Some group theory definitions

Contents

1 Sets and functions

Definition 1.1. We will not define a *set* formally. Informally, it is a collection of objects.

Given a set S and a "thing" s, we write $s \in S$ if s is a member of S. In fact, a good way to think about a set is that for any "thing" t, either $t \in S$ or $t \notin S$. (In particular, the "thing" t cannot "be in S twice".)

Definition 1.2. If S, T are sets, we say S is a subset of T and write $S \subseteq T$ if the following statement is true:

$$\text{for all things } t: \text{ if } t \in S, \text{ then } t \in T.$$

This is often and conveniently abbreviated:

$$\text{for all } s \in S,\ s \in T.$$

Definition 1.3. Suppose S, T are sets. We say $S = T$ when $S \subseteq T$ and $T \subseteq S$.

Definition 1.4. Suppose that S, T are sets.

- $S \cup T := \{\text{things } t \mid t \in S \text{ or } t \in T\}$.
- $S \cap T := \{\text{things } t \mid t \in S \text{ and } t \in T\}$.
- $S \setminus T := \{\text{things } t \mid t \in S \text{ and } t \notin T\}$.
- $S \times T = \{(s,t) \mid s \in S \text{ and } t \in T\}$.

Definition 1.5. We will also decline to formally define functions. (Although it would be easier to formally define these than sets.) A *function* consists of three things:

- a domain (which is a set),
- a codomain (which is a possibly different set), and
- a rule that assigns to every element of the function's domain an element of the function's codomain.

If I write "$f\colon S \to T$", this is a function with domain S and codomain T. I wil also say "f is a function *from* S *to* T. For every element $s \in S$, the element of T that f assigns to s is denoted $f(s)$. (In particular, for any $s \in S$, we know $f(s) \in T$.)

Definition 1.6. Suppose $f\colon S \to T$ is a function. The *range of* f is the set

$$\{t \in T \mid \text{there exists } s \in S \text{ such that } f(s) = t\}.$$

Synonyms are *the image of* f or the notation "$f(S)$".

Definition 1.7. Suppose f, g are functions. We say that $f = g$ when

- the functions f, g have the same domain and codomain and
- for every s in the domains of f, g, we have $f(s) = g(s)$.

Definition 1.8. Suppose that S is a set. Define *the identity function on* S to be the function, which we will denote "Id_S", with domain and codomain S, along with the rule:

$$\text{for all } s \in S,\ \mathrm{Id}_S(s) = s.$$

Definition 1.9. Suppose $f\colon S \to T$ is a function.

- We say that f is *injective* if

$$\text{for all } s_1, s_2 \in S\colon \text{ if } f(s_1) = f(s_2), \text{ then } s_1 = s_2.$$

- We say that f is *surjective* if

$$\text{for all } t \in T,\ \text{there exists } s \in S \text{ such that } f(s) = t.$$

- We say that f is *bijective* if it is injective and surjective.

Definition 1.10. Suppose that $f\colon R \to S$ and $g\colon S \to T$ are functions. The *composition* of f and g, denoted $g \circ f$, is the function with domain R and codomain T, along with the rule

$$\text{for all } r \in R\colon \quad (g \circ f)(r) = g(f(r)).$$

Fact 1.11. *Function composition is associative. Specifically: if*

- $f\colon R \to S$,
- $g\colon S \to T$, *and*
- $h\colon T \to U$

are functions, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Definition 1.12. Suppose $f\colon S \to T$ is a function, and $g\colon T \to S$ is another function. We say that g *is the inverse of* f if

- $g \circ f = \mathrm{Id}_S$ and
- $f \circ g = \mathrm{Id}_T$.

If a function has an inverse, we say it is *invertible*.

Fact 1.13. *Suppose $f\colon S \to T$ is a function. Then the following statement is true:*

$$f \text{ is bijective} \quad \text{if and only if} \quad f \text{ is invertibe}$$

2 Integers

Definition 2.1. Suppose that $m, n \in \mathbb{Z}$. We say m *divides* n

$$\text{there exists } j \in \mathbb{Z} \text{such that } n = j \cdot m.$$

We also say n *is divisible by* m or n *is a multiple of* m. The notation we use is $m \mid n$.

Example 2.2.

- The statement $9 \mid 45$ is true because $45 = 5 \cdot 9$.
- The statement $9 \mid 44$ is false.
- The statement $9 \nmid 44$ is true.
- The statement $9 \mid 0$ is true because $0 = 0 \cdot 9$.
- The statement $0 \nmid 9$ is true.

3 Group basics

Definition 3.1. Let S be a set. A *binary operation on* S is a function (Definition 1.5) from $S \times S$ to S. Usually we give our binary operations names like "$\star$". And if $(s_1, s_2) \in S \times S$, we usually write $s_1 \star s_2$ instead of "$\star(s_1, s_2)$".

Definition 3.2. Suppose S is a set and $\star$ is a binary operation on S (Definition 3.1).

- We say $\star$ is *commutative* if

$$\text{for all } r, s \in S,\ r \star s = s \star r.$$

- We say $\star$ is *associative* if

$$\text{for all } r, s, t \in S,\ (r \star s) \star t = r \star (s \star t).$$

- If $e \in S$ has the property that

$$\text{for all } s \in S,\ e \star s = s \star e,$$

  we say that e is *an identity for* $\star$.

- We remark that if e is an identity for $\star$, then it is the only identity for $\star$. Indeed, if f is an identity for $\star$, then

$$\begin{aligned} e &= e \star f && \text{(since } f \text{ is an identity)} \\ &= f && \text{(since } e \text{ is an identity).} \end{aligned}$$

- Suppose e is an identity for $\star$ (necessarily the unique identity). If $s, t \in S$ have the property that $s \star t = t \star s = e$, then we say that t *is the inverse of* s and s *is the inverse of* t. We also say that s and t are *invertible*.

Definition 3.3. Suppose that G is a set with a binary operation $\star$ (Definition 3.1). We say that $(G, \star)$ is a *group* if

- $\star$ is associative,
- $\star$ admits an identity,
- every element of G has an inverse. (Remark: this last bullet point only makes sense because $\star$ has a (unique) identity—see Definition 3.1.)

If $(G, \star)$ is a group, we will often be lazy and allow ourselves to write "G is a group".

Definition 3.4. If $(G, \star)$ is a group (Definition 3.3), we say that G is *abelian* if $\star$ is commutative.

Definition 3.5. If $n \in \mathbb{Z}_{\geq 3}$, then D_n is the symmetry group of an n-sided regular polygon with the operation of function composition.