Chapter 1. GROUPS AND GROUP ACTIONS

The standard abstract algebra course presents a basic study of groups, rings, and fields. Groups, rings, and fields are types of "number systems" that have certain special properties. In fact, of the following familiar number systems:

a) the integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
b) the rational numbers, $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{P}\}$,
c) the real numbers, $\mathbb{R}$,
with the operations of addition, $+$, and multiplication, $\times$;

the integers $\mathbb{Z}$ form a ring, the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ form fields, and all of these form groups under the operation of addition.

We need to find exactly what properties these structures have and what the implications of these properties are.

Chapter 1. GROUPS AND GROUP ACTIONS

§1T. Groups

We start with some basics, just a set and one operation. We can think of the operation as addition or multiplication, or something else, like composition of functions.

(1.1.1) Definition.

- A **group** is a set G and an operation $\times: G \times G \to G$ (we write $\times(a, b)$ as ab for $a, b \in G$) such that
  a) $(g_1 g_2)g_3 = g_1(g_2 g_3)$ for all $g_1, g_2, g_3 \in G$.
  b) There exists an **identity** element, $1 \in G$, such that $1g = g1 = g$ for all $g \in G$.
  c) For each $g \in G$ there exists an **inverse**, $g^{-1} \in G$, of g such that $gg^{-1} = g^{-1}g = 1$.
- A **subgroup** of a group G is a subset $H \subseteq G$ such that
  a) If h_1, $h_2 \in H$ then $h_1 h_2 \in H$.
  b) $1 \in H$.
  c) If $h \in H$ then $h^{-1} \in H$.
- The **trivial group**, (1), is the set containing only 1 with the operation given by $1 \cdot 1 = 1$.

HW: Show, using Ex. 2.2.5 a), Part I, that if G is a group then the identity element of G is unique.

HW: Show, using Ex. 2.2.5 b), Part I, that if $g \in G$ then the inverse g^{-1} of g is unique.

HW: Why isn't $\{0, 1, 2, 3, 4, 5\}$ a group?

Given such a definition the next step is to find out what kinds of structures fit the definition and explore them. Examples of groups are:

a) The integers, $\mathbb{Z}$, with the operation of addition.
b) The integers mod n, $\mathbb{Z}_n$, where $n \in \mathbb{N}$.
c) The symmetric group, S_n.
d) The general linear group of invertible matrices, $Gl_n(\mathbb{C})$.

Cosets

Let G be a group and let H be a subgroup of G. We will use the subgroup H to divide up the group G.

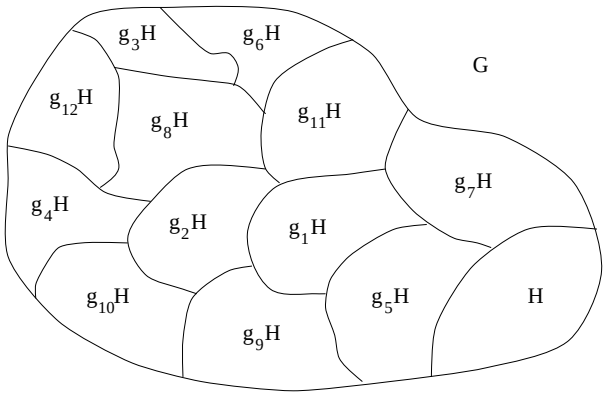
(1.1.2) Definition.

- A **left coset** of H in G is a set $gH = \{gh \mid h \in H\}$ where $g \in G$.
- G/H (pronounced "G **mod** H") is the set of left cosets of H in G.

- A **right coset** in G is a set $Hg = \{hg \mid h \in H\}$ where $g \in G$.
- $H\backslash G$ is the set of right cosets of H in G.

Unless we specify otherwise we shall always work with left cosets and just call them **cosets**.

HW: Let G be a group and let H be a subgroup of G. Let x and g be two elements of G. Show that $x \in gH$ if and only if $gH = xH$.



(1.1.3) Proposition. *Let G be a group and let H be a subgroup of G. Then the cosets of H in G partition G.*

(1.1.4) Proposition. *Let G be a group and let H be a subgroup of G. Then for any g_1, $g_2 \in G$,*

$$\text{Card}(g_1H) = \text{Card}(g_2H).$$

(1.1.5) Corollary. *Let H be a subgroup of a group G. Then*

$$\text{Card}(G) = \text{Card}(G/H)\,\text{Card}(H).$$

The results (0.3)-(0.5) show that the cosets of a subgroup H divide the group G into equal size pieces, one of these pieces being the subgroup H itself.

(1.1.6) Definition.

