) - (b_t a_s^{-1} x^{s-t})a(x) \\ &= q_1(x)a(x) + r_1(x) - (b_t a_s^{-1} x^{s-t})a(x) \\ &= \big(q_1(x) - b_t a_s^{-1} x^{s-t}\big)a(x) + r_1(x). \end{aligned}$$

So, if $q(x) = q_1(x) - b_t a_s^{-1} x^{s-t}$ and $r(x) = r_1(x)$ then

$$b(x) = q(x)a(x) + r(x)$$

and either $r(x) = 0$ or $\deg\big(r(x)\big) < \deg\big(a(x)\big)$.
So $\mathbb{F}[x]$ with size function given by deg is a Euclidean domain. □

Proposition C.4.4. — *Let R, S be commutative rings and let $\varphi\colon R \to S$ be a ring homomorphism. Then the map*

$$\begin{array}{cccc} \psi\colon & R[x] & \longrightarrow & S[x] \\ & r_0 + r_1x + r_2x^2 + \cdots & \longmapsto & \varphi(r_0) + \varphi(r_1)x + \varphi(r_2)x^2 + \cdots \end{array}$$

is a ring homomorphism.

Proof. —
To show: (a) If $f(x), g(x) \in R[x]$ then $\psi\big(f(x) + g(x)\big) = \psi\big(f(x)\big) + \psi\big(g(x)\big)$.
(b) If $f(x), g(x) \in R[x]$ then $\psi\big(f(x)g(x)\big) = \psi\big(f(x)\big)\psi\big(g(x)\big)$.
(c) $\psi(1_R) = 1_S$ where 1_R and 1_S are the identities in R and S respectively.

(a) Let $f(x), g(x) \in R[x]$ and let $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = r_0' + r_1'x + r_2'x^2 + \cdots$.
Then

$$\begin{aligned} \psi\big(f(x) + g(x)\big) &= \psi\big((r_0 + r_0') + (r_1 + r_1')x + (r_2 + r_2')x^2 + \cdots\big) \\ &= \varphi(r_0 + r_0') + \varphi(r_1 + r_1')x + \varphi(r_2 + r_2')x^2 + \cdots. \end{aligned}$$

Since φ is a homomorphism,

$$\begin{aligned} \psi\big(f(x) + g(x)\big) &= \big(\varphi(r_0) + \varphi(r_0')\big) + \big(\varphi(r_1) + \varphi(r_1')\big)x + \big(\varphi(r_2) + \varphi(r_2')\big)x^2 + \cdots \\ &= \big(\varphi(r_0) + \varphi(r_1)x + \varphi(r_2)x^2 + \cdots\big) + \big(\varphi(r_0') + \varphi(r_1')x + \varphi(r_2')x^2 + \cdots\big) \\ &= \psi\big(f(x)\big) + \psi\big(g(x)\big). \end{aligned}$$

(b) Let $f(x), g(x) \in R[x]$ and let $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = r_0' + r_1'x + r_2'x^2 + \cdots$.
Then

$$\psi\big(f(x)g(x)\big) = \psi(c_0 + c_1x + c_2x^2 + \cdots), \quad \text{where} \quad c_k = \sum_{i+j=k} r_i r_j'.$$

So $\psi\big(f(x)g(x)\big) = \varphi(c_0) + \varphi(c_1)x + \varphi(c_2)x^2 + \cdots$.

Since φ is a homomorphism,

$$\varphi(c_k) = \varphi\Big(\sum_{i+j=k} r_i r_j'\Big) = \sum_{i+j=k} \varphi(r_i r_j') = \sum_{i+j=k} \varphi(r_i)\varphi(r_j').$$

So

$$\psi\big(f(x)g(x)\big) = d_0 + d_1x + d_2x^2 + \cdots, \quad \text{where} \quad d_k = \sum_{i+j=k} \varphi(r_i)\varphi(r_j').$$

So, by the distributive law in S,

$$\begin{aligned}\psi\big(f(x)g(x)\big) &= \big(\varphi(r_0) + \varphi(r_1)x + \varphi(r_2)x^2 + \cdots\big)\big(\varphi(r_0') + \varphi(r_1')x + \varphi(r_2')x^2 + \cdots\big) \\ &= \varphi\big(f(x)\big)\varphi\big(g(x)\big).\end{aligned}$$

(c) Let 1_R be the identity in R.

$$\begin{aligned}\psi(1_R) &= \psi(1_R + 0_Rx + 0_Rx^2 + \cdots) \\ &= \varphi(1_R) + \varphi(0_R)x + \varphi(0_R)x^2 + \cdots.\end{aligned}$$

Since φ is a homomorphism then $\varphi(1_R) = 1_S$ and $\varphi(0_R) = 0_S$.
So $\psi(1_R) = 1_S + 0_Sx + 0_Sx^2 + \cdots = 1_S$.

So ψ is a homomorphism. □

Proposition C.4.5. — *Let R be a commutative ring and let $\alpha \in R$. Then the evaluation homomorphism $\mathrm{ev}_\alpha\colon R[x] \to R$ is a ring homomorphism.*

Proof. —
To show: (a) If $f(x), g(x) \in R[x]$ then $\mathrm{ev}_\alpha\big(f(x)+g(x)\big) = \mathrm{ev}_\alpha\big(f(x)\big) + \mathrm{ev}_\alpha\big(g(x)\big)$.
(b) If $f(x), g(x) \in R[x]$ then $\mathrm{ev}_\alpha\big(f(x)g(x)\big) = \mathrm{ev}_\alpha\big(f(x)\big)\mathrm{ev}_\alpha\big(g(x)\big)$.
(c) $\mathrm{ev}_\alpha(1_R) = 1_R$, where 1_R is the identity in R.

(a) Let $f(x), g(x) \in R[x]$ and let $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = s_0 + s_1x + s_2x^2 + \cdots$.
Then

$$\begin{aligned}\mathrm{ev}_\alpha\big(f(x)+g(x)\big) &= \mathrm{ev}_\alpha\big((r_0+s_0) + (r_1+s_1)x + (r_2+s_2)x^2 + \cdots\big) \\ &= (r_0+s_0) + (r_1+s_1)\alpha + (r_2+s_2)\alpha^2 + \cdots.\end{aligned}$$

By the distributive law in R,

$$\begin{aligned}\mathrm{ev}_\alpha\big(f(x)+g(x)\big) &= r_0 + s_0 + r_1\alpha + s_1\alpha + r_2\alpha^2 + s_2\alpha^2 + \cdots \\ &= (r_0 + r_1\alpha + r_2\alpha^2 + \cdots) + (s_0 + s_1\alpha + s_2\alpha^2 + \cdots) \\ &= \mathrm{ev}_\alpha\big(f(x)\big) + \mathrm{ev}_\alpha\big(g(x)\big).\end{aligned}$$

(b) Let $f(x), g(x) \in R[x]$ and let $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = s_0 + s_1x + s_2x^2 + \cdots$.
Then

$$\mathrm{ev}_\alpha\big(f(x)g(x)\big) = \mathrm{ev}_\alpha(c_0 + c_1x + c_2x^2 + \cdots) \quad \text{where} \quad c_k = \sum_{i+j=k} r_i s_j.$$

So $\mathrm{ev}_\alpha\big(f(x)g(x)\big) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots$.
Now compute $\mathrm{ev}_\alpha\big(f(x)\big)\mathrm{ev}_\alpha\big(g(x)\big)$.

$$\mathrm{ev}_\alpha\big(f(x)\big)\mathrm{ev}_\alpha\big(g(x)\big) = (r_0 + r_1\alpha + r_2\alpha^2 + \cdots)(s_0 + s_1\alpha + s_2\alpha^2 + \cdots).$$

By the distributive law in R,

$$\begin{aligned}\mathrm{ev}_\alpha\big(f(x)\big)\mathrm{ev}_\alpha\big(g(x)\big) &= r_0s_0 + r_1s_0\alpha + r_0s_1\alpha + r_0s_2\alpha^2 + r_1s_1\alpha^2 + r_2s_0\alpha^2 + \cdots \\ &= r_0s_0 + (r_1s_0 + r_0s_1)\alpha + (r_0s_2 + r_1s_1 + r_2s_0)\alpha^2 + \cdots \\ &= c_0 + c_1\alpha + c_2\alpha^2 + \cdots \quad \text{where}\end{aligned}$$

$$c_k = \sum_{i+j=k} r_is_j.$$

So

$$\mathrm{ev}_\alpha\big(f(x)g(x)\big) = \mathrm{ev}_\alpha\big(f(x)\big)\mathrm{ev}_\alpha\big(g(x)\big).$$

(c) Let 1_R be the identity in R and let 0_R be the zero in R.
Then

$$\mathrm{ev}_\alpha(1_R) = \mathrm{ev}_\alpha(1_R + 0_Rx + 0_Rx^2 + \cdots) = 1_R + 0_R\alpha + 0_R\alpha^2 + \cdots = 1_R.$$

So ev_α is a ring homomorphism. □

Lemma C.4.6. — (Gauss' Lemma) *Let R be a UFD. Let $f(x), g(x) \in R[x]$ be primitive polynomials. Then $f(x)g(x)$ is a primitive polynomial.*

Proof. — Assume $f(x) = r_0 + r_1x + r_2x^2 + \cdots$ and $g(x) = s_0 + s_1x + s_2x^2 + \cdots$ are primitive polynomials in $R[x]$.
Proof by contradiction.
Assume $f(x)g(x)$ is not primitive.
Then there exists an irreducible element $p \in R$ that divides all the coefficients of $f(x)g(x)$.
Since $f(x)$ is primitive there must be at least one coefficient of $f(x)$ which is not divisible by p.
Since $g(x)$ is primitive there must be at least one coefficient of $g(x)$ which is not divisible by p.
Let m be the smallest m such that r_m is not divisible by p.
Let n be the smallest n such that s_n is not divisible by p.
Suppose that $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots$.
Then, since p divides r_i, for all $i < m$, and p divides s_j, for all $j < m$,

$$\begin{aligned}c_{m+n} &= r_ms_n + r_{m-1}s_{n+1} + r_{m+1}s_{n-1} + \cdots + r_0s_{m+n} + r_{m+n}s_0 \\ &= r_ms_n + pc,\end{aligned}$$

where c is some element of R.
Since c_{m+n} is divisible by p it follows that $r_ms_n = c_{m+n} - pc$ is divisible by p.
Suppose that $d \in R$ such that $r_ms_n = pd$.
Let

$$r_m = a_1 \cdots a_k, \quad s_n = b_1 \cdots b_l, \quad \text{and} \quad d = d_1 \cdots d_q,$$

be factorizations of r_m, s_n and d into irreducible elements $a_1, \ldots, a_k, b_1, \ldots, b_l, d_1, \ldots, d_q \in R$.
Then

$$a_1 \cdots a_kb_1 \cdots b_l = pd_1 \cdots d_q.$$

By uniqueness of factorizations,

either p is associate to a_i for some $1 \leqslant i \leqslant k$,
or p is associate to b_j for some $1 \leqslant j \leqslant l$.

So either $p_i = up$ or $q_j = up$ for some unit $u \in R$.
Then, either $a = upp_1 \cdots \hat{p}_i \cdots p_m$, or $b = upq_1 \cdots \hat{q}_j \cdots q_n$,
where $\hat{}$ denotes omitting the factor p_i or q_j.
Thus, either r_m or s_n is divisible by p.
Contradiction.
So $f(x)g(x)$ is a primitive polynomial.
THIS IS A REALLY BAD PROOF □

Proposition C.4.7. — *Let R be a UFD. Let $\mathbb{F}$ be the field of fractions of R and let $f(x) \in \mathbb{F}[x]$. Then*

(a) There exists an element $c \in \mathbb{F}$ and a primitive polynomial $g(x) \in R[x]$ such that

$$f(x) = cg(x).$$

(b) The factors c and $g(x)$ are unique up to multiplication by a unit IN WHERE????.

(c) $f(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $g(x)$ is irreducible in $R[x]$.

Proof. —

(a) Let $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_k}{b_k}x^k \in \mathbb{F}[x]$.
Then $f(x) = \frac{1}{b_0 b_1 \cdots b_k}(c_0 + c_1 x + \cdots + c_k x^k)$
where $c_i = a_i b_1 \cdots \hat{b}_i \cdots b_k$, where the $\hat{b}_i$ denotes omission of the factor b_i.
Let $d = \gcd(c_0, c_1, \ldots, c_k)$.
Then

$$f(x) = \frac{d}{b_0 \cdots b_k}(c_0' + c_1' x + \cdots + c_k' x^k)$$

where $c_i' = \frac{c_i}{d}$.
Note that $c_i' \in R$ since d divides c_i.
Furthermore $c_0' + c_1'x + \cdots + c_k'x^k = g(x)$ is primitive since $\gcd(c_0', c_1', \ldots, c_k') = 1$.
So

$$f(x) = cg(x)$$

where $c = \frac{d}{b_0 b_1 \cdots b_k} \in F$ and $g(x) = c_0' + c_1'x + \cdots + c_k'x^k \in R[x]$ is a primitive polynomial.

(b) Suppose $f(x) = cg(x)$ and $f(x) = CG(x)$ where $c, C \in \mathbb{F}$ and $g(x), G(x) \in R[x]$ are primitive polynomials.
Let $g(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$ and let $G(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k$.
Suppose $c = \frac{a}{b}$ and $C = \frac{A}{B}$ where $a, b, A, B \in R$.
Since $f(x) = \dfrac{a}{b} g(x) = \dfrac{A}{B} G(x)$ then

$$aBg(x) = bAG(x).$$

So $aBa_i = bAb_i$ for $i \in \{1, \ldots, k\}$.
Since $g(x)$ is primitive then $\gcd(aBa_0, aBa_1, \ldots, aBa_k) = aB$.
Since $G(x)$ is primitive then $\gcd(bAb_0, bAb_1, \ldots, bAb_k) = bA$.
Thus, by Proposition 3.2.10????,

$$aB = ubA \text{ for some unit } u \in R.$$

So $\dfrac{a}{b} = u \cdot \left(\dfrac{A}{B}\right)$.
So $c = uC$ where $u \in R$ is a unit.
So $CG(x) = cg(x) = uCg(x)$.
By the cancellation law, $G(x) = ug(x)$.

So $c = uC$ and $G(x) = ug(x)$.
So c and $g(x)$ are unique up to multiplication by a unit.

(c) $\Longrightarrow$:
Assume that $f(x)$ is irreducible in $F[x]$.
Proof by contradiction. YIKES???????
Assume $g(x)$ is not irreducible in $R[x]$.
Then there are $g_1(x)$ and $g_2(x)$ in $R[x]$ such that $g(x) = g_1(x)g_2(x)$.
So $f(x) = cg(x) = cg_1(x)g_2(x)$.
Since $R[x] \subseteq F[x]$ then $g_1(x), g_2(x) \in F[x]$.
So $f(x)$ is not irreducible in $F[x]$.
Contradiction.
So $g(x)$ is irreducible in $R[x]$.

