CHAPTER G

STRUCTURE AND ACTION: GROUPS AND GROUP ACTIONS

The standard abstract algebra course presents the basic properties of groups, rings, and fields. The motivation is to study the properties of the number systems that we use, some of these being:

(a) the positive integers, $\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$,
(b) the integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
(c) the rational numbers, $\mathbb{Q} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}_{>0}\right\}$,
(d) the real numbers, $\mathbb{R}$,

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

G.1. 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.

Definition G.1.1. — A **group** is a set G with a function

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g_1, g_2) & \mapsto & g_1 g_2 \end{array} \quad \text{such that}$$

(a) If $g_1, g_2, g_3 \in G$ then $(g_1 g_2)g_3 = g_1(g_2 g_3)$,
(b) There exists an **identity** 1 in G such that if $g \in G$ then $1g = g1 = g$,
(c) If $g \in G$ then there exists an **inverse to** g, $g^{-1} \in G$, such that $gg^{-1} = g^{-1}g = 1$.

HW: Show that the identity $1 \in G$ is unique.
HW: Show that if $g \in G$ the the inverse $g^{-1} \in G$ is unique.
HW: Why isn't $\{1, 2, 3, 4, 5\}$ a group?

Important examples of groups are:

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

Group homomorphisms are used to compare groups. A group homomorphism must preserve the structures that distinguish a group: the operation, the identity, and the inverses.

Definition G.1.2. — Let G and H be groups with identities 1_G and 1_H respectively.

- A **group homomorphism** is a function $f\colon G \to H$ such that
  (a) If $g_1, g_2 \in G$ then $f(g_1g_2) = f(g_1)f(g_2)$,
  (b) $f(1_G) = 1_H$.
  (c) If $g \in G$ then $f(g^{-1}) = f(g)^{-1}$.
- A **group isomorphism** is a group homomorphism $f\colon G \to H$ such that the inverse function $f^{-1}\colon H \to G$ exists and f^{-1} is a group homomorphism.
- Two groups G and H are **isomorphic**, $G \simeq H$, if there exists a group isomorphism $f\colon G \to H$ 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 is meant by classifying groups "up to isomorphism".

HW: Show that $f\colon G \to H$ is a group isomorphism if and only if $f\colon G \to H$ is a bijective group homomorphism.

The following proposition says that (b) and (c) in the definition of a group homomorphism come "for free" once one assumes that $f\colon G \to H$ satisfies (a).

Proposition G.1.1. — *Let G and H be groups with identities 1_G and 1_H, respectively. Let $f\colon G \to H$ be a function such that*

(a) If $g_1, g_2 \in G$ then $f(g_1g_2) = f(g_1)f(g_2)$.

Then

(b) $f(1_G) = 1_H$ and
(c) If $g \in G$ then $f(g) = f(g)^{-1}$.

Definition G.1.3. — Let G be a group.

- A **subgroup** of a group G is a subset $H \subseteq G$ such that
  (a) If h_1, $h_2 \in H$ then $h_1h_2 \in H$,
  (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 $1 \cdot 1 = 1$.

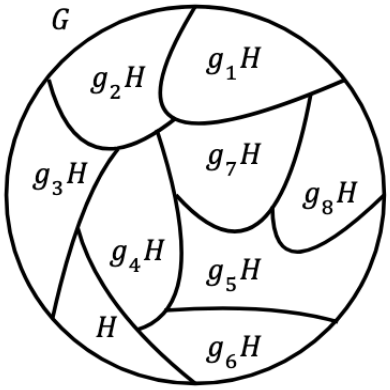
G.1.1. Cosets. — Let G be a group and let H be a subgroup of G. We will use the subgroup H to divide up the group G.

Definition G.1.4. — Let G be a group and let H be a subgroup of G.

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



Proposition G.1.2. — *Let G be a group and let H be a subgroup of G. Then the cosets of H in G partition G.*

Proposition G.1.3. — *Let G be a group and let H be a subgroup of G. If g_1, $g_2 \in G$ then*

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

Corollary G.1.4. — *Let H be a subgroup of a group G. Then*

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

The above results 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.