- A set of **coset representatives** of H in G is a set of distinct elements $\{g_i\}$ of G such that
  a) each coset of H is of the form g_iH for some g_i and
  b) $g_iH \neq g_jH$ unless $g_i = g_j$.
- The **index** of a subgroup H in a group G, $\mid G : H \mid$, is the number of cosets of H in G.

$$\mid G : H \mid = \text{Card}(G/H).$$

HW: Show that $\mid G : (1) \mid = \text{Card}(G)$.

Quotient Groups $\leftrightarrow$ Normal Subgroups

Let H be a subgroup of a group G. We can try to make the set G/H of cosets of H into a group by defining a multiplication operation on the cosets. The only problem is that this doesn't work for the cosets of just any subgroup, the subgroup has to have special properties.

(1.1.7) Definition.

- A subgroup, N of G, is **normal** if for each $n \in N$, $gng^{-1} \in N$ for all $g \in G$.

HW: Show that a subgroup N of a group G is normal if and only if $gN = Ng$ for all $g \in G$.

(1.1.8) Proposition. *Let N be a subgroup of a group G. N is a normal subgroup of G if and only if G/N with the operation given by $(aN)(bN) = abN$ is a group.*

(1.1.9) Definition.

- The **quotient group**, G/N, is the set of cosets of a normal subgroup N of a group G with the operation given by $(aN)(bN) = (abN)$.

Wow!! We actually made this weird set of cosets into a *group*!!

HW: Let N be a subgroup of a group G. Show that N is a normal subgroup of G if and only if the operation on G/N given by $(aN)(bN) = abN$ is well defined.

Homomorphisms

Group homomorphisms are used to compare groups. Let G and H be groups with identities 1_G and 1_H respectively.

(1.1.10) Definition.

- A **group homomorphism**, $f: G \to H$, is a map between groups G and H such that

$$f(gg') = f(g)f(g') \text{ for all } g, g' \in G.$$

- A **group isomorphism** is a bijective group homomorphism.
- Two groups G and H are **isomorphic**, $G \simeq H$, if there exists a group isomorphism $f: G \to H$ between them.

Two groups are isomorphic if both the elements of the groups and their operations match up exactly. Think of two groups that are isomorphic as being "the same". When we are classifying groups we put two groups in the same class only if they are isomorphic. This is what we mean by classifying groups "up to isomorphism".

HW: Show that if $G = N$ then $G/N \simeq (1)$.

(1.1.11) Proposition. *Let $f: G \to H$ be a group homomorphism. Let 1_G and 1_H be the identities for G and H respectively. Then*

a) $f(1_G) = 1_H$.
b) For any $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

(1.1.12) Definition.

- The **kernel** of a group homomorphism $f: G \to H$ is the set

$$\ker f = \{g \in G \mid f(g) = 1_H\},$$

  where 1_H is the identity in H.
- The **image** of a group homomorphism $f: G \to H$ is the set

$$\text{im } f = \{h \in H \mid f(g) = h \text{ for some } g \in G\}.$$

(1.1.13) Proposition. *Let $f: G \to H$ be a group homomorphism. Then*

a) $\ker f$ *is a normal subgroup of* G.
b) $\operatorname{im} f$ *is a subgroup of* H.

(1.1.14) Proposition. *Let* $f : G \to H$ *be a group homomorphism. Let* 1_G *be the identity in* G. *Then*
a) $\ker f = (1_G)$ *if and only if* f *is injective.*
b) $\operatorname{im} f = H$ *if and only if* f *is surjective.*

Notice that the proof of Proposition 1.1.14 b) does not use the fact that $f: G \to H$ is a homomorphism only the fact that $f: G \to H$ is a function.

HW: Show that if S and T are any two sets and $f: S \to T$ is a map then $\operatorname{im} f = T$ if and only if f is surjective.

(1.1.15) Theorem.
a) Let $f: G \to H$ *be a group homomorphism and let* $K = \ker f$. *Define*

$$\begin{array}{rccc} \hat{f}: & G/\ker f & \to & H \\ & gK & \mapsto & f(g). \end{array}$$

Then $\hat{f}$ *is a well defined injective group homomorphism.*

b) Let $f: G \to H$ *be a group homomorphism and define*

$$\begin{array}{rccc} f': & G & \to & \operatorname{im} f \\ & g & \mapsto & f(g). \end{array}$$

Then f' *is a well defined surjective group homomorphism.*

c) If $f: G \to H$ *is a group homomorphism then*

$$G/\ker f \simeq \operatorname{im} f,$$

where the isomorphism is a group isomorphism.