(c) $\Longleftarrow$:
Assume $g(x)$ is irreducible in $R[x]$.
Proof by contradiction. YIKES??????
Assume $f(x)$ is not irreducible in $\mathbb{F}[x]$.
Then there are $f_1(x)$ and $f_2(x)$ in $F[x]$ such that $f(x) = f_1(x)f_2(x)$.
So, by (a), there exist $c_1, c_2 \in F$ and primitive polynomials $g_1(x), g_2(x) \in R[x]$ such that

$$f_1(x) = c_1g_1(x) \quad \text{and} \quad f_2(x) = c_2g_2(x).$$

Let $c = c_1c_2$.
Then $f(x) = cg_1(x)g_2(x)$.
By Gauss' lemma $g_1(x)g_2(x)$ is a primitive polynomial in $R[x]$.
So, by (b), $g(x) = ug_1(x)g_2(x)$, where $u \in R$. IS THIS RIGHT???
So $g(x)$ is not irreducible in $R[x]$.
Contradiction.FIX THIS
So $f(x)$ is irreducible in $F[x]$.

□

Theorem C.4.8. — *Let R be a unique factorization domain. Then $R[x]$ is a unique factorization domain.*

Proof. — Assume $g(x) \in R[x]$ and let $g(x) = a_0 + a_1x + \cdots a_kx^k$.
To show: (a) $g(x)$ has a factorization into irreducible factors in $R[x]$.
(b) The factorization of $g(x)$ is unique up to multiplication by units in $R[x]$ and rearrangement of the factors.

(a) By Theorems 3.3.5, 3.2.2, and 3.2.6, $F[x]$ is a UFD and so $g(x)$ has a factorization in $F[x]$,

$$g(x) = f_1(x)f_2(x)\cdots f_r(x), \quad \text{where } f_i(x) \in F[x] \text{ are irreducible in } F[x].$$

Then, by Proposition 3.3.12(a), there exist elements $c_1, \dots c_r \in \mathbb{F}$ and primitive polynomials
$g_1(x), \dots, g_r(x) \in R[x]$ such that

$$f_i(x) = c_ig_i(x), \quad \text{for } i \in \{1, \dots, k\}.$$

Since the factors $f_i(x)$ are irreducible in $F[x]$ then it follows from Proposition 3.3.12(c) that
the polynomials $g_i(x)$ are irreducible in $R[x]$.

Since the $g_i(x)$ are primitive, by Gauss' lemma, the product $g_1(x)\cdots g_r(x)$ is primitive.
So

$$g(x) = cg_1(x)g_2(x)\cdots g_r(x), \quad \text{where } c = c_1c_2\cdots c_r \in \mathbb{F}.$$

We also know that $g(x) = \gcd(a_0,\ldots,a_k)g'(x)$, where $g'(x)$ is a primitive polynomial in $R[x]$.
Thus, by Proposition 3.3.12(b), $c = u\gcd(a_0,\ldots,a_k)$ where $u \in R$ is a unit. USE THE NOTATION $R^\times$?????
It follows that $c \in R$.
Since R is a UFD then c has a factorization

$$c = d_1\cdots d_s,$$

where the elements d_j are irreducible elements in R.
So

$$g(x) = d_1\cdots d_s\cdot g_1(x)\cdots g_r(x),$$

is a factorization of $g(x)$ into irreducibles in $R[x]$.

(b) Suppose that $g(x) = d'_1d'_2\cdots d'_lg'_1(x)g'_2(x)\cdots g'_m(x)$ is another factorization of $g(x)$ into irreducible factors in $R[x]$.
By Proposition 3.3.12(c), each of the factors $g'_i(x)$ is irreducible in $\mathbb{F}[x]$.
So $g(x) = d'_1d'_2\cdots d'_lg'_1(x)g'_2(x)\cdots g'_m(x)$ and $g(x) = d_1\cdots d_sg_1(x)\cdots g_r(x)$, are both factorizations of $g(x)$ in $\mathbb{F}[x]$.
By Theorems 3.3.5, 3.2.2, and 3.2.6, $\mathbb{F}[x]$ is a UFD, and so $r = m$ and there is a permutation σ such that and $\alpha_i \in \mathbb{F}^\times$ such that

$$g'_{\sigma(i)}(x) = \alpha_ig_i(x).$$

Proposition 3.3.12(b), gives that each $\alpha_i \in R^\times$.
Let $u = \alpha_1\alpha_2\cdots\alpha_r$.
Then

$$\begin{aligned} g(x) = d_1\cdots d_s\cdots g_1(x)\cdots g_r(x) &= d'_1d'_2\cdots d'_lg'_1(x)g'_2(x)\cdots g'_m(x) \\ &= ud'_1d'_2\cdots d'_lg_1(x)g_2(x)\cdots g_m(x). \end{aligned}$$

Then Proposition 3.3.12(b) implies that there is a unit $v \in R$ such that

$$d_1\cdots d_s = vud'_1\cdots d'_l.$$

Since $R[x]$ is a UFD, $s = l$ and there is a permutation τ such that

$$d_{\tau(i)} = u_id'_i,$$

where the u_i are units in R.
So there is a rearrangement of the factors d'_i and $g'_j(x)$ such that, up to multiplication by units in R, they are the same as the factors d_i and $g_j(x)$.
So the factorization of $g(x)$ in $R[x]$ is unique.

So $R[x]$ is a UFD. □

THESE NEXT TWO RESULTS ARE NOT IN THE ORIGINAL VERSION??

Lemma C.4.9. — *Let R be a UFD. For each irreducible element $p \in R$ let $\pi_p\colon R \to R/pR$ be the quotient surjection (Part 1, Ex. 2.1.5????). Let $\tilde{\pi}_p\colon R[x] \to \frac{R}{pR}[x]$ be the corresponding homomorphism between polynomial rings (Prop 3.1.6????). Let $f(x) \in R[x]$. Then $f(x)$ is not primitive if and only if there exists an irreducible element $p \in R$ such that $\tilde{\pi}_p\big(f(x)\big) = 0$.*

Proof. —
$\Rightarrow$: Assume $f(x) = c_0 + c_1x + \cdots + c_kx^k$ is not primitive.
Then there exists $p \in R$ irreducible such that p divides c_0, p divides c_1, …, p divides c_k.
So $c_0, c_1, \ldots, c_k \in pR$.
So $\pi_p(c_0) = \pi_p(c_1) = \cdots = \pi_p(c_k) = 0$.
So $\hat{\pi}_p\big(f(x)\big) = \pi_p(c_0) + \pi_p(c_1)x + \cdots + \pi_p(c_k)x^k = 0$.

$\Leftarrow$: Assume that $f(x) = c_0 + c_1x + \cdots + c_kx^k$ and that there exists an irreducible element $p \in R$ such that $\hat{\pi}_p\big(f(x)\big) = 0$.
Then $\pi_p(c_0) = \pi_p(c_1) = \cdots = \pi_p(c_k) = 0$.
So $c_0, c_1, \ldots, c_k \in pR$.
So p divides c_0, p divides c_1, …, and p divides c_k.
So $f(x)$ is not primitive. □

Lemma C.4.10. — (Gauss' Lemma) *Let R be a UFD. Let $f(x), g(x) \in R[x]$ be primitive polynomials. Then $f(x)g(x)$ is a primitive polynomial.*

Proof. — We shall prove the contrapositive:
To show: If $f(x)g(x)$ is not primitive then either $f(x)$ is not primitive or $g(x)$ is not primitive.
Assume $f(x)g(x)$ is not primitive.
Then, by Lemma ????X.X, there exists an irreducible element $p \in R$ such that

$$\hat{\pi}_p\big(f(x)g(x)\big) = 0,$$

where $\hat{\pi}_p \colon R[x] \to \frac{R}{pR}[x]$ is the homomorphism between polynomial rings induced by the quotient surjection $\pi_p \colon R \to R/pR$.
Since $\hat{\pi}_p$ is a homomorphism,

$$\hat{\pi}_p\big(f(x)g(x)\big) = \hat{\pi}_p\big(f(x)\big)\hat{\pi}_p\big(g(x)\big) = 0.$$

By Lemma X.X????, pR is a prime ideal.
Thus, by Proposition X.X???, R/pR is an integral domain.
So either

$$\hat{\pi}_p\big(f(x)\big) = 0 \quad \text{or} \quad \hat{\pi}_p\big(g(x)\big) = 0.$$

Thus, by Lemma X.X,

$$\text{either } f(x) \text{ is not primitive} \quad \text{or} \quad g(x) \text{ is not primitive.}$$

□

C.5. Proofs: Fields, Integral Domains, Fields of Fractions

Lemma C.5.1. — *Let F be a commutative ring. Then F is a field if and only if the only ideals of F are (0) and F.*

Proof. —
$\Rightarrow$: Assume F is a field.
To show: The only ideals of F are (0) and F.
Let I be an ideal of F.
Suppose $I \neq (0)$.
Then there is an element $x \in I$ with $x \neq 0$.
Since F is a field, there is an element $x^{-1} \in F$ such that $xx^{-1} = 1$.

So $1 = x^{-1}x \in I$.
So, if $y \in F$, then $y = y \cdot 1 \in I$.
So $F \subseteq I \subseteq F$.
So $I = F$.
So the only ideals of F are (0) and F.

$\Leftarrow$: Assume that the only ideals of F are (0) and F.
To show: F is a field.
Let $x \in F$, $x \neq 0$.
Since $(x) \neq (0)$ then $(x) = F$.
So there exists $y \in F$ such that $xy = 1$.
So F is a field. □

Theorem C.5.2. — *Let R be a commutative ring and let M be an ideal of R. Then R/M is a field if and only if M is a maximal ideal.*

Proof. —
$\Rightarrow$: Assume R/M is a field.
Then, by Lemma 3.1.2, the only ideals of R/M are (0) and R/M.
By the correspondence theorem, Ex. 2.1.5(c), there is a one-to-one correspondence between
ideals of R/M and ideals of R containing M.
Thus the only ideals of R containing M are M and R.
So M is a maximal ideal.

$\Leftarrow$: Assume M is a maximal ideal.
Then the only ideals of R containing M are M and R.
By the correspondence theorem, Ex. 2.1.5(c), there is a one-to-one correspondence between ideals of R/M and ideals of R containing M.
Thus the only ideals of R/M are (0) and R/M.
So, by Lemma 3.1.2, R/M is a field. □

Proposition C.5.3. — *(Cancellation Law) Let R be an integral domain. If $a, b, c \in R$ and $c \neq 0$ and $ac = bc$ then $a = b$.*

Proof. — Assume $a, b, c \in R$ and $c \neq 0$ and $ac = bc$.
Then $0 = ac - bc = (a - b)c$.
Since R is an integral domain and $c \neq 0$ then $a - b = 0$.
So $a = b$. □

Theorem C.5.4. — *Let R be a commutative ring and let P be an ideal of R. Then R/P is an integral domain if and only if P is a prime ideal.*

Proof. —
$\Rightarrow$: Assume R/P is an integral domain.
To show: P is a prime ideal.
Let $a, b \in R$ and suppose $ab \in P$.
To show: Either $a \in P$ or $b \in P$.
Since $ab \in P$ then $(a + P)(b + P) = ab + P = 0 + P$ in R/P.
Since R/P is an integral domain then either $a + P = 0 + P$ or $b + P = 0 + P$.
Thus either $a \in P$ or $b \in P$.

So P is a prime ideal.

$\Leftarrow$: Assume P is a prime ideal.
To show: R/P is an integral domain.
Let $a, b \in R$ such that $(a+P)(b+P) = 0+P$.
To show: Either $a+P = 0+P$ or $b+P = 0+P$.
Then $ab+P = 0+P$.
So $ab \in P$.
Since P is prime then either $a \in P$ or $b \in P$.
So either $a+P = 0+P$ or $b+P = 0+P$.
So R/P is an integral domain. □

Proposition C.5.5. — *Let R be an integral domain. Let $F_R = \left\{\frac{a}{b} \mid a, b \in R, b \neq 0\right\}$ be the set of fractions. Then equality of fractions is an equivalence relation.*

Proof. —
To show: (a) $a/b = a/b$.
(b) If $a/b = c/d$ then $c/d = a/b$.
(c) If $a/b = c/d$ and $c/d = e/f$ then $a/b = e/f$.

(a) Since $ab = ba$ then $a/b = a/b$.
(b) Assume $a/b = c/d$.
Then $ad = bc$.
Since R is commutative then $cb = da$.
So $c/d = a/b$.
(c) Assume $a/b = c/d$ and $c/d = e/f$.
Then $ad = bc$ and $cf = de$.
To show: $af = be$.
Since $ad = bc$ and $cf = de$ then $adcf = bcde$.
Thus, by commutativity, $afcd = becd$.
Then, by the cancellation law for an integral domain, Proposition 3.1.5, $af = be$.
So $a/b = e/f$.

□

Proposition C.5.6. — *Let R be an integral domain. Let $F_R = \left\{\frac{a}{b} \mid a, b \in R, b \neq 0\right\}$ be its set of fractions. Let equality of fractions be as defined in Proposition 3.1.8????. Then the operations $+ \colon F_R \times F_R \to F$ and $\times \colon F_R \times F_R \to F_R$ given by*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \textit{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

are well defined.

Proof. — Assume $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$.
To show: (a) $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$.
(b) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$

(a) To show: $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$.
To show: $(ad+bc)b'd' = (a'd'+b'c')bd$.

We know that $ab' = ba'$ and $cd' = dc'$.
So

$$\underbrace{adb'}d' + b\underbrace{cb'd'} = a'bdd' + bdb'c' = (a'd' + b'c')bd.$$

So $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a'}{b'} + \dfrac{c'}{d'}$.

(b) To show: $\dfrac{ac}{bd} = \dfrac{a'c'}{b'd'}$.
To show: $acb'd' = a'c'bd$.
We know that $ab' = ba'$ and $cd' = dc'$.
So

$$acb'd' = ba'cd' = ba'dc' = a'c'bd.$$

So $\dfrac{ac}{bd} = \dfrac{a'c'}{b'd'}$. □

Theorem C.5.7. — *Let R be an integral domain and let $F_R = \left\{\frac{a}{b} \mid a \in R, b \in R - \{0\}\right\}$ be the set of fractions. Let equality of fractions be as defined in Proposition 3.1.8???? and let operations $+\colon F_R \times F_R \to F_R$ and $\times\colon F_R \times F_R \to F_R$ be as given in Proposition 3.1.9????. Then F_R is a field.*

Proof. —
To show: (a) F_R is a ring.
(b) F_R is commutative.
(c) If $x \in F_R$ and $x \neq 0$ then there exists $x^{-1} \in F_R$ such that $xx^{-1} = 1$.

