Contents

Change logs

27 nov ’24 Following “Teddy”’s advice, made *closure* expressed implicitly via the range of $*$; added definition of Abelian groups and section for generators and element order.

20 nov ’24 Added “direct products”, preparing for homo-/isomorphism and interesting examples.

18 nov ’24 Started project as a complementary exercise for the Group Theory lesson on Brilliant.org.

1 Group "Axioms"

Definition 1.1 (Group)**.** Given set G and operation $* : G \times G \to G$, we say "G is a group under $*$" if and only if it has all of **associativity**, **identity**, and **invertibility**.

$$\forall f, g, h \in G, \quad (f * g) * h = f * (g * h) \tag{G.Assoc}$$
$$\exists! e \in G \quad \forall g \in G, \quad e * g = g * e = g \tag{G.Id}$$
$$\forall g \in G \quad \exists! f \in G, \quad f * g = g * f = e \tag{G.Inv}$$

Note 1.2. A few observations about 1.1:

1. G.Id is equivalent to demanding the existence of both left and right identit**ies**; uniqueness is derived.
   given $\exists e, e' \in G \quad \forall g \in G, \quad eg = ge' = g$
   then $e = ee' = e'$
2. Similarly, G.Inv follows existing both left and right inverse**s** per $g \in G$, assuming G.Assoc and G.Id.
   given $\forall g \in G \quad \exists f, f' \in G, \quad fg = gf' = e$
   then $f = f(gf') = (fg)f' = f'$

Definition 1.3 (Order of a group)**.** The order of a *finite* group G is exactly $\operatorname{order} G = |G|$.

Exercise 1.4 (Commonly used groups)**.** Show that these are indeed groups; how "big" are they?

D_n	Rotations / reflections of n-gons.	S_n	Permutations of a size-n set.
$Z_n, \mathbb{Z}/n\mathbb{Z}$	$\{0..(n-1)\}$ and $\mathbb{Z}$ under $(+)$ mod n.	Z_n^*	$\{a \in Z_n \mid a \perp n\}$ under $(\times)$ mod n.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	(under $+$)	$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	(with 0 removed, under $\times$)

(these are used a *lot*.)

Definition 1.5 (Direct products)**.** With groups F, G, define the *direct product* as "cartesian product with a mapped operator": (Note that all three occurrences of $*$ are actually different operators.)

$$F \times G = \{(f, g) : f \in F, g \in G\}\ ;$$
$$(f, g) * (f', g') = (f * f', g * g')\ .$$

Corollary 1.5.1 ($F \times G$'s are groups)**.** The identity is (e_F, e_G) and the inverse of (f, g) is (f^{-1}, g^{-1}). □

Definition 1.6 (Abelian Groups)**.** Just gonna throw this here cuz the definition itself is fairly simple. An Abelian group G is a group that also observes commutativity for all its elements,

$$G \text{ Abelian iff. } \forall g, g' \in G,\ gg' = g'g$$

2 Subgroups

Definition 2.1 (Subgroup relationship $\leq$). Literally, "subset that is also a group (under the same $*$)."

$$H \leq G \text{ iff. } G, H \text{ group}_* \wedge H \subseteq G$$

Note that this requires the range of $*$ restricted to $H \times H$ to be H itself.

Theorem 2.2 (Shared identity). Given $H \leq G$ group and the identities $e \in G, e' \in H$, then $e = e'$.

Proof. From the assumption, fix any $h \in H$, then also $h \in G$; thus $eh = h = e'h$.
Let $(\cdot)^{-1}$ denote inverse in G, then $ehh^{-1}{e'}^{-1} = e$, but also $ehh^{-1}{e'}^{-1} = e'$, so $e = e'$. ■

Corollary 2.2.1 (Shared inverse). Given $H \leq G$ group, $f, h \in H, g \in G$ s.t. $hf = e = fg$, then $h = g$. This is done by an argument similar to 1.2. □

Note that I didn't cite 1.2 for shared identity, because that requires knowing the identity $e \in G$ is an element of H — which is sorta shown via $e = e' \in H$, leading to cyclic argument.

Theorem 2.3 (Subgroup test). Given nonempty $H \subseteq G$ group, the following is sufficient to show $H \leq G$:

1. H is closed under $*$, i.e. $\forall g, h \in H,\ g * h \in H$.
2. H is closed under (G's) inversion, i.e. $\forall h \in H\ \forall h' \in G$ s.t. $hh' = h'h = e,\ h' \in H$.

Proof. To show (1.) and (2.) are sufficient, we assume both and show H group; once shown, $H \leq G$ follows from $H \subseteq G$ by the definition of subgroups.