Direct Products

Suppose H and K are groups. The idea is to make $H \times K$ into a group.

(1.1.16) Definition.

- 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 all $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We say that the multiplication in $H \times K$ is **componentwise**.

- More generally, given groups $G_1, \ldots, G_n$, the **direct product** $G_1 \times \cdots \times G_n$ is the set given by $G_1 \times \cdots \times G_n$ with the operation given by
$$(h_1, \ldots, h_i, \ldots, h_n)(k_1, \ldots, k_i, \ldots, k_n) = (h_1 k_1, \ldots, h_i k_i, \ldots, h_n k_n)$$
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 $G_1 \times \cdots \times G_n$ are groups with identities given by $(1_H, 1_K)$ and $(1_{G_1}, \ldots, 1_{G_n})$ respectively (1_{G_i} denotes the identity in the group G_i).

Further Definitions

(1.1.17) Definition.

- A group G is **abelian** if $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$.
- The **center**, $Z(G)$, of a group G is the set

$$Z(G) = \{c \in G \mid cg = gc \text{ for all } g \in G\}.$$

HW: Give an example of a non-abelian group.

HW: Prove that every subgroup of an abelian group is normal.

HW: Prove that $Z(G)$ is a subgroup of G.

HW: Prove that $Z(G)$ is a normal subgroup of G.

HW: Prove that $Z(G) = G$ if and only if G is abelian.

(1.1.18) Definition.

- The **order**, $|G|$, of a group G is the number of elements in G.

$$|G| = \text{Card}(G).$$

- Let G be a group and $g \in G$. The **order**, $o(g)$, of g is the smallest positive integer n such that $g^n = 1$. If no such integer exists then $o(g) = \infty$.

(1.1.19) Definition.

- Let G be a group and let S be a subset of G. The **subgroup generated by S**, $\langle S \rangle$, is a subgroup $\langle S \rangle$ of G such that
  a) $S \subseteq \langle S \rangle$.
  b) If H is a subgroup of G and $S \subseteq H$ then $\langle S \rangle \subseteq H$.

$\langle S \rangle$ is the smallest subgroup of G containing S. Think of $\langle S \rangle$ as gotten by adding to S exactly those elements of G that are needed to make a group.

HW: Let G be a group and let S be a subset of G. Show that the subgroup generated by S, $\langle S \rangle$, exists and is unique. Hint: use Ex. 1.1.2.

(1.2.1) Definition.

- An **action** of a group G on a set S is a mapping $\alpha: G \times S \to S$ (the convention is to write gs for $\alpha(g,s)$) such that
  a) $g(hs) = (gh)s$ for all $g, h \in G, s \in S$.
  b) $1s = s$, for all $s \in S$.

Examples of group actions are given below in this section and in the Exercises.

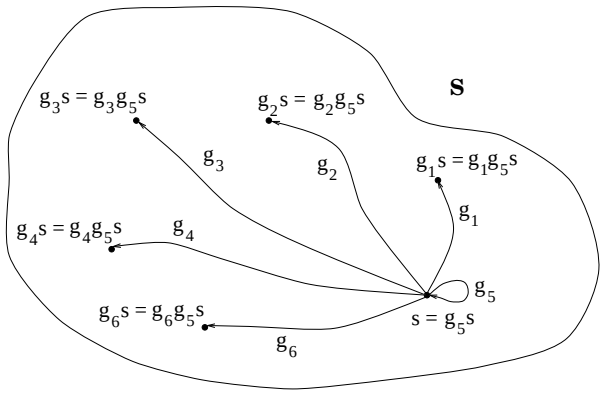
(1.2.2) Definition. Suppose a group G, a set S, and an action of G on S are given.

- The **stabilizer** of an element $s \in S$ under the action of G is the set

$$G_s = \{g \in G \mid gs = s\}.$$

- The **orbit** of an element $s \in S$ under the action of G is the set

$$Gs = \{s' \in S \mid gs = s' \text{ for some } g \in G\}.$$



(1.2.3) Proposition. *Suppose G is a group acting on a set S and let $s \in S$ and $g \in G$. Then*
a) G_s is a subgroup of G.
b) $G_{gs} = gG_sg^{-1}$.

The following proposition is an analogue of Proposition 1.1.3.