(a) To show: (aa) $+\colon F_R \times F_R$ is well defined.
(ab) $\times\colon F_R \times F_R$ is well defined.
(ac) If $p/q, m/n, r/s \in F_R$ then $\big(p/q + m/n\big) + r/s = p/q + \big(m/n + r/s\big)$.
(ad) If $p/q, m/n \in F_R$ then $p/q + m/n = m/n + p/q$.
(ae) There is an element $0 \in F_R$ such that $0 + m/n = m/n$ for all m/n.
(af) If $x \in F_R$ then there is an element $-x \in F_R$ such that $x + (-x) = 0$.
(ag) If $p/q, m/n, r/s \in F_R$ then $p/q \cdot \big(m/n \cdot r/s\big) = \big(p/q \cdot m/n\big) \cdot r/s$.
(ah) There is an element $1 \in F_R$ such that $1 \cdot x = x$ for all $x \in F_R$.
(ai) If $m/n, p/q, r/s \in F_R$ then $m/n\big(p/q + r/s\big) = m/n \cdot p/q + m/n \cdot r/s$ and $\big(p/q + r/s\big)m/n = p/q \cdot m/n + r/s \cdot m/n$.

(aa) and
(ab) are proved in Proposition 3.1.9?????.
(ac) Assume $p/q, m/n, r/s \in F_R$.
To show: $(p/q + m/n) + r/s = p/q + (m/n + r/s)$.
By the definition of the operation $+\colon F_R \times F_R \to F_R$,

$$\begin{aligned}\left(\frac{p}{q} + \frac{m}{n}\right) + \frac{r}{s} &= \frac{pn + mq}{qn} + \frac{r}{s} \\ &= \frac{(pn + mq)s + qnr}{qns} \\ &= \frac{pns + mqs + qnr}{qns}.\end{aligned}$$

By the definition of the operation $+\colon F_R \times F_R \to F_R$,

$$\begin{aligned}\frac{p}{q} + \left(\frac{m}{n} + \frac{r}{s}\right) &= \frac{p}{q} + \left(\frac{ms+nr}{ns}\right) \\ &= \frac{pns + q(ms+nr)}{qns} \\ &= \frac{pns+qms+qnr}{qns}.\end{aligned}$$

Since R is commutative (R is an integral domain),

$$\frac{pns+mqs+qnr}{qns} = \frac{pns+qms+qnr}{qns}.$$

So

$$\left(\frac{p}{q} + \frac{m}{n}\right) + \frac{r}{s} = \frac{p}{q} + \left(\frac{m}{n} + \frac{r}{s}\right).$$

(ad) Assume $p/q, m/n \in F_R$.
To show: $p/q + m/n = m/n + p/q$.
By the definition of $+\colon F_R \times F_R \to F_R$,

$$\frac{p}{q} + \frac{m}{n} = \frac{pn+qm}{qn}.$$

By the definition of $+\colon F_R \times F_R \to F_R$,

$$\frac{m}{n} + \frac{p}{q} = \frac{mq+np}{nq}.$$

Since R is commutative,

$$\frac{pn+qm}{qn} = \frac{mq+np}{nq}.$$

So

$$\frac{p}{q} + \frac{m}{n} = \frac{m}{n} + \frac{p}{q}.$$

(ae) To show: There is an element $0 \in F_R$ such that if $m/n \in F_R$ then $0 + m/n = m/n$.
Let $0 = 0/1 \in F_R$.
To show: If $m/n \in F_R$ then $0/1 + m/n = m/n$.
Assume $m/n \in F_R$.
Then

$$\frac{0}{1} + \frac{m}{n} = \frac{0 \cdot n + m}{1 \cdot n} = \frac{0+m}{n} = \frac{m}{n}.$$

If $m/n \in F_R$ then $0/1 + m/n = m/n$ for all $m/n \in F_R$.
So $0/1$ is an identity for $+\colon F_R \times F_R \to F_R$.

(af) Assume $m/n \in F_R$.
Then

$$\frac{m}{n} + \frac{(-m)}{n} = \frac{mn + (-mn)}{n^2} = \frac{0}{n^2}.$$

To show: $0/n^2 = 0/1$.
Since $0 = 0 \cdot 1 = 0 \cdot n^2 = 0$ then $0/n^2 = 0/1$.
So

$$\frac{m}{n} + \frac{(-m)}{n} = \frac{0}{1}.$$

(ag) Assume $p/q, m/n, r/s \in F_R$.

To show: $p/q \cdot (m/n \cdot r/s) = (p/q \cdot m/n) \cdot r/s = pmr/qns$.
By the definition of the operation $\times\colon F_R \times F_R \to F_R$,

$$\frac{p}{q} \cdot \left(\frac{m}{n} \cdot \frac{r}{s}\right) = \frac{p}{q} \cdot \left(\frac{mr}{ns}\right) = \frac{pmr}{qns}.$$

By the definition of the operation $\times\colon F_R \times F_R \to F_R$,

$$\left(\frac{p}{q} \cdot \frac{m}{n}\right) \cdot \frac{r}{s} = \frac{r}{s} = \left(\frac{pm}{qn}\right) \cdot \frac{r}{s} = \frac{pmr}{qns}.$$

So

$$\frac{p}{q} \cdot \left(\frac{m}{n} \cdot \frac{r}{s}\right) = \left(\frac{p}{q} \cdot \frac{m}{n}\right) \cdot \frac{r}{s}.$$

(ah) To show: There is an element $1 \in F_R$ such that if $m/n \in F_R$ then $1 \cdot m/n = m/n$.
Let $1 = 1/1 \in F_R$.
To show: If $m/n \in F_R$ then $1/1 \cdot m/n = m/n$.
Assume $m/n \in F_R$.
Then

$$\frac{1}{1} \cdot \frac{m}{n} = \frac{1 \cdot m}{1 \cdot n} = \frac{m}{n}.$$

So $1/1$ is an identity element for $\times\colon F_R \times F_R \to F_R$.

(ai) Assume $m/n, p/q, r/s \in F_R$.
To show: (aia) $m/n(p/q + r/s) = m/n \cdot p/q + m/n \cdot r/s$.
(aib) $(p/q + r/s)m/n = p/q \cdot m/n + r/s \cdot m/n$.

(aia) By the definitions of the operations

$$\begin{aligned}\frac{m}{n} \cdot \left(\frac{p}{q} + \frac{r}{s}\right) &= \frac{m}{n} \cdot \frac{ps + qr}{qs} \\ &= \frac{m(ps + qr)}{nqs} \\ &= \frac{mps + mqr}{nqs}\end{aligned}$$

and

$$\begin{aligned}\frac{m}{n} \cdot \frac{p}{q} + \frac{m}{n} \cdot \frac{r}{s} &= \frac{mp}{nq} + \frac{mr}{ns} \\ &= \frac{mpns + nqmr}{nqns}.\end{aligned}$$

To show: $\dfrac{mps + mqr}{nqs} = \dfrac{mpns + nqmr}{nqns}$.
To show: $(mps + mqr)nqns = nqs(mpns + nqmr)$.
By commutativity of R and the distributive property in R,

$$\begin{aligned}(mps + mqr)nqns &= nqsn(mps + mqr) \\ &= nqs(mpns + nqmr).\end{aligned}$$

So

$$\frac{mps + mqr}{nqs} = \frac{mpns + nqmr}{nqns}.$$

So

$$\frac{m}{n} \cdot \left(\frac{p}{q} + \frac{r}{s}\right) = \frac{m}{n} \cdot \frac{p}{q} + \frac{m}{n} \cdot \frac{r}{s}.$$

(aib) By the definitions of the operations

$$\begin{aligned}\left(\frac{p}{q}+\frac{r}{s}\right)\cdot\frac{m}{n} &= \frac{ps+qr}{qs}\cdot\frac{m}{n}\\ &= \frac{(ps+qr)m}{qsn}\\ &= \frac{psm+qrm}{qsn}\end{aligned}$$

and

$$\begin{aligned}\frac{p}{q}\cdot\frac{m}{n}+\frac{r}{s}\cdot\frac{m}{n} &= \frac{pm}{qn}+\frac{rm}{sn}\\ &= \frac{pmsn+qnrm}{qnsn}.\end{aligned}$$

To show: $\dfrac{psm+qrm}{qsn}=\dfrac{pmsn+qnrm}{qnsn}$.
To show: $(psm+qrm)qnsn = qsn(pmsn+qnrm)$.
By commutativity of R and the distributive property in R,

$$\begin{aligned}(psm+qrm)qnsn &= qsnn(psm+qrm)\\ &= qsn(pmsn+qnrm).\end{aligned}$$

So

$$\frac{psm+qrm}{qsn}=\frac{pmsn+qnrm}{qnsn}.$$

So

$$\left(\frac{p}{q}+\frac{r}{s}\right)\cdot\frac{m}{n}=\frac{p}{q}\cdot\frac{m}{n}+\frac{r}{s}\cdot\frac{m}{n}.$$

(b) To show: F_R is commutative.
To show: If $m/n, p/q \in F_R$ then $m/n\cdot p/q = p/q\cdot m/n$.
Assume $m/n, p/q\in F_R$.
By the definition of $\times\colon F_R\times F_R\to F_R$.

$$\frac{m}{n}\cdot\frac{p}{q}=\frac{mp}{nq}\quad\text{and}\quad\frac{p}{q}\cdot\frac{m}{n}=\frac{pm}{pq}.$$

By commutativity in R,

$$\frac{mp}{nq}=\frac{pm}{qn}.$$

So

$$\frac{m}{n}\cdot\frac{p}{q}=\frac{p}{q}\cdot\frac{m}{n}$$

So F_R is commutative.

(c) To show: If $x\in F_R$ and $x\neq 0$ then there exists $x^{-1}\in F_R$ such that $xx^{-1}=1$.
Assume $x=m/n\in F_R$ and $m/n\neq 0/1$.
Then, by equality of fractions, $m\cdot 1\neq 0\cdot n$.
So $m\neq 0$.
Let $x^{-1}=n/m$. Note: $n/m\in F_R$ since $m\neq 0$.
To show: $m/n\cdot n/m = 1/1$.
By the definition of $\times\colon F_R\times F_R\to F_R$,

$$\frac{m}{n}\cdot\frac{n}{m}=\frac{mn}{nm}.$$

To show: $\frac{mn}{nm}=\frac{1}{1}$.
But $mn=nm$, by commutativity in R.
So, by the definition of equality of fractions,

$$\frac{mn}{nm}=\frac{1}{1}.$$

So, if $x=m/n$ and $m/n\ \neq\ 0$ then $x^{-1}=n/m\in F_R$ and $xx^{-1}=\frac{m}{n}\cdot\frac{n}{m}=\frac{1}{1}$.
So F_R is a field. □

Proposition C.5.8. — *Let R be an integral domain with identity 1 and let F_R be its field of fractions. Then the map $\varphi\colon R\to F_R$ given by*

$$\begin{array}{cccc}\varphi\colon & R & \longrightarrow & F_R \\ & r & \longmapsto & \frac{r}{1}\end{array}$$

is an injective ring homomorphism.

Proof. — To show: (a) φ is a ring homomorphism. (b) φ is injective.

(a) To show: (aa) If $r,s\in R$ then $\varphi(r+s)=\varphi(r)+\varphi(s)$.
(ab) If $r,s\in R$ then $\varphi(rs)=\varphi(r)\varphi(s)$.
(ac) $\varphi(1)=\frac{1}{1}$.

(aa) Assume $r,s\in R$.
Then

$$\varphi(r+s)=\frac{r+s}{1}\qquad\text{and}\qquad\varphi(r)+\varphi(s)=\frac{r}{1}+\frac{s}{1}.$$

By the definition of $+\colon F_R\times F_R\to F_R$,

$$\frac{r}{1}+\frac{s}{1}=\frac{r\cdot 1+1\cdot s}{1\cdot 1}=\frac{r+s}{1}.$$

So

$$\varphi(r+s)=\varphi(r)+\varphi(s).$$

(ab) Assume $r,s\in R$.
Then, by the definition of $\times\colon F_R\times F_R\to F_R$,

$$\varphi(rs)=\frac{rs}{1}=\frac{r}{1}\cdot\frac{s}{1}=\varphi(r)\varphi(s).$$

(ac) By the definition of $\varphi\colon F_R\to R$,

$$\varphi(1)=\frac{1}{1}.$$

So φ is a ring homomorphism.

(b) To show: If $r,s\in R$ and $\varphi(r)=\varphi(s)$ then $r=s$.
Assume $r,s\in R$ and $\varphi(r)=\varphi(s)$.
Then $r/1=s/1$.
Thus, by the definition of equality of fractions, $1\cdot r=1\cdot s$.
So $r=s$.
So φ is injective.

So φ is an injective ring homomorphism. □

C.6. Proofs: Euclidean Domains, PIDs and UFDs

Theorem C.6.1. — *A Euclidean domain is a principal ideal domain.*

Proof. — Assume R is a Euclidean domain with size function $\sigma\colon (R-\{0\}) \to \mathbb{Z}_{\geqslant 0}$.
Let I be an ideal of R.
To show: There exists an element $a \in R$ such that $I = aR$.

Case 1: $I = \{0\}$.
Case 2: $I \neq \{0\}$.
Let $a \in I$, $a \neq 0$, such that $\sigma(a)$ is as small as possible.
To show: $I = aR$.
To show: (a) $I \subseteq aR$.
(b) $aR \subseteq I$.

(a) Let $b \in I$.
To show: $b \in (a)$.
Then there exist $q, r \in R$ such that $b = aq + r$ where either $r = 0$ or $\sigma(r) < \sigma(a)$.
Since $r = b - aq$ and $b \in I$ and $a \in I$ then $r \in I$.
Since $a \in I$ is such that $\sigma(a)$ is as small as possible we cannot have $\sigma(r) < \sigma(a)$.
So $r = 0$.
So $b = aq$.
So $b \in aR$.
So $I \subseteq aR$.

(b) To show: $aR \subseteq I$.
But $a \in I$.
So $aR \subseteq I$.
So $I = aR$.
So every ideal I of R is a principal ideal.

So R is a principal ideal domain. □

Proposition C.6.2. — *Let $p, q \in R$. Then*

(a) p is a unit $\Longleftrightarrow$ $pR = R$.
(b) p divides q $\Longleftrightarrow$ $qR \subseteq pR$.
(c) p is a proper divisor of q $\Longleftrightarrow$ $qR \subsetneq pR \subsetneq R$.
(d) p is an associate of q $\Longleftrightarrow$ $pR = qR$.
(e) p is irreducible $\Longleftrightarrow$ $pR \neq 0$ and $pR \neq R$ and
If $q \in R$ and $qR \supseteq pR$ then either $qR = pR$ or $qR = R$.

Proof. —

(a) $\Rightarrow$: Assume p is a unit.
Let $u \in R$ such that $up = 1$.
Then $1 = up \in pR$.
So, if $r \in R$ then $r \cdot 1 \in pR$.
So $R \subseteq (p) \subseteq R$.
So $(p) = R$.