From (1.) follows the range of $*$ restricted to $H \times H$ is H; associativity in H is implied by associativity in G; once we show that $e \in H$, it'll also follow that e is the identity in H, then from (2.) we'll also have invertibility of H.

To show $e \in H$: pick any $h \in H$ since $H \neq \emptyset$, then by (2.) we have $h' \in H$ s.t. $hh' = e$, then by (1.) we have $e \in H$. ■

3 Cosets & Langrange's Theorem

Definition 3.1 (Left and right cosets)**.** Given groups $H \leq G$ and $g \in G$, the cosets of H under G about g are

$$gH = \{gh : h \in H\} \tag{Co.L}$$
$$Hg = \{hg : h \in H\} \tag{Co.R}$$

Corollary 3.1.1 (The gH's are "same-sized")**.** Given $H \leq G$ group, $\forall g \in G,\ H \leftrightarrow gH$.

The reason? From invertibility in G, $(h \in H)\ h \mapsto gh$ has to be a bijection. □

This also applies to right cosets by a similar argument. Note that "same-sized" is in quotes since G, H may not be finite, but the bijection argument still applies.

Lemma 3.1.2 (The gH's partition the group)**.** With $H \leq G$ group, let's define a "same-coset" relation R for $g, g' \in G$ by requiring they share a factor f: (we'll just do the left factor here; the right factor is similar.)

$$g\ R\ g' \text{ iff. } \exists f \in G,\ g, g' \in fH$$

We want to show that R is an equivalence relation.

Proof. First, we would want to expand on the RHS of the iff by Co.L:

$$\forall f, g \in G,\ (g \in fH \iff \exists h \in H,\ g = fh)$$

Reflexivity let $f = g \in G$, then since $e \in H$ we have $g = fe \in fH$, thus $g\ R\ g$.

Symmetry (the definition of R is symmetric, duh.) Suppose $g, g' \in G$ s.t. $g\ R\ g'$, then we may pick an $f \in G$ s.t. $g, g' \in fH$, so (obviously) $g', g \in fH$, therefore $g'\ R\ g$.

Transitivity This is less obvious, and depends on showing $g'\ R\ g \implies g' \in gH$; once shown, for $g'\ R\ g$ and $g\ R\ g''$ (and by symmetry, $g''\ R\ g$), we can let $f = g$ and derive $g', g'' \in fH$, thus $g'\ R\ g''$.

To show $g'\ R\ g \implies g' \in gH$: pick $f \in G,\ h, h' \in H$ s.t. $g = fh \wedge g' = fh'$ and let $h'' = h^{-1}h' \in H$ (by invertibility and closure), then $g' = gh''$, thus $g' \in gH$. ■

Theorem 3.2 (Lagrange's Theorem)**.** Given finite groups $H \leq G$, $|H|$ divides $|G|$.

Proof. From 3.1.1 and 3.1.2:

$$|G| = \sum_{S \in \mathsf{co.l}(H)} |S| = \sum_{S \in \mathsf{co.l}(H)} |H| = |\mathsf{co.l}(H)| \cdot |H|$$

where $\mathsf{co.l}(H) = \{gH : g \in G\}$ is finite (since G finite) and non-empty (since $eH \in \mathsf{co.l}(H)$); then our desired result follows. ■

4 Generators & Element Order

Definition 4.1 ("Generate"). Given $S \subseteq G$ group, the set *generated* by S is that produced by finite compositions of the elements of S.

Corollary 4.1.1 (Generated Subgroup). The set generated by $S \subseteq G$ is a subset of G implied by closure of $* : G \times G \to G$, and is further a group iff. it contains all inverses of elements of S (as closure is implied by the definition of "set of all finite compositions"). □

Corollary 4.1.2 (Subsets of finite groups generate subgroups). $\forall S \subseteq G$ finite group, let H be the set generated by S, then $H \leq G$. Here we'll just show that $\forall g \in S, g^{-1} \in H$ and use the previous corollary for the rest:

Fix any $g \in S$; from closure of $* : G \times G \to G$, we have $\forall n \in \mathbb{N}, g^n \in G$. Let $A = \{g^n : n \in \{0..|G|\}\}$, then by the pigeon-hole principle $\exists n, m \in \{0..|G|\}, n < m \land g^n = g^m$; pick these n, m, then $g^{m-n} = e$, so $g^{m-n-1} = g^{-1}$. □

Definition 4.2 (Element Order). Given $g \in G$ group that generates a subgroup of G, let order g be the minimum $k \in \mathbb{N}^+$ s.t. $g^k = e$.

Corollary 4.2.1 (Element order divides finite group order). This follows from Lagrange's and 4.1.2. □

5 Quotient groups

Definition 5.1 (Normal subgroup). Given $H \leq G$ group, H is *normal* under G iff. $\forall g \in G,\ gH = Hg$