(1.2.4) Proposition. *Let G be a group which acts on a set S. Then the orbits partition the set S.*

(1.2.5) Corollary. *If G is a group acting on a set S and Gs_i denote the orbits of the action of G on S then*

$$\text{Card}(S) = \sum_{\substack{\text{distinct} \\ \text{orbits}}} \text{Card}(Gs_i).$$

It is possible to view the stabilizer G_s of an element $s \in S$ as an analogue of the kernel of a homomorphism and the orbit Gs of an element $s \in S$ as an analogue of the image of a homomorphism. One might say

group actions, $\alpha: G \times S \to S$,	are to	group homomorphisms, $f: G \to H$,	as
stabilizers, G_s,	are to	kernels, $\ker f$,	as
orbits, Gs,	are to	images, $\text{im } f$.	

From this point of view the following corollary is an analogue of Corollary 1.1.5.

(1.2.6) Proposition. *Let G be a group acting on a set S and let $s \in S$. If Gs is the orbit containing s and G_s is the stabilizer of s then*

$$| G{:}G_s | = \mathrm{Card}(Gs)$$

where $| G{:}G_s |$ is the index of $G_s \in G$.

(1.2.7) Corollary. *Let G be a group acting on a set S. Let $s \in S$, let G_s denote the stabilizer of s, and let Gs denote the orbit of s. Then*

$$\mathrm{Card}(G) = \mathrm{Card}(Gs)\mathrm{Card}(G_s).$$

Conjugation

(1.2.8) Definition.

- Let S be a subset of a group G. The **normalizer** of S in G is the set

$$N_S = \{x \in G \mid xSx^{-1} = S\},$$

where $xSx^{-1} = \{xsx^{-1} \mid s \in S\}$.

(1.2.9) Proposition. *Let H be a subgroup of G and let N_H be the normalizer of H in G. Then*

a) H is a normal subgroup of N_H.

b) If K is a subgroup of G such that $H \subseteq K \subseteq G$ and H is a normal subgroup of K then $K \subseteq N_H$.

This proposition says that N_H is the largest subgroup of G such that H is normal in this subgroup.

(1.2.10) Proposition. *Let G be a group and let $\mathcal{S}$ be the set of subsets of G. Then*

a) G acts on $\mathcal{S}$ by

$$\begin{array}{rccc} \alpha\colon & G \times \mathcal{S} & \to & \mathcal{S} \\ & (g, S) & \mapsto & gSg^{-1} \end{array}$$

where $gSg^{-1} = \{gsg^{-1} \mid s \in S\}$. We say that G acts on $\mathcal{S}$ by **conjugation**.

b) If S is a subset of G then N_S is the stabilizer of S under the action of G on $\mathcal{S}$ by conjugation.

(1.2.11) Definition.

- Two elements $g_1, g_2 \in G$ are **conjugate** if $g_1 = hg_2h^{-1}$ for some $h \in G$.
- Let G be a group and let $g \in G$. The **conjugacy class** , $\mathcal{C}_g$, of g is the set of all conjugates of g.
- Let g be an element of a group G. The **centralizer** or **normalizer** of g is the set

$$Z_g = \{x \in G \mid xgx^{-1} = g\}.$$

(1.2.12) Proposition. *Let G be a group. Then*

a) G acts on G by

$$\begin{array}{rccc} & G \times G & \to & G \\ & (g, s) & \mapsto & gsg^{-1}. \end{array}$$

We say that G acts on itself by conjugation.

b) Two elements $g_1, g_2 \in G$ are conjugate if and only if they are in the same orbit under the action of G on itself by conjugation.

c) The conjugacy class, $\mathcal{C}_g$, of $g \in G$ is the orbit of g under the action of G on itself by conjugation.

d) The centralizer, Z_g, of $g \in G$ is the stablilizer of g under the action of G on itself by conjugation.

(1.2.13) Definition.

- Let S be a subset of a group G. The **centralizer** of S in G is the set

$$Z_S = \{x \in G \mid xsx^{-1} = s \text{ for all } s \in S\}.$$

(1.2.14) Lemma. *Let G_s be the stabilizer of $s \in G$ under the action of G on itself by conjugation. Then*

a) For each subset $S \subseteq G$,

$$Z_S = \bigcap_{s \in S} G_s.$$

b) $Z(G) = Z_G$, where $Z(G)$ denotes the center of G.

c) $s \in Z(G)$ if and only if $Z_S = G$.

d) $s \in Z(G)$ if and only if $\mathcal{C}_s = \{s\}$.

(1.2.15) Proposition. *(The Class Equation) Let $\mathcal{C}_{g_i}$ denote the conjugacy classes in a group G and let $|\mathcal{C}_{g_i}|$ denote* $\mathrm{Card}(\mathcal{C}_{g_i})$. *Then*

$$|G| = |Z(G)| + \sum_{|\mathcal{C}_{g_i}|>1} \mathrm{Card}(\mathcal{C}_{g_i}).$$