$\Leftarrow$: Assume $pR = R$.
Then $1 \in pR$.
So there exists $i \in R$ such that $pu = 1$.

So p is a unit.
(b) $\Rightarrow$: Assume p divides q.
So there exists $a \in R$ such that $pa = q$.
So $q \in pR$.
So $qR \subseteq pR$.

$\Leftarrow$: Assume $qR \subseteq pR$.
Then $q \in pR$.
So there exists $a \in R$ such that $q = ap$.
So p divides q.

(c) $\Rightarrow$: Assume p is a proper divisor of q.
Let $a \in R$ such that $q = ap$ and such that a is not a unit.
To show: (ca) $qR \subseteq pR$. (cb) $qR \neq pR$. (cc) $pR \neq R$.
(ca) Since $q = pa$ then $q \in pR$,
So $qR \subseteq pR$.
(cb) Proof by contradiction. YIKES???????
Assume $(q) = (p)$.
Then there exists $b \in R$ such that $p = bq$.
So $q = pa = baq$.
Thus, since R is an integral domain then the cancellation law gives that $ba = 1$.
So a is a unit.
Contradiction, a is not a unit.
So $qR \neq pR$.
(cc) By part (a), since p is not a unit then $pR \neq R$.

(c) $\Leftarrow$: Assume $qR \subsetneqq pR \subseteq R$.
To show: p is a proper divisor of q.
To show: (ca) There exists $a \in R$ such that $q = ap$.
(cb) a is not a unit.
(cc) p is not a unit.
(ca) By part (a), since $qR \subseteq pR$ then p divides q.
So there exists $a \in R$ such that $q = ap$.
(cb) Proof by contradiction. YIKES????
Assume a is a unit.
Then there is a $u \in R$ such that $ua = 1$.
So $p = uap = uq$.
So $p \in qR$.
So $pR \subseteq qR$.
So $pR = qR$.
This is a contradiction to the assumption $qR \subseteq pR$.
So a is not a unit.
(cc) By part (a), since $pR \neq R$ then p is not a unit.

(d) $\Rightarrow$: Assume p is an associate of q.
To show: (da) $pR \subseteq qR$.
(db) $qR \subseteq pR$.

(da) Then there exists a unit $a \in R$ such that $p = aq$.
So $p \in qR$.
So $pR \subseteq qR$.

(db) Since $p = aq$ and a is a unit then $q = a^{-1}p$.
So $q \in pR$.
So $qR \subseteq pR$.
So $qR = pR$.

(d) $\Leftarrow$: Assume $qR = pR$.
To show: (da) There exists $a \in R$ such that $p = aq$.
(db) a is a unit.

(da) Since $pR \subseteq qR$ then $p \in qR$.
So there exists $a \in R$ such that $p = aq$.

(db) Since $qR \subseteq pR$ then $q \in pR$.
So there exists $b \in R$ such that $q = bp$.
So $p = aq = abp$.
Then, by the cancellation law, $1 = ab$.
So a is a unit.

(e) $\Rightarrow$: Assume p is irreducible.
To show: (ea) $pR \neq \{0\}$.
(eb) $pR \neq R$.
(ec) If $q \in R$ and $qR \subseteq pR$ then either $qR = pR$ or $qR = R$.

(ea) Since $p \neq 0$then $pR \neq \{0\}$.

(eb) Since p is not a unit tnen, by part (a), $pR \neq R$.

(ec) Assume $q \in R$ and $qR \supseteq pR$.
Proof by contradiction. YIKES??????
Assume $qR \neq pR$ and $qR \neq R$.
Then $R \supsetneq qR \supsetneq pR$.
So, by part (c), q is a proper divisor of p.
This is a contradiction to p being irreducible.
So either $qR = pR$ or $qR = R$.

(e) $\Leftarrow$: Assume $pR \neq 0$ and $pR \neq R$ and if $q \in R$ and $qR \supseteq pR$ then either $qR = pR$ or $qR = R$.
To show: (ea) $p \neq 0$.
(eb) p is not a unit.
(ec) p has no proper divisor.

(ea) Since $pR \neq \{0\}$ then $p \neq 0$.

(eb) Since $pR \neq R$ then, by part (a), p is not a unit.

(ec) Assume p has a proper divisor $q \in R$.
Then, by part (c), $pR \subsetneq qR \subsetneq R$.
But this is a contradiction to the assumption that if $q \in R$ and $qR \supseteq pR$ then either $qR = pR$ or $qR = R$.
So p has no proper divisor.

□

Lemma C.6.3. — *If R is a principal ideal domain and $p \in R$ is an irreducible element of R then pR is a prime ideal.*

Proof. — Let $p \in R$ be an irreducible element.
Let $a, b \in R$ and suppose $ab \in pR$.
To show: If $a \notin pR$ then $b \in pR$.
Assume $a \notin pR$. Then let $d \in R$ such that $dR = \langle a, p\rangle$, the ideal generated by a and p.
Since $p \in \langle a, p\rangle$ then $pR \subseteq \langle a, p\rangle = dR$.
Since $a \notin pR$ then $dR = \langle a, p\rangle \neq pR$.
Thus, since p is irreducible then $\langle a, p\rangle = dR = 1 \cdot R = R$.
So there exist $r, s \in R$ such that $ra + sp = 1$.
So $b = rab + spb$.
Thus, since $ab \in pR$ and $pb \in pR$ then $b \in pR$.
So pR is a prime ideal. □

Lemma C.6.4. — *Let R be a principal ideal domain. There does* not *exist an infinite sequence of elements $a_1, a_2, \ldots \in R$ such that $(0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$.*

Proof. — Proof by contradiction. FIX THIS BY SHOWING CONTRAPOSITIVE
Suppose $a_1, a_2, \ldots \in R$ is an infinite sequence of elements such that $(0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$.
First we show that

$$I = \bigcup_{i \in \mathbb{Z}_{\geqslant 1}} (a_i) \qquad \text{is an ideal.}$$

To show: (a) If $a \in I$ and $r \in R$ then $ra \in I$.
(b) If $a_1, a_2 \in I$ then $a_1 + a_2 \in I$.

(a) Let $a \in I$ and $r \in R$.
Then there exists $n \in \mathbb{Z}_{\geqslant 1}$ such that $a \in (a_n)$.
So $ra \in (a_n)$.
So $ra \in I$.

(b) Let $a_1, a_2 \in I$.
Then there exists $m, n \in \mathbb{Z}_{\geqslant 1}$ such that $a_1 \in (a_m)$ and $a_2 \in (a_n)$.
Since $(a_m) \subseteq (a_{m+n})$ and $(a_n) \subseteq (a_{m+n})$ then $a_1, a_2 \in (a_{m+n})$.
So $a_1 + a_2 \in (a_{m+n})$.
So $a_1 + a_2 \in I$.
So I is an ideal.

Since R is a principal ideal domain then there exists $a \in R$ such that $I = (a)$.
Since $a \in I$ then there exists $n \in \mathbb{Z}_{\geqslant 1}$ such that $a \in (a_n)$.
So $I = (a) \subseteq (a_n) \subseteq (a_{n+1}) \subseteq I$.
So $(a_n) = (a_{n+1})$.
But this is a contradiction to the assumption that $(a_n) \subsetneq (a_{n+1})$.
So R does not contain an infinite sequence of elements $a_1, a_2, \ldots \in R$ such that $(0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$. □

Theorem C.6.5. — *A principal ideal domain is a unique factorization domain.*

Proof. — Let R be a principal ideal domain.
To show: (a) If $x \in R$ then there exist irreducible elements $p_i, \ldots, p_m \in R$ such that $x = p_i \cdots p_m$.
(b) If $x \in R$ and $x = p_1 \cdots p_m$ and $x = uq_1 \cdots q_n$ where $p_1, \ldots, p_m, q_1, \ldots, q_n$ are irreducible and u is a unit then $m = n$ and there exists a permutation $\sigma\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$ and units $u_1, \ldots, u_n \in R$ such that $q_i = u_i p_{\sigma(i)}$ for $i \in \{1, \ldots, n\}$.

(a) Proof by contradiction. YIKES???????

Suppose $x \in R$ and x cannot be written as $x = p_1 \cdots p_m$ with $p_1, \ldots, p_m$ are irreducible.
Then $x = x$ is not irreducible.
So $x = a_1 b_1$ for some $b_1 \in R$ and some a_1 which is not irreducible and
which is a proper divisor of x.
So $x = a_2 b_2 b_1$ where $a_1 = a_2 b_2$ for some $b_2 \in R$ and some a_2 which is not irreducible and
which is a proper divisor of a_1.
We can continue this process and obtain a sequence of elements $a_1, a_2, \ldots \in R$ such that
each a_{i+1} is a proper divisor of a_i.
So, by Proposition 3.2.4 (c), $0 \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$.
But this is a contradiction to Lemma 3.2.8.????
So x can be written as $x = p_1 \cdots p_m$ where all $p_1, \ldots, p_m$ are irreducible.

(b) Suppose $x \in R$ and $x = p_1 \cdots p_n = u q_1 \cdots q_m$ where $u \in R$ is a unit and $p_1, \ldots, p_n$, $q_1, \ldots, q_m \in R$ are irreducible.
To show: $m = n$ and there is a bijective map $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ such that
$q_i = u_i p_{\sigma(i)}$ for some $u_i \in R$.
The proof is by induction on n.
Case $n = 1$.
Suppose $x \in R$ and $x = p_1 = u q_1 \cdots q_m$ where $u \in R$ is a unit and $p_1, q_1, \ldots, q_m \in R$
are irreducible.
Suppose $m > 1$.
Then using Proposition 3.2.4 d), $(q_1 \cdots q_m) = (u q_1 \cdots q_m) = (p_1)$.
So $q_1 \cdots q_m \in (p_1)$.
Since p_1 is irreducible, by Lemma 3.2.7, (p_1) is a prime ideal.
So $q_j \in (p_1)$ for some $1 \leqslant j \leqslant m$.
So $(q_j) \subseteq (p_1)$.
Since q_j is irreducible, $(q_j) = (p_1)$.
So $q_j = u_1 p_1$ for some unit $u_1 \in R$.
So $q_1 \cdots q_{j-1} (u_1 p_1) q_{j+1} \cdots q_m = p_1$.
By the cancellation law, $u_1 q_1 \cdots q_{j-1} q_{j+1} \cdots q_m = 1$.
So q_1 is a unit.
This is a contradiction to q_1 being irreducible.
So $m = 1$.
So $x = p_1 = u q_1$ where $u \in R$ is a unit.

Induc tion assumption: Assume that if $k < n$ and $y = a_1 a_2 \cdots a_k = u' b_1 \cdots b_l$ where $u' \in R$
is a unit and $a_1, \ldots, a_k$, $b_1, \ldots, b_l \in R$ are irreducible then $l = k$ and there is a bijective
map $\sigma'\colon \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ such that for each i, $b_i = u_i a_{\sigma(i)}$ for some unit $u_i \in R$.

Assume that $x = p_1 \cdots p_n = u q_1 \cdots q_m$ where $u \in R$ is a unit and $p_1, \ldots, p_n$, $q_1, \ldots, q_m \in R$ are all irreducible.
We know $p_1 \cdots p_n = u q_1 \cdots q_m$.

So $(uq_1 \cdots q_m) = (q_1 \cdots q_m) \subseteq (p_n)$.
So $q_1 \cdots q_m \in (p_n)$.
By Lemma 3.2.7, (p_n) is a prime ideal.
So $q_j \in (p_n)$ for some j.
So $(q_j) \subseteq (p_n)$.
So $(q_j) = (p_n)$ since q_j is irreducible.
So q_j and p_n are associates.
So $u_n p_n = q_j$ for some unit $u_n \in R$.
Then $p_1 \cdots p_n = uq_1 \cdots q_{j-1}(u_n p_n)q_{j+1} \cdots q_m$.
By cancellation, $p_1 \cdots p_{n-1} = (uu_n)q_1 \cdots \hat{q}_j \cdots q_m$,
where the hat over the q_j denotes that the q_j is omitted from the product.
By the induction hypothesis, $m - 1 = n - 1$ and there exists a bijective map $\sigma' \colon \{1, 2, \ldots, j-1\} \cup \{j+1, \ldots, n\} \to \{1, 2, \ldots, n-1\}$ such that $u_i p_{\sigma'(i)} = q_i$ where
$u_i \in R$ is a unit.
So $m = n$.
Define $\sigma \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by

$$\sigma(i) = \begin{cases} \sigma'(i), & \text{if } i \neq j; \\ n, & \text{if } i = j. \end{cases}$$

Then $q_i = u_i p_{\sigma(i)}$ for each $1 \leqslant i \leqslant n$.

So R is a unique factorization domain. □

Proposition C.6.6. — *Let R be a unique factorization domain and let $a_0, a_1, \ldots, a_n \in R$. Then*

(a) $\gcd(a_0, a_1, \ldots, a_n)$ *exists.*
(b) $\gcd(a_0, a_1, \ldots, a_n)$ *is unique up to multiplication by a unit.*

Proof. — (a) Let $P = \{p_1, p_2, \ldots, p_k\}$ be a maximal set of irreducible elements such that

(1) Every $p_j \in P$ divides some a_i, $0 \leqslant i \leqslant n$.
(2) No two of the elements of P are associate.

Let $a_i = q_1 \cdots q_m$ be a factorization of a_i into irreducible elements.
Each factor q_r, $1 \leqslant r \leqslant m$, is associate to some $p_{j_r} \in P$, otherwise $P' = P \cup \{q_r\}$ is a larger set satisfying (1) and (2).
So for each factor q_r, $1 \leqslant r \leqslant m$, $q_r = u_r p_{j_r}$ for some unit $u_r \in R$ and some $p_{j_r} \in P$. So

$$\begin{aligned} a_i &= u_1 p_{j_1} u_2 p_{j_2} \cdots u_r p_{j_r} \\ &= u p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_k^{e_{ik}} \end{aligned}$$

where $u \in R$ is a unit and e_{ij} are integers $e_{ij} \geqslant 0$.
Let $e_j = \min_i\{e_{ij}\}$.
Define $d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.
To show: (aa) d divides a_i for all $1 \leqslant i \leqslant n$. (ab) If d' divides a_i for all $1 \leqslant i \leqslant n$ then d' divides d.

(aa) Let i be such that $1 \leqslant i \leqslant n$.
Since $e_j \leqslant e_{ij}$ for all $1 \leqslant j \leqslant k$,

$$d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{divides } a_i = u p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_k^{e_{ik}}.$$

So d divides a_i for all $1 \leqslant i \leqslant n$.