Notice the analogy between Proposition F.2.2 and Proposition R.1.2 and Proposition R.2.2 and Proposition G.1.2.

Definition G.1.5. — Let G be a group and let H be a subgroup of G.

- 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 H in a group G is $\mathrm{Card}(G/H)$.

HW: Show that $\mathrm{Card}(G/\{1\}) = \mathrm{Card}(G)$.

G.1.2. 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.

Definition G.1.6. — Let G be a group.

- A **normal subgroup** N is a subgroup of G such that if $n \in N$ and $g \in G$ then $gng^{-1} \in N$.

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

Theorem G.1.5. — *Let N be a subgroup of a group G. Then N is a normal subgroup of G if and only if G/N with the operation given by $(aN)(bN) = abN$ is a group.*

Notice the analogy between Theorem F.2.3, Theorem R.2.3, Theorem R.1.3 and Theorem G.1.5.

Definition G.1.7. — Let G be a group and let N be a normal subgroup of G.

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

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

Theorem G.1.6. — *Let N be a subgroup of a group G. Then N is a normal subgroup of G if and only if the operation on G/N given by $(aN)(bN) = abN$ is well defined.*

HW: Show that if $G = N$ then N is a normal subgroup of G and $G/N \cong \{1\}$.

G.1.3. Kernel and image of a group homomorphism. —

Definition G.1.8. — Let $f\colon G \to H$ be a group homomorpihsm.

- The **kernel** of f is the set
$$\ker f = \{g \in G \mid f(g) = 1_H\},$$
where 1_H is the identity in H.
- The **image** of f is the set
$$\mathrm{im} f = \{f(g) \mid g \in G\}.$$

Proposition G.1.7. — *Let $f\colon G \to H$ be a group homomorphism. Then*

(a) $\ker f$ *is a normal subgroup of G.*

(b) $\mathrm{im} f$ *is a subgroup of H.*

Proposition G.1.8. — *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) $\mathrm{im} f = H$ *if and only if f is surjective.*

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

Theorem G.1.9. — *(a) Let $f\colon G \to H$ be a group homomorphism and let $K = \ker f$. Define*

$$\begin{array}{rccc} \hat{f}\colon & G/\ker f & \longrightarrow & H \\ & gK & \longmapsto & f(g). \end{array}$$

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

(b) Let $f\colon G \to H$ be a group homomorphism and define

$$\begin{array}{rccc} f'\colon & G & \longrightarrow & \mathrm{im} f \\ & g & \longmapsto & f(g). \end{array}$$

Then f' is a well defined surjective group homomorphism.

(c) If $f\colon G \to H$ is a group homomorphism then

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

where the isomorphism is a group isomorphism.

G.1.4. Direct Products. — Suppose H and K are groups. The idea is to make $H \times K$ into a group.

Definition G.1.9. — Let H and K be groups.

- 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** $G_1 \times \cdots \times G_n$ is the set $G_1 \times \cdots \times G_n$ with 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.

The operation in the direct product is just the operations of the original groups acting **componentwise**.

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).

G.1.5. Further Definitions. —

Definition G.1.10. —

- An **abelian group** is a group G such that if $g_1, g_2 \in G$ then $g_1 g_2 = g_2 g_1$.
- The **center** $Z(G)$ of a group G is the set
$$Z(G) = \{c \in G \mid \text{if } g \in G \text{ then } cg = gc\}.$$

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 normal subgroup of G.

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

Definition G.1.11. — Let G be a group and $g \in G$.

- The **order of** G is $\mathrm{Card}(G)$, the number of elements 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 $o(g) = \infty$.

Definition G.1.12. — Let G be a group and S a subset of G.

- The **subgroup generated by S** is the 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 $\langle S \rangle \subseteq H$.

The subgroup $\langle S \rangle$ 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 exists and is unique.