(ab) Assume d' divides a_i for all $1 \leqslant i \leqslant n$.
Let $d' = q_1 \cdots q_m$ be a factorization of d' into irreducible elements.
Since d' divides a_i for all $1 \leqslant i \leqslant n$, each factor q_r of d' divides a_i for all $1 \leqslant i \leqslant n$.
So each q_r is associate to some p_{j_r}, otherwise $P' = P \cup \{q_r\}$
is a larger set satisfying (1) and (2).
So, for each factor q_r of d', $q_r = u_r p_{j_r}$ for some unit $u_r \in R$ and some $p_{j_r} \in P$.
So

$$d' = u_1 p_{j_1} u_2 p_{j_2} \cdots u_k p_{j_k} = u p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k},$$

where $u \in R$ is a unit and the f_j are integers $f_j \geqslant 0$.
Since d' divides a_i for all $1 \leqslant i \leqslant n$, then for each f_j,

$$f_j \leqslant e_{ij} \text{for all } 1 \leqslant i \leqslant n.$$

So, for each f_j, $f_j \leqslant \min_i\{e_{ij}\}$.
So, for each f_j, $f_j \leqslant e_j$.
So $d' = u p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ divides $d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

So d is a greatest common divisor of $a_1, a_2, \ldots, a_n$.

(b) Assume d and d' are both greatest common divisors of $a_0, \ldots, a_n$.
Then d divides d' and d' divides d.
So $d = ad'$ for some $a \in R$ and $d' = bd$ for some $b \in R$.
So $d = abd$.
By the cancellation law, $ab = 1$.
So a, b are units in R.

□

C.7. Extensions: Euclidean Domains, PIDs and UFDs

Example 1.

Proposition C.7.1. — *Let R be a commutative ring and let $x \in R$. Let xR denote the set*

$$xR = \{xr \mid r \in R\}.$$

Then $(x) = Rx$.

Proof. —
To show: (a) $(x) \subseteq Rx$. (b) $Rx \subseteq (x)$.

(a) To show: (aa) $x \in Rx$.
(ab) Rx is an ideal.

(aa) $x = 1x \in Rx$.

(ab) If $r_1x, r_2x \in Rx$ then $r_1x + r_2x = (r_1 + r_2)x \in Rx$.
If $rx \in Rx$ and $s \in R$ then $s(rx) = (sr)x \in Rx$.
So Rx is an ideal.
So $(x) \subseteq Rx$.

(b) Let $rx \in Rx$.
Then, since $x \in (x)$ and (x) is an ideal then $rx \in (x)$.
So $(x) = Rx$.
So $Rx \subseteq (x)$.

□

Example 2. Let R be a factorial ring. Let $a_0, a_1, \dots, a_n \in R$. A **greatest common divisor**, $\gcd(a_0, a_1, \dots, a_n)$, of $a_0, a_1, \dots, a_n$ is an element $d \in R$ such that

(a) d divides a_i for all $i = 0, 1, \dots, n$.
(b) If d' divides a_i for all $i = 0, 1, \dots, n$ then d' divides d.

Let R be a factorial ring and let $a_0, a_1, \dots, a_n \in R$. Then show that

(a) $\gcd(a_0, a_1, \dots, a_n)$ exists.
(b) $\gcd(a_0, a_1, \dots, a_n)$ is unique up to multiplication by a unit.

Example 3. Let R be a factorial ring and let $p \in R$ be an irreducible element. Show that (p) is a prime ideal of R. **Example 4.** Show that the ring of integers $\mathbb{Z}$ with size function given by

$$\begin{array}{rccc} \sigma\colon & \mathbb{Z} - \{0\} & \to & \mathbb{Z}_{\geqslant 0} \\ & a & \mapsto & |a|. \end{array}$$

is a Eucilidean domain.

Example 5. $F[x]$ is a Euclidean domain with

$$\begin{array}{rccc} \sigma\colon & F[x] - \{0\} & \to & \mathbb{Z}_{\geqslant 0} \\ & p(x) & \mapsto & \deg\bigl(p(x)\bigr) \end{array}$$

Example 6. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain with

$$\begin{array}{rccc} \sigma\colon & \mathbb{Z}[i] - \{0\} & \to & \mathbb{Z}_{\geqslant 0} \\ & a + bi & \mapsto & a^2 + b^2. \end{array}$$

Example 7. $\mathbb{Z}[x]$ is a factorial ring not a principal ideal domain.
So is $\mathbb{Z}[\sqrt{-5}]$.
$\langle x, 2\rangle \subseteq \mathbb{Z}[x]$ is not principal.

Example 8. $R = \bigl\{a + b(1 + \sqrt{19}i)/2 \mid a, b \in \mathbb{Z}\bigr\}$ is a principal ideal domain that is <u>not</u> a Euclidean domain.

Example 8. Eisenstein criterion.
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}_{>0}$ be a prime integer.

(a) p does not divide a_n,
(b) p divides each of $a_{n-1}, a_{n-2}, \dots, a_0$,
(c) p^2 does not divide a_0,

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. — (sketch)
Let $\pi_p\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ denote the quotient map $a \mapsto \overline{a}$.
Let $\hat{\pi}_p\colon \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ be the extension of π_p to polynomial rings.
By (a) and (b), $\hat{\pi}_p\bigl(f(x)\bigr) = \overline{a}_n x^n$ where $\overline{a}_n = \pi_p(a_n)$.
Assume $f(x)$ is not irreducible.
Then $f(x) = g(x)h(x)$ for some $g(x) = g_k x^k + \cdots + g_0$ and $h(x) = h_l x^l + \cdots + h_0$.
Since $\hat{\pi}_p$ is a homomorphism, $\hat{\pi}_p\bigl(f(x)\bigr) = \overline{a}_n x^n = (\overline{g}_k x^k + \cdots + \overline{g}_0)(\overline{h}_l x^l + \cdots + \overline{h}_0)$.
The only way to factor $\overline{a}_n x^n$ is $(\overline{g}_k x^k)(\overline{h}_l x^l) = \overline{a}_n x^n$.
So $\overline{g}_{k-1} = \cdots = \overline{g}_0 = \overline{h}_{l-1} = \cdots = \overline{h}_0 = 0$.

So p divides g_0 and p divides h_0.
Since $f(x) = \big(g(x)\big)\big(h(x)\big)$ then $a_0 = g_0h_0$.
So p^2 divides a_0.
This contradicts assumption (c).
So $f(x)$ is irreducible. □

Example 9. Let $f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ and let p be a prime integer such that p does not divide a_n. Let $\hat{\pi}_p \colon \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ be the canonical homomorphism (see Ex. X). If $\hat{\pi}_p\big(f(x)\big)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 9. If $f(x) \in \mathbb{Z}[x]$, deg $\big(f(x)\big) > 0$, and $f(x)$ is irreducible in $\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 10. Let $f(x) \in \mathbb{Z}[x]$. $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if

either $f(x) = \pm p$, where p is a prime integer,
or $f(x)$ is a primitive polynomial and $f(x)$ is irreducible in $\mathbb{Q}[x]$.

CHAPTER D

TOWARDS CLASSIFYING GROUPS

D.1. Products and semidirect products of Groups

Direct products and semidirect products will be our main tools for classifying groups.

D.1.1. Direct Products. — Suppose H and K are groups. The idea is to make $H \times K$ into a group.

Definition D.1.1. —

- The *direct product*, $H \times K$, of two groups H and K is the set $H \times K$ with the operation given by

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

for $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

- More generally, given groups $G_1, \ldots, G_n$, the **direct product** $G = \prod_i G_i$ is the set $G = \prod_i G_i$ with the operation given by

$$(\ldots, h_i, \ldots)(\ldots, k_i, \ldots) = (\ldots, h_i k_i, \ldots),$$

where $h_i, k_i \in G_i$ and $h_i k_i$ is given by the operation in the group G_i.

HW: Show that these are good definitions, i.e., that, as defined above, $H \times K$ and $\prod_i G_i$ are groups with identities given by $(1_H, 1_K)$ and $(\ldots, 1_{G_i}, \ldots)$ respectively (1_{G_i} denotes the identity in the group G_i).

The main theorem is the following:

Theorem D.1.1. — *Let H, K be subgroups of a group G and let 1_G denote the identity in G. Suppose*

(a) $G = HK$,
(b) Both H and K are normal in G, and
(c) $H \cap K = \{1_G\}$.

Then

$$\begin{array}{ccc} H \times K & \xrightarrow{\sim} & G \\ (h, k) & \longmapsto & hk \end{array} \quad \text{is an isomorphism.}$$

D.1.2. Automorphisms. — Automorphisms are needed to define semidirect products.

Definition D.1.2. — An **automorphism** is an isomorphism between a group and *itself.*

Note: There can be many different automorphisms of a group G.

HW: Give a concrete example of a group with more than one automorphism.

Definition D.1.3. — Let G be a group.

- The **automorphisms** of G, $\mathrm{Aut}(G)$, is the set of automorphisms of G.
- Let $g \in G$. **Conjugation by** g is the map c_g given by

$$\begin{array}{rccc} c_g\colon & G & \to & G \\ & h & \mapsto & ghg^{-1} \end{array}$$

- $\mathrm{Inn}(G)$ is the set $\mathrm{Inn}(G) = \{c_g \mid g \in G\}$.

Theorem D.1.2. — *Let G be a group.*

(a) $\mathrm{Aut}(G)$ *with the operation of composition of functions is a group.*

(b) The map

$$\begin{array}{rccc} c\colon & G & \to & \mathrm{Aut}(G) \\ & g & \mapsto & c_g \end{array}$$

is a well defined homomorphism. Furthermore,

$$\mathrm{im}\ c = \mathrm{Inn}(G) \qquad \textit{and} \qquad \ker\ c = Z(G),\ \textit{the center of}\ G.$$

(c) $\mathrm{Inn}(G)$ *is a subgroup of* $\mathrm{Aut}(G)$.

HW: Give an example of a group G such that $\mathrm{Inn}(G) \neq \mathrm{Aut}(G)$.

HW: Prove that $G/Z(G) \simeq \mathrm{Inn}(G)$.

D.1.3. Semidirect Products. — The motivation for semidirect products comes from the fact that if G is a group and if H and K are subgroups of G with K normal in G then HK is a subgroup of G. Suppose that $HK = G$. That raises the question: Can G somehow be expressed nicely as a combination of the two groups H and K? In the case when both subgroups were normal, and $H \cap K$ was $\{1\}$ then $G \simeq H \times K$ (Theorem D.1.1). Semidirect products treat the case when only one of H and K are normal.

Definition D.1.4. — Let H and K be groups and let

$$\begin{array}{rccc} \theta\colon & H & \to & \mathrm{Aut}(K) \\ & h & \mapsto & \theta_h \end{array} \quad \text{be a homomorphism.}$$

The **semidirect product of** H **and** K **via** θ, $H \times_\theta K$, is the group given by the Cartesian product $H \times K$ with the operation given by

$$(h_1, k_1)(h_2, k_2) = \big(h_1 h_2, \theta_{h_2}(k_1) k_2\big)$$

for $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Proposition D.1.3. — *Let H and K be groups and let $\theta\colon H \to \mathrm{Aut}(K)$ be a homomorphism. Then $H \times_\theta K$ is a group.*

Theorem D.1.4. — *Suppose H and K are subgroups of a group G with K normal in G such that*

(a) $G = HK$,

(b) K is normal in G, and

(c) $H \cap K = (1)$, where 1 is the identity in G.

Let θ be given by

$$\begin{array}{rccc} \theta\colon & H & \to & \mathrm{Aut}(K) \\ & h & \mapsto & c_h, \end{array} \quad \textit{where} \quad \begin{array}{rccc} c_h\colon & K & \to & K \\ & k & \mapsto & hkh^{-1}. \end{array}$$

Then θ is a function, θ is a group homomorphism and

$$\begin{array}{ccc} H \times_\theta K & \xrightarrow{\sim} & G \\ (h,k) & \longmapsto & hk \end{array} \quad \textit{is an isomorphism.}$$

HW: Prove that if $\ker\theta = K$, then $H \times_\theta K = H \times K$.

HW: Prove that if $\mathrm{im}\,\theta = (1)$, then $H \times_\theta K = H \times K$.

D.2. p-groups and Sylow p-subgroups

D.2.1. p-Groups. —

Definition D.2.1. — Let $p \in \mathbb{Z}_{>0}$ be a prime.

- A **p-group** is a group of order p^a with $a \in \mathbb{Z}_{>0}$.

Proposition D.2.1. — *If G is a p-group then G contains an element of order p.*

Proposition D.2.2. — *If G is a p-group and* $\mathrm{Card}(G) \neq 1$ *then the center of G is not* $\{1\}$,

$$\mathrm{Card}(Z(G)) \neq 1.$$

Proposition D.2.3. — *Let $p \in \mathbb{Z}_{>0}$ be a prime and let G be a group of cardinality p^2. Then G is abelian.*

Theorem D.2.4. — *If G is a p-group of order p^a, then there exists a chain, of normal subgroups of G,*

$$(1) \subseteq N_1 \subseteq N_2 \subseteq \ldots \subseteq N_{a-1} \subseteq G,$$

such that $\mathrm{Card}(N_i) = p^i$.

D.2.2. The Sylow Theorems. —

Definition D.2.2. — Let $p \in \mathbb{Z}_{>0}$ be prime, let $a, b \in \mathbb{Z}_{>0}$ such that p does not divide b and let G be a finite group of cardinality $p^a b$.

- A **p-Sylow subgroup of** G is a subgroup of G of cardinality p^a.

Theorem D.2.5. — First Sylow theorem. *Let $p \in \mathbb{Z}_{>0}$ be prime, let $a, b \in \mathbb{Z}_{>0}$ such that p does not divide b and let G be a finite group of cardinality $p^a b$.*

G has a subgroup of order p^a.

Theorem D.2.6. — Second Sylow theorem. *Let $p \in \mathbb{Z}_{>0}$ be prime, let $a, b \in \mathbb{Z}_{>0}$ such that p does not divide b and let G be a finite group of cardinality $p^a b$.*

All the p-Sylow subgroups of G are conjugates of each other.

Theorem D.2.7. — Third Sylow theorem. *Let $p \in \mathbb{Z}_{>0}$ be prime, let $a, b \in \mathbb{Z}_{>0}$ such that p does not divide b and let G be a finite group of cardinality $p^a b$.*

The number of p-Sylow subgroups of G is $1 \bmod p$.

D.3. Solvable and nilpotent Groups

Definition D.3.1. — Let G be a group. Let $g, h \in G$.

- The **commutator** of g and h is
$$[g,h] = g^{-1}h^{-1}gh.$$

Definition D.3.2. — Let G be a group.

- The **derived group** $[G,G]$ of G is the group generated by all commutators of elements of G,
$$[G,G] = \big\langle [g,h] \mid g,h \in G \big\rangle.$$

Definition D.3.3. — Let G be a group.

- The **derived series** of G is the sequence
$$G = D^0(G) \supseteq D^1(G) \supseteq D^2(G) \supseteq \cdots, \qquad \text{where } D^i(G) = \big[D^{i-1}(G), D^{i-1}(G)\big].$$
- The **lower central series** of G is the sequence
$$G = C^1(G) \supseteq C^2(G) \supseteq C^3(G) \supseteq \cdots, \qquad \text{where } C^i(G) = \big[G, C^{i-1}(G)\big].$$
- The **upper central series** of G is the sequence
$$(1) = Z^0(G) \subseteq Z^1(G) \subseteq Z^2(G) \subseteq \cdots,$$
where $Z^i(G)$ is the subgroup of G such that $Z\big(G/Z^{i-1}(G)\big) = Z^i(G)/Z^{i-1}(G)$.

Definition D.3.4. —

- A group G is **nilpotent** if there exists $n \in \mathbb{Z}_{>0}$ such that $C^{n+1}(G) = \{1\}$.
- The **nilpotency class** of a nilpotent group G is the least integer $n \in \mathbb{Z}_{>0}$ such that $C^{n+1}(G) = \{1\}$.

Proposition D.3.1. —

(a) A group G is nilpotent if there exists $n \in \mathbb{Z}_{>0}$ such that $Z^{n+1}(G) = G$.
(b) The least integer n such that $Z^{n+1}(G) = G$ is the nilpotency class of G.

Definition D.3.5. —

- A group G is **solvable** if there exists $n \in \mathbb{Z}_{>0}$ such that $D^n(g) = \{1\}$.
- If G is a solvable group the least integer $n \in \mathbb{Z}_{>0}$ such that $D^n(G) = \{1\}$ is the **solvability class** of G.

Proposition D.3.2. — *Every nilpotent group is solvable.*

(1) 6.12 CRD Theorem G is a finite nilpotent group.
   (a) Each Sylow subgroup is normal in G.
   (b) G is the direct product of its Sylow subgroups.
(2) p-group ⇒ nilpotent ⇒ solvable ⇒ supersolvable.

Proposition D.3.3. — *A finite group is **solvable** if and only if it has a composition series whose factors are cyclic of prime order.*

Definition D.3.6. — A finite group G is **supersolvable** if G is solvable and G has a composition series
$$G \supseteq G_1 \supseteq \cdots \supseteq G_{s+1} = \{1\}$$
such that G_i is a normal subgroup of G for all i.

Definition D.3.7. — A **composition series** of a group G is a chain of subgroups

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_s \supseteq G_{s+1} = (1)$$

such that $G_i/G_{i+1} \neq (1)$ are simple.

Solvable and Nilpotent Groups

(1) A_n is solvable if $n \leqslant 4$ and A_n is not solvable if $n \geqslant 5$.
(2) S_n is solvable if $n \leqslant 4$ and not solvable if $n \geqslant 5$.
(3) abelian $\Rightarrow$ solvable
(4) *Burnside Theorem* If $|G| = p^a q^b$ then G is solvable.
(5) S_3 is solvable not nilpotent.

Theorem D.3.4. — *A finite group G is solvable if and only if $\Im$ composition series with cyclic factors of prime order.*

D.3.1. Proofs for Group products. —

Theorem D.3.5. — *Let H, K be subgroups of a group G and let 1_G denote the identity in G. Suppose*

(a) $G = HK$,
(b) Both H and K are normal in G, and
(c) $H \cap K = (1_G)$.

Then $G \simeq H \times K$.

Proof. —
To show: G is isomorphic to $H \times K$.
To show: There exists an isomorphism $\beta\colon G \to H \times K$.
Define

$$\begin{array}{rccc} \alpha\colon & H \times K & \to & G \\ & (h,k) & \mapsto & hk \end{array}$$

To show: (a) α is a homomorphism.
(b) α is injective.
(c) α is surjective.

(a) Let $(h_1,k_1),(h_2,k_2) \in H \times K$.
To show: $\alpha\big((h_1,k_1)(h_2,k_2)\big) = \alpha\big((h_1,k_1)\big)\alpha\big((h_2,k_2)\big)$.

$$\begin{aligned} \alpha\big((h_1,k_1)(h_2,k_2)\big) &= \alpha\big((h_1h_2,k_1k_2)\big) \\ &= h_1h_2k_1k_2 \\ &= h_1k_1k_1^{-1}h_2k_1h_2^{-1}h_2k_2 \\ &= h_1k_1(k_1^{-1}h_2k_1h_2^{-1})h_2k_2 \\ &= \alpha(h_1,k_1)(k_1^{-1}h_2k_1h_2^{-1})\alpha(h_2,k_2). \end{aligned}$$

Since H is normal in G, $k_1^{-1}h_2k_1 \in H$.
So $(k_1^{-1}h_2k_1)h_2^{-1} \in H$.
Since K is normal in G then $h_2k_1h_2^{-1} \in K$.
So $k_1^{-1}(h_2k_1h_2^{-1}) \in K$.
Since $H \cap K = (1_G)$ then $k_1^{-1}h_2k_1h_2^{-1} = 1_G$.
So $\alpha\big((h_1,k_1)(h_2,k_2)\big) = \alpha(h_1,k_1)\alpha(h_2,k_2)$.
So α is a homomorphism.

(b) By Proposition XXX, we need to show: $\ker\alpha = \{(1_G,1_G)\}$, where 1_G is the identity in G.
Let $(h,k) \in \ker\alpha$. Then

$$\alpha\big((h,k)\big) = hk = 1_G.$$

So $h = k^{-1}$ and $h \in H \cap K$. So $h = 1_G$.
Also $k = h^{-1}$ and $k \in H \cap K$. So $k = 1_G$.
So $(h,k) = (1_G,1_G)$.
So $\ker\alpha = \{(1_G,1_G)\}$.
So α is injective.

(c) To show: If $g \in G$ then there exists $h \in H$ and $k \in K$ such that $g = \alpha\big((h,k)\big)$.
Let $g \in G$.

Since $G = HK$ then there exists $h \in H$ and $k \in K$ such that $g = hk$. So

$$g = hk = \alpha(h, k).$$

So α is surjective.

So α is an isomorphism. □

Theorem D.3.6. — *Let G be a group.*

(a) $\mathrm{Aut}(G)$ *with the operation of composition of functions is a group.*

(1) (b)] The map

$$\begin{array}{cccc} c\colon & G & \to & \mathrm{Aut}(G) \\ & g & \mapsto & c_g \end{array}$$

is a well defined homomorphism. Furthermore,

$$\mathrm{im}\, c = \mathrm{Inn}(G) \qquad \textit{and} \qquad \ker c = Z(G), \textit{ the center of } G.$$

(c) $\mathrm{Inn}(G)$ *is a subgroup of* $\mathrm{Aut}(G)$*.*

Proof. — (a) To show: (aa) The operation is well defined.

(ab) There is an element $\iota_G \in \mathrm{Aut}(G)$ such that if for $\alpha \in \mathrm{Aut}(G)$ then $\iota_G \circ \alpha = \alpha = \alpha \circ \iota_G$.

(ac) If $\alpha \in \mathrm{Aut}(G)$ then there exists an element $\alpha^{-1} \in \mathrm{Aut}(G)$ such that $\alpha \circ \alpha^{-1} = \iota_G = \alpha^{-1} \circ \alpha$.

(aa) To show: (aaa) If α, $\beta \in \mathrm{Aut}(G)$ then $\alpha \circ \beta \in \mathrm{Aut}(G)$.

(aab) If $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathrm{Aut}(G)$ and $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$ then $\alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2$.

(aaa) Assume $\alpha, \beta \in \mathrm{Aut}(G)$.

To show: $\alpha \circ \beta \in \mathrm{Aut}(G)$.

To show: (aaaa) $\alpha \circ \beta$ is bijective.

(aaab) $\alpha \circ \beta$ is a homomorphism.

(aaaa) By § XXX Ex. XXX $\alpha \circ \beta$ is a bijective map from G to G.

(aaab) Assume $g_1, g_2 \in G$. Then, since both α and β are homomorphisms,

$$\begin{aligned}(\alpha \circ \beta)(g_1 g_2) &= \alpha\big(\beta(g_1 g_2)\big) \\ &= \alpha\big(\beta(g_1)\beta(g_2)\big) \\ &= \alpha\big(\beta(g_1)\big)\alpha\big(\beta(g_2)\big) \\ &= (\alpha \circ \beta)(g_1) \cdot (\alpha \circ \beta)(g_2).\end{aligned}$$

So $\alpha \circ \beta$ is a homomorphism.

So $\alpha \circ \beta \in \mathrm{Aut}(G)$.

(aab) Assume $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathrm{Aut}(G)$ and $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$.

This, if $g \in G$ then

$$\begin{aligned}(\alpha_1 \circ \beta_1)(g) &= \alpha_1\big(\beta_1(g)\big) \\ &= \alpha_2\big(\beta_2(g)\big) \\ &= (\alpha_2 \circ \beta_2)(g).\end{aligned}$$

So $\alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2$.

So the operation on $\mathrm{Aut}(G)$ is well defined.

(ab) Let $\iota_G\colon G \to G$ be the identity map on G.

To show: (aba) $\iota_G \in \mathrm{Aut}(G)$.

(abb) If $\alpha \in \mathrm{Aut}(G)$ then $\iota_G \circ \alpha = \alpha = \alpha \circ \iota_G$.

(aba) To show: (abaa) ι_G is a bijection.
(abab) ι_G is a homomorphism.

(abaa) This is *very* easy. *You* prove it.

(abab) Assume $g_1, g_2 \in G$. Then

$$\begin{aligned}\iota_G(g_1g_2) &= g_1g_2 \\ &= \iota_G(g_1)\iota_G(g_2).\end{aligned}$$

So ι_G is a homomorphism.
So $\iota_G \in \mathcal{R}mathrmAut(G)$.

(abb) Assume $\alpha \in \mathrm{Aut}(G)$. Then, if $g \in G$ then

$$\begin{aligned}(\iota_G \circ \alpha)(g) &= \iota_G\big(\alpha(g)\big) \\ &= \alpha(g) \\ &= \alpha\big(\iota_G(g)\big) \\ &= (\alpha \circ \iota_G)(g)\end{aligned}$$

So $\iota_G \circ \alpha = \alpha = \alpha \circ \iota_G$.
Thus, if $\alpha \in \mathrm{Aut}(G)$ then $\iota_G \circ \alpha = \alpha = \alpha \circ \iota_G$.
So ι_G is an identity in $\mathrm{Aut}(G)$.

(ac) Assume $\alpha \in \mathrm{Aut}(G)$.
To show: There exists $\alpha^{-1} \in \mathrm{Aut}(G)$ such that $\alpha \circ \alpha^{-1} = \iota_G = \alpha^{-1} \circ \alpha$.
Since $\alpha \in \mathrm{Aut}(G)$ then α is bijective.
Therefore, by Theorem XXX, there exists an inverse function to α, α^{-1}, such that $\alpha \circ \alpha^{-1} = \iota_G = \alpha^{-1} \circ \alpha$.
To show: $\alpha^{-1} \in \mathrm{Aut}(G)$.
To show: (aca) α^{-1} is bijective.
(acb) α^{-1} is a homomorphism.

(aca) Since $\alpha \circ \alpha^{-1} = \iota_G = \alpha^{-1} \circ \alpha$ then α is an inverse function to α^{-1}.
Therefore, by Proposition XXX, α^{-1} is bijective.

(acb) Let $g_1, g_2 \in G$.
Since α is bijective there exist $h_1, h_2 \in G$ such that $\alpha(h_1) = g_1$ and $\alpha(h_2) = g_2$.
Since α and α^{-1} are inverse functions and α is a homomorphism then

$$\begin{aligned}\alpha^{-1}(g_1g_2) &= \alpha^{-1}\big(\alpha(h_1)\alpha(h_2)\big) \\ &= \alpha^{-1}\big(\alpha(h_1h_2)\big) \\ &= h_1h_2 \\ &= \alpha^{-1}\big(\alpha(h_1)\big)\alpha^{-1}\big(\alpha(h_2)\big) \\ &= \alpha^{-1}(g_1)\alpha^{-1}(g_2).\end{aligned}$$

So α^{-1} is a homomorphism.
So $\alpha^{-1} \in \mathrm{Aut}(G)$.
So there exists $\alpha^{-1} \in \mathrm{Aut}(G)$ such that $\alpha \circ \alpha^{-1} = \iota_G = \alpha^{-1} \circ \alpha$.

So $\mathrm{Aut}(G)$ is a group.

(b) Let c be given by

$$\begin{array}{rccc} c\colon & G & \to & \mathrm{Aut}(G) \\ & g & \mapsto & c_g. \end{array}$$

To show: (ba) c is well defined.

(bb) c is a homomorphism.
(bc) im$c = \mathrm{In}(G)$.
(bd) $\ker c = Z(G)$, the center of G.

(ba) To show: c is well defined.
To show: (baa)f $g \in G$ then $c_g \in \mathrm{Aut}(G)$.
(bab) If $g_1, g_2 \in G$ and $g_1 = g_2$ then $c_{g_1} = c_{g_2}$.

(baa) To show: $c_g \in \mathrm{Aut}(G)$.
To show: (baaa) c_g is injective.
(baab) c_g is surjective.
(baac) c_g is a homomorphism.

(baaa) To show: If $h_1, h_2 \in G$ and $c_g(h_1) = c_g(h_2)$ then $h_1 = h_2$.
Assume $h_1, h_2 \in G$ and $c_g(h_1) = c_g(h_2)$.
Then

$$gh_1g^{-1} = c_g(h_1) = c_g(h_2) = gh_2g^{-1}.$$

Multiplying both sides on the left by g^{-1} and on the right by g gives

$$h_1 = h_2.$$

So c_g is injective.

(baab) To show: If $h \in G$ then there exists some $k \in G$ such that

$$c_g(k) = h.$$

Assume $h \in G$. Let $k = g^{-1}hg$. Then

$$c_g(k) = gkg^{-1} = gg^{-1}hgg^{-1} = h.$$

So c_g is surjective.

(baac) Assume $h_1, h_2 \in G$.
To show: $c_g(h_1h_2) = c_g(h_1)c_g(h_2)$.

$$\begin{aligned} c_g(h_1h_2) &= gh_1h_2g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \\ &= c_g(h_1)c_g(h_2). \end{aligned}$$

So c_g is a homomorphism.
So $c_g \in \mathrm{Aut}(G)$.

(bab) Assume $g_1, g_2 \in G$ and $g_1 = g_2$.
To show: $c_{g_1} = c_{g_2}$.
If $h \in G$ then

$$\begin{aligned} c_{g_1}(h) &= g_1hg_1^{-1} \\ &= g_2hg_2^{-1} \\ &= c_{g_2}(h) \end{aligned}$$

So $c_{g_1} = c_{g_2}$.

So c is well defined.

(bb) Assume g_1, $g_2 \in G$.
To show: $c_{g_1} \circ c_{g_2} = c_{g_1g_2}$.

If $h \in G$ then

$$\begin{aligned}(c_{g_1} \circ c_{g_2})(h) &= c_{g_1}\big(c_{g_2}(h)\big) \\ &= c_{g_1}(g_2 h g_2^{-1}) \\ &= g_1 g_2 h g_2^{-1} g_1^{-1} \\ &= g_1 g_2 h (g_1 g_2)^{-1} \\ &= c_{g_1 g_1}(h)\end{aligned}$$

So $c_{g_1} \circ c_{g_2} = c_{g_1 g_2}$.
So c is a homomorphism.

(bc) To show: $\mathrm{im} c = \mathrm{In}(G)$.
This follows from the definitions.

(bd) To show: $\ker c = Z(G)$.
To show: (bda) $\ker c \subseteq Z(G)$.
(bdb) $Z(G) \subseteq \ker c$.

(bda) Let $g \in \ker c$. Then $c_g = \iota_G$.
So, if $h \in G$ then

$$h = c_g(h) = ghg^{-1}.$$

So if $h \in G$ then $gh = hg$.
So $g \in Z(G)$.
So $\ker c \subseteq Z(G)$.

(bdb) Let $g \in Z(G)$.
Then, if $h \in G$ then $gh = hg$.
So, if $h \in G$ then

$$c_g(h) = ghg^{-1} = h = \iota_G(h),$$

So $c_g = \iota_G$.
So $g \in \ker c$.
So $Z(G) \subseteq \ker c$.
So $\ker c = Z(G)$.
So c is a well defined homomorphism.

(c) Let c be as in part (b).
Since c is a group homomorphism and $\mathrm{im}\, c = \mathrm{Inn}(G)$ then $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ by Proposition XXX.

□

Proposition D.3.7. — *Let H and K be groups and let $\theta \colon H \to \mathrm{Aut}(K)$ be a homomorphism. Then $H \times_\theta K$ is a group.*

Proof. —
To show: (a) If $(h_1, k_1), (h_2, k_2) \in H \times_\theta K$ then $(h_1, k_1) \cdot (h_2, k_2) \in H \times_\theta K$.
(b) There is an identity in $H \times_\theta K$.
(c) If $(h_1, k_1) \in H \times_\theta K$ then there is an inverse for (h_1, k_1) in $H \times_\theta K$.

(a) Assume $(h_1, k_1), (h_2, k_2) \in H \times_\theta K$.
By definition, $(h_1, k_1) \cdot (h_2, k_2) = \big(h_1 h_2, \theta_{h_2}(k_1) k_2\big)$.
Since $\theta_{h_2} \colon K \to K$ is a map from K to K then $\theta_{h_2}(k_1) \in K$.
So

$$(h_1, k_1) \cdot (h_2, k_2) = \big(h_1 h_2, \theta_{h_2}(k_1) k_2\big) \in H \times_\theta K.$$

(b) Let 1_H, 1_K be the identities on H and K respectively.
To show: (ba) If $(h,k) \in H \times_\theta K$ then $(1_H, 1_K)(h,k) = (h,k)$.
(bb) If $(h,k) \in H \times_\theta K$ then $(h,k)(1_H, 1_K) = (h,k)$.

(ba) Let$(h,k) \in H \times_\theta K$. Then $(1_H, 1_K)(h,k) = \big(h, \theta_h(1_K)k\big)$.
Since θ_h is an automorphism then $\theta_h(1_K) = 1_K$.
So
$$(1_H, 1_K)(h,k) = \big(h, \theta_h(1_K)k\big) = (h, 1_K k) = (h,k).$$

(bb) Let $(h,k) \in H \times_\theta K$.
Then $(h,k)(1_H, 1_K) = \big(h, \theta_{1_H}(k)1_K\big)$.
Since θ is a homomorphism then $\theta_{1_H} = \iota_K$ is the identity map on K.
So $\theta_{1_H}(k) = \iota_K(k) = k$.
So
$$(h,k)(1_H, 1_K) = \big(h, \theta_{1_H}(k)\big) = (h,k).$$

So $(1_H, 1_K)$ is an identity in $H \times_\theta K$.

(c) Assume $(h,k) \in H \times_\theta K$.
To show: (ca) $\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big)(h,k) = (1_H, 1_K)$.
(cb) $(h,k)\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big) = (1_H, 1_K)$.

(ca) We have $\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big)(h,k) = \Big(h^{-1}h, \theta_h\big(\theta_{h^{-1}}(k^{-1})\big)k\Big)$.
Since θ is a homomorphism, $\theta_{h^{-1}} = \theta_h^{-1}$.
So
$$\begin{aligned}\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big)(h,k) &= \Big(h^{-1}h, \theta_h\big(\theta_{h^{-1}}(k^{-1})\big)k\Big)\\ &= \Big(1_H, \theta_h\big(\theta_h^{-1}(k^{-1})\big)k\Big)\\ &= (1_H, k^{-1}k)\\ &= (1_H, 1_K).\end{aligned}$$

(cb) We have $(h,k)\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big) = \big(hh^{-1}, \theta_{h^{-1}}(k)\theta_{h^{-1}}(k^{-1})\big)$.
Since $\theta_{h^{-1}}$ is an automorphism, $\theta_{h^{-1}}(k^{-1}) = \theta_{h^{-1}}(k)^{-1}$.
So
$$\begin{aligned}(h,k)\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big) &= \big(hh^{-1}, \theta_{h^{-1}}(k)\theta_{h^{-1}}(k^{-1})\big)\\ &= \big(1_H, \theta_{h^{-1}}(k)\theta_{h^{-1}}(k)^{-1}\big)\\ &= (1_H, 1_K).\end{aligned}$$

So $\big(h^{-1}, \theta_{h^{-1}}(k^{-1})\big) \in H \times_\theta K$ is an inverse for (h,k).

So $H \times_\theta K$ is a group. □

Theorem D.3.8. — *Suppose H and K are subgroups of a group G with K normal in G such that*

(a) $G = HK$,
(b) K is normal in G, and
(c) $H \cap K = (1)$, where 1 is the identity in G.

Let θ be given by
$$\begin{array}{rccc} \theta\colon & H & \to & \mathrm{Aut}(K) \\ & h & \mapsto & c_h \end{array} \quad \textit{where} \quad \begin{array}{rccc} c_h\colon & K & \to & K \\ & k & \mapsto & hkh^{-1}. \end{array}$$
Then θ is a well defined homomorphism and $G \simeq H \times_\theta K$.

Proof. —
To show: (a) θ is well defined.
(b) θ is a homomorphism.
(c) $G \simeq H \times_\theta K$.

(a) To show: (aa) If $h \in H$ then $c_h \in \mathrm{Aut}(K)$.
(ab) If h_1, $h_2 \in H$ and $h_1 = h_2$ then $c_{h_1} = c_{h_2}$.

(aa) Assume $h \in H$.
To show: (aaa) c_h is well defined.
(aab) c_h is a homomorphism.
(aac) c_h is injective.
(aad) c_h is surjective.

(aaa) To show: (1) $c_h(k) \in K$.
(2) If $k_1, k_2 \in K$, and $k_1 = k_2$ then $c_h(k_1) = c_h(k_2)$.
(1) $c_h(k) = hkh^{-1} \in K$ since K is *normal.*
(2) This is clear.
So c_h is well defined.

(aab) Let $k_1, k_2 \in K$.
Then

$$c_h(k_1)c_h(k_2) = hk_1h^{-1}hk_2h^{-1} = hk_1k_2h^{-1} = c_h(k_1k_2).$$

So c_h is a homomorphism.

(aac) To show: If $k_1, k_2 \in K$ and $c_h(k_1) = c_h(k_2)$ then $k_1 = k_2$.
Assume $k_1, k_2 \in K$ and $c_h(k_1) = c_h(k_2)$.
Then

$$hk_1h^{-1} = c_h(k_1) = c_h(k_2) = hk_2h^{-1}.$$

Multiplying both sides on the left by h^{-1} and on the right by h gives

$$k_1 = k_2.$$

So c_h is injective.

(aad) To show: If $k_1 \in K$ then there exists $k_2 \in K$ such that

$$c_h(k_2) = k_1.$$

Assume $k_1 \in K$. Let $k_2 = h^{-1}k_1h$.
Then

$$c_h(k_2) = hk_2h^{-1} = hh^{-1}k_1hh^{-1} = k_1.$$

So c_h is surjective.
So θ is well defined.

(b) To show: θ is a homomorphism.
Let $h_1, h_2 \in H$.
To show: $c_{h_1} \circ c_{h_2} = c_{h_1h_2}$.
If $k \in K$ then

$$\begin{aligned}(c_{h_1} \circ c_{h_2})(k) &= c_{h_1}\big(c_{h_2}(k)\big)\\ &= c_{h_1}(h_2kh_2^{-1})\\ &= h_1h_2kh_2^{-1}h_1^{-1}\\ &= h_1h_2k(h_1h_2)^{-1}\\ &= c_{h_1h_2}(k),\end{aligned}$$

So $c_{h_1} \circ c_{h_2} = c_{h_1 h_2}$.
So θ is a homomorphism.

(c) To show: $H \times_\theta K$ is isomorphic to $G = HK$.
Define

$$\begin{array}{rccc} \alpha\colon & H \times_\theta K & \to & HK \\ & (h,k) & \mapsto & hk. \end{array}$$

To show: (ca) α is a homomorphism.
(cb) α is injective.
(cc) α is surjective.

(ca) Assume $(h_1,k_1),(h_2,k_2) \in H \times_\theta K$.
Then

$$\begin{aligned} \alpha\big((h_1,k_1)(h_2,k_2)\big) &= \alpha\Big(\big(h_1h_2, \theta_{h_2}(k_1)k_2\big)\Big) \\ &= h_1h_2\theta_{h_2}(k_1)k_2 \\ &= h_1h_2h_2^{-1}k_1h_2k_2 \\ &= h_1k_1h_2k_2, \end{aligned}$$

and

$$\alpha\big((h_1,k_1)\big)\alpha\big((h_2,k_2)\big) = h_1k_1h_2k_2.$$

So $\alpha\big((h_1k_1)(h_2,k_2)\big) = \alpha\big((h_1,k_1)\big)\alpha\big((h_2,k_2)\big)$.
So α is a homomorphism.

(cb) To show: $\ker\alpha = \{(1_G,1_G)\}$.
Assume $(h,k) \in \ker\alpha$.
Then $\alpha(h,k) = hk = 1_G$.
So $h = k^{-1}$ and $h = k^{-1} \in H$ and $h = k^{-1} \in K$.
Since $H \cap K = (1_G)$ then $h = k^{-1} = 1_G$.
So $(h,k) = (1_G,1_G)$.
So $\ker\alpha = \{(1_G,1_G)\}$.
So α is injective.

(cc) Let $g \in G$.
Since $G = HK$ then $g = hk$ for some $h \in H$ and $k \in K$.
Then

$$\alpha(h,k) = hk = g.$$

So α is surjective.

So α is an isomorphism.

So $G \simeq H \times_\theta K$. □

D.3.2. Proofs for p-groups and p-Sylow subgroups. —

Proposition D.3.9. — *If G is a p-group then G contains an element of order p.*

Proof. — To show: There exists $g \in G$ such that $o(g) = p$.
Since $\mathrm{Card}(G) > 1$ there exists $x \in G$ with $x \neq 1$.
Then $o(x) \neq 1$.
Since $o(x)$ divides $\mathrm{Card}(G) = p^a$ then $o(x) = p^b$ with $0 < b \leqslant a$.
Let $g = x^{p^{b-1}}$.
Since $o(x) = p^b$ then

$$g = x^{p^{b-1}} \neq 1, \quad \text{and} \quad g^p = \left(x^{p^{b-1}}\right)^p = x^{p^{b-1}p} = x^{p^b} = 1.$$

So $o(g) = p$. □

Proposition D.3.10. — *If G is a p-group and* $\mathrm{Card}(G) > 1$ *then the center of G is not* $\{1\}$,

$$\mathrm{Card}(Z(G)) \neq 1.$$

Proof. — To show: $\left|Z(G)\right| \neq 1$.

(a) Since $\mathrm{Card}(G) = p^a$ then p divides $\mathrm{Card}(G)$.

(b) Let $\mathcal{C}_g$ be a conjugacy class in G.
By Theorem xxx, $\mathcal{C}_g$ is an orbit under the action of G on itself by conjugation.
By Theorem ???, $\mathrm{Card}(\mathcal{C}_g)$ divides $\mathrm{Card}(G) = p^a$.
Thus, if $\mathrm{Card}(\mathcal{C}_g) \neq 1$ then p divides $\mathrm{Card}(\mathcal{C}_g)$.

(c) The Class equation is

$$\mathrm{Card}(G) = \mathrm{Card}(Z(G)) + \sum_{\mathrm{Card}(\mathcal{C}_g) \neq 1} \mathrm{Card}(\mathcal{C}_g),$$

where the sum is over all distinct conjugacy classes such that $\mathrm{Card}(\mathcal{C}_g) \neq 1$.
Since p divides $\mathrm{Card}(G)$ and p divides every term in the sum we <u>cannot</u> have $\mathrm{Card}(Z(G)) = 1$.

So $\mathrm{Card}(Z(G)) \neq 1$. □

Proposition D.3.11. — *Let p be a prime and let G be a group of order p^2. Then G is abelian.*

Proof. — To show: The cardinality of the center of G is p^2, $\mathrm{Card}(Z(G)) = p^2$.
By Proposition xxx, $\mathrm{Card}(Z(G))$ divides $\mathrm{Card}(G) = p^2$.
To show: (a) $\mathrm{Card}(Z(G)) \neq 1$.
(b) $\mathrm{Card}(Z(G)) \neq p$.

(a) By Proposition xxx, $\mathrm{Card}(Z(G)) \neq 1$.

(b) We will assume $\mathrm{Card}(Z(G)) = p$ and derive a contradiction.
Let $x \in G$ with $x \notin Z(G)$.
Since $Z(G)$ is a normal subgroup of G then $G/Z(G)$ is a group and

$$\mathrm{Card}(G/Z(G)) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(Z(G))} = \frac{p^2}{p} = p.$$

So, by Proposition xxx, $G/Z(G)$ is cyclic.
Since $x \notin Z(G)$ then $Z(G) \neq xZ(G)$.
So $xZ(G)$ generates $G/Z(G)$, i.e.

$$G/Z(G) = \{Z(G),\ xZ(G),\ x^2Z(G),\ \ldots,\ x^{p-1}Z(G)\}.$$

Let $g \in G$. Then there exists $k \in \mathbb{Z}_{[0,p-1]}$ such that $gZ(G) = x^k Z(G)$.
So there exists $z \in Z(G)$ such that $g = x^k z$.
Then

$$xg = xx^k z = x^k xz = x^k zx = gx.$$

So $x \in Z(G)$. This is a contradiction.

So $\mathrm{Card}(Z(G)) \neq p$.
So $\mathrm{Card}(Z(G)) = p^2 = \mathrm{Card}(G)$.
So G is abelian. □

Theorem D.3.12. — *If G is a p-group of order p^a, then there exists a chain, of normal subgroups of G*

$$(1) \subseteq N_1 \subseteq N_2 \subseteq \ldots \subseteq N_{a-1} \subseteq G,$$

such that $Card(N_i) = p^i$.

Proof. — We know that $Z(G)$ of G is a normal subgroup of G of order at least p.
$Z(G)$ contains a subgroup of order p by proposition x.x.
This subgroup is a normal subgroup of G of order p.
Let N_1 be this subgroup.
Doing the same argument on G/N_1 gives a normal subgroup N_2/N_1 of G/N_1 of order p in G/N_1.
Then by the correspondence theorem this corresponds to a normal subgroup N_2 of G of order p^2 that contains N_1.
In general, since G/N_i is a p-group of order p^{a-i} it contains a normal subgroup of order p in G/N_i which corresponds to a normal subgroup N_{i+1} of G which contains N_i. □

Theorem D.3.13. — First Sylow theorem. *G has a subgroup of order p^a.*

Proof. — To show: There exists a subgroup of G of order p^a.
Let $\mathcal{S}$ be the set of subsets of G with p^a elements.
Let G act on $\mathcal{S}$ by left multiplication

$$\begin{array}{ccc} G \times \mathcal{S} & \to & \mathcal{S} \\ (g, S) & \mapsto & gS \end{array} \quad \text{where } gS = \{gs \mid s \in S\}.$$

To show: (a) p does not divide $\mathrm{Card}(\mathcal{S})$.
(b) There exists $S \in \mathcal{S}$ such that p does not divide the order $\mathrm{Card}(GS)$ of the orbit GS.
(c) Let S be as in (b). Then $\mathrm{Card}(\mathrm{Stab}_G(S)) \geqslant p^a$.
(d) Let S be as in (b). $\mathrm{Card}(\mathrm{Stab}_G(S) \leqslant p^a$.
This will show that $\mathrm{Stab}_G(S)$ is a subgroup of G of order p^a.

(a) $\mathrm{Card}(\mathcal{S})$ is the number of subsets of G with p^a elements.

$$\mathrm{Card}(\mathcal{S}) = \binom{\mathrm{Card}(G)}{p^a} = \binom{p^a b}{p^a} = \frac{p^a b(p^a b - 1) \cdots (p^a b - j) \cdots (p^a b - p^a + 1)}{p^a(p^a - 1) \cdots (p^a - j) \cdots 1}.$$

Suppose p^i divides $p^a b - j$.
Then there exists $k \in \mathbb{Z}_{>0}$ such that $p^i k = p^a b - j$.
So $j = p^a b - p^i k$ and

$$p^a - j = p^a - p^a b + p^i k = p^i(p^{a-i} - p^{a-i} b + k).$$

So p^i divides $p^a - j$.

Thus, any factors of p in the numerator of $\mathrm{Card}(\mathcal{S}) = \binom{p^a b}{p^a}$ are canceled by factors of p in the denominator.
So p does not divide $\mathrm{Card}(\mathcal{S})$.

(b) It follows from Proposition xxx that

$$\mathrm{Card}(\mathcal{S}) = \sum_{\text{distinct orbits}} \mathrm{Card}(GS),$$

where the sum is over the distinct orbits GS of G acting on $\mathcal{S}$.
Since p does not divide $\mathrm{Card}(\mathcal{S})$ then there exists $S \in \mathcal{S}$ such that p does not divide $\mathrm{Card}(GS)$.

(c) Fix $S \in \mathcal{S}$ such that p does not divide $\mathrm{Card}(GS)$.
By Proposition xxx,

$$p^a b = \mathrm{Card}(G) = \mathrm{Card}(\mathrm{Stab}_G(S))\mathrm{Card}(GS),$$

where $\mathrm{Stab}_G(S)$ is the stabilizer of S.
Since p does not divide $\mathrm{Card}(GS)$ then there exists $k \in \mathbb{Z}_{\geqslant 1}$ such that $\mathrm{Card}(\mathrm{Stab}_G(S)) = p^a k$.
So $\mathrm{Card}(\mathrm{Stab}_G(S)) \geqslant p^a$.

(d) Let $s \in S \subseteq G$ and let $G_S = \mathrm{Stab}_G(S)$.
Then $G_S s \subseteq S$, since $G_S S = S$.
Since all cosets of G_S are the same size (Proposition xxx) then

$$\mathrm{Card}(G_S s) = \mathrm{Card}(G_S).$$

Since $G_S s \subseteq S$ then $\mathrm{Card}(G_S s) \leqslant \mathrm{Card}(S) = p^a$.
So $\mathrm{Card}(G_S) \leqslant p^a$.

So $\mathrm{Card}(G_s) = p^a$.
So G contains a subgroup of order p^a. □

Theorem D.3.14. — Second Sylow theorem. *All the p-Sylow subgroups of G are conjugates of each other.*

Proof. —
Let P be a p-Sylow subgroup of G.
Let H be another p-Sylow subgroup of G
To show: There exists $g \in G$ such that $H \subseteq gPg^{-1}$.

(a) First we find the right $g \in G$.
H acts on G/P by left multiplication,

$$\begin{array}{ccc} H \times G/P & \to & G/P \\ (h, g_1 P) & \mapsto & hg_1 P. \end{array}$$

The orbits are Hg_1P for $g_1 \in G$.
By Proposition xxx,

$$\mathrm{Card}(Hg_1P) \quad \text{divides} \quad \mathrm{Card}(H) = p^a.$$

So either $\mathrm{Card}(Hg_1P) = 1$ or p divides $\mathrm{Card}(Hg_1P)$.

By Proposition xxx,

$$b = \frac{p^a b}{p^a} = \frac{\mathrm{Card}(G)}{\mathrm{Card}(P)} = \mathrm{Card}\big(\frac{G}{P}\big) = \sum_{\text{distinct orbits}} \mathrm{Card}(Hg_1P).$$

Since p does not divide b, there is an orbit HgP such that $\mathrm{Card}(HgP) = 1$.

(b) Now show $H \subseteq gPg^{-1}$.
Let $h \in H$. Since $\mathrm{Card}(HgP) = 1$,

$$HgP = gP,$$

So there exists $p \in P$ such that $hg = gp$.
So $h = gpg^{-1} \in gPg^{-1}$.
So $H \subseteq gPg^{-1}$.

(c) Since $H \subseteq gPg^{-1}$ and $\mathrm{Card}(H) = \mathrm{Card}(gPg^{-1})$ is finite then $H = gPg^{-1}$.

So H is a conjugate of P. □

Theorem D.3.15. — Third Sylow theorem. *The number of p-Sylow subgroups of G is $1 \bmod p$.*

Proof. — Let $\mathcal{S}$ be the set of all p-Sylow subgroups of G.
Let P be a p-Sylow subgroup of G.
The group P acts on $\mathcal{S}$ by conjugation.

$$\begin{array}{ccc} P \times \mathcal{S} & \to & \mathcal{S} \\ (p, Q) & \mapsto & pQp^{-1}. \end{array}$$

For each $Q \in \mathcal{S}$ let $P * Q$ denote the orbit of Q under this action.
To show: (a) $\mathrm{Card}(\mathcal{S}) = \displaystyle\sum_{\text{distinct orbits}} \mathrm{Card}(P * Q)$.

(b) Either $\mathrm{Card}(P * Q) = 0 \bmod p$ or $\mathrm{Card}(P * Q) = 1$.

(c) If $\mathrm{Card}(P*Q) = 1$ then $Q = P$, so there is only one orbit with $\mathrm{Card}(P*Q) = 1$.

(a) This follows from Proposition xxx.

(b) By Proposition xxx, $\mathrm{Card}(P * Q)$ divides $\mathrm{Card}(P) = p^a$.
So either $\mathrm{Card}(P * Q) = 1$ or p divides $\mathrm{Card}(P * Q)$.

(c) Assume $\mathrm{Card}(P * Q) = 1$.
To show: $P = Q$.
If $\mathrm{Card}(P * Q) = 1$ then $pQp^{-1} = Q$ for $p \in P$.
So, if $p \in P$ then $p \in N_Q$, where N_Q is the normalizer of Q.
So $P \subseteq N_Q$.
We know $Q \subseteq N_Q$ also. So P and Q are both p-Sylow subgroups of N_Q.
So, by Theorem xxx, P and Q are conjugates in N_Q.
So there exists $n \in N_Q$ such that $nQn^{-1} = P$.
But, by Proposition xxx, Q is normal in N_Q, so $nQn^{-1} = Q$.
So $P = Q$.

Then (a), (b), and (c) give that $\mathrm{Card}(\mathcal{S}) = 1 \bmod p$. □

D.4. Exercises for the "products of groups" section

Exercise ?.?.1 An **extension** of a group H by a group N is a group G such that there exist homomorphisms $i\colon N \to G$ and $p\colon G \to H$ such that

$$(1) \to N \xrightarrow{i} G \xrightarrow{p} H \to (1)$$

is an exact sequence. See §1 Ex. XX.
A **section of** p is a homomorphism $s\colon H \to G$ such that $p \circ s = \mathrm{id}_G$, the identity on G.
A **retraction** is a homomorphism $r\colon G \to N$ such that $r \circ i = \mathrm{id}_N$, the identity on N.

$$(1) \to N \underset{r}{\overset{i}{\rightleftharpoons}} G \underset{s}{\overset{p}{\rightleftharpoons}} H \to (1).$$

Exercise ?.?.2 Equivalence classes of extensions which respect G module structure of A $\simeq H^2(G, A)$.
Equivalence classes of split extensions $\mapsto 1$.
See Rotman 79, Theorem 10.24 and Curtis and Reiner p. 183.

Exercise ?.?.3 Classes of automorphisms of $A \times G$ which are identity in both A and $G \simeq$ derivations on $G \simeq H^1(G, A)$.
See Curtis and Reiner p. 181.

HW: The dihedral group of order 8 D_8 is a split extension of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

HW: The quaternion group Q is a nonsplit extension of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

D.5. Examples for p-groups and Sylow theorems

Exercise ?.?.1 *p-Sylow Subgroups*
The second Sylow theorem implies that the number of p-Sylow subgroups of G divides the order of G. This is because if we consider the action of G on the p-Sylow subgroups by conjugation, the only orbit consists of a p-Sylow subgroup and all its conjugates, which by the second Sylow theorem is all the p-Sylow subgroups of G. Since the cardinality of the orbit must divide the order of G, the number of p-Sylow subgroups of G divides the order of G.

Exercise ?.?.2 *Classifying the groups of order 21*
By the third Sylow theorem, $1, 8, 15, 22, \ldots$ are the possibilities for the number of 7-Sylow subgroups, and $1, 4, 7, 10, 13, 16, \ldots$ are the possibilities for the number of 3-Sylow subgroups.

The second Sylow theorem forces that there be exactly one 7-Sylow subgroup and either one or seven 3-Sylow subgroups since the number of Sylow subgroups must divide 21, the order of the group.

Since there is only 1 7-Sylow subgroup of G, call it K, and all conjugates K equal K, K is normal in G. Since K has order 7, $K \simeq Z_7$.

Case 1. One 3-Sylow subgroup.
If there is only 1 3-Sylow subgroup, call it H, then H is also normal in G and is isomorphic to Z_3. Now the $K \cap H = (1)$ since any element in the intersection must have order dividing both 3 and 7, the only possibility being 1, the only element of order 1. Now, HK is a subgroup of G since K in normal in G, and since $H \cap K = (1)$, $|HK| = |H||K| = 3 \cdot 7 = 21 = |G|$. So $G = HK$. Then theorem x.x gives that $G \simeq H \times K \simeq Z_7 \times Z_3$.

Case 2. Four 3-Sylow subgroups.
Let H be one of the 3-Sylow subgroups of G. Once again, $H \simeq Z_3$. H is *normal* in G. But by the same reasoning as before, $H \cap K = (1)$ and $HK = G$. Theorem x.x states that this is enough to write G as a semidirect product of H and K. The number of ways to do this depends on how many different homomorphisms $\theta\colon H \to \mathrm{Aut}(K)$ there are. Suppose that x is a generator of H and y is a generator of K. Then θ is completely determined by where x goes i.e. what $x^{-1}yx$ is. We know that it is of the form y^i since it is an element of K. Suppose that $x^{-1}yx = y^i$. Then $y = x^{-3}yx^3 = y^{i^3}$ forcing $i^3 = 1 \bmod 7$. The possibilities for i are $2and4$. The semidirect products obtained by these two possibilities are isomorphic since if $x^{-1}yx = y^2$, then $x^{-2}yx^2 = y^4$, and since x and x^2 are both generators of H the map sending $x \mapsto x^2, y \mapsto y$ will be an isomorphism of the two semidirect products. So in this case $G \simeq Z_3 \times_\theta Z_7$ and any two such semidirect products are isomorphic.

Exercise ?.?.3 *Groups of order* $\leqslant 10$.

Order 1	$\{1\}$
Order 2	$\mathbb{Z}/2\mathbb{Z}$
Order 3	$\mathbb{Z}/3\mathbb{Z}$
Order 4	$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Order 5	$\mathbb{Z}/5\mathbb{Z}$
Order 6	$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad S_3 \cong D_3$
Order 7	$\mathbb{Z}/7\mathbb{Z}$
Order 8	$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$
	The dihedral group, D_4
	The quaternion group, Q_8
Order 9	$\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
Order 10	$\mathbb{Z}/10\mathbb{Z}$,
	$\mathbb{Z}/5\mathbb{Z} \times_\theta \mathbb{Z}/2\mathbb{Z}$ where $\theta = ?$

INDEX

BIBLIOGRAPHY

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969 ix+128 pp. MR0242802.

[Bou] N. Bourbaki, *General Topology*, Springer-Verlag, 1989. MR1726779.

[Bre] A. Bressan, *Lecture notes on functional analysis, With applications to linear partial differential equations* Graduate Studies in Mathematics **143** American Mathematical Society, Providence, RI, 2013. ISBN: 978-0-8218-8771-4, MR2987297.

[Isa] I. Martin Isaacs, *Algebra. A graduate course*, Brooks/Cole Publishing Co., Pacific Grove, CA, 1994. xii+516 pp. ISBN: 0-534-19002-2 MR1276273 and I. Martin Isaacs *Algebra: a graduate course*, Reprint of the 1994 original. Graduate Studies in Mathematics, 100. American Mathematical Society, Providence, RI, 2009. xii+516 pp. ISBN: 978-0-8218-4799-2 MR2472787

[Mah] K. Mahler, *Introduction to p-adic numbers and their functions*, Cambridge University Press, 1973. ISBN: 0-521-20001-6, MR0347711.

[Rub] J. Hyam Rubinstein, *Lecture notes for Metric and Hilbert Spaces*, University of Melbourne 2010-2013.

[BRu] W. Rudin, *Principles of mathematical analysis*, Third edition, International Series in Pure and Applied Mathematics, McGraw-Hill 1976. MR0385023.

[Ru] W. Rudin, *Real and complex analysis*, Third edition, McGraw-Hill, 1987. MR0924157.