

Some group theory definitions

Math 344

September 27, 2026

Contents

1	Sets and functions	1
2	Integers	3
2.1	Long division	3
3	Group basics	3
4	Some examples of groups	5
5	Functions from groups to other groups	5
6	Group invariants	5
6.1	Order	5
6.2	Cyclic groups	6
7	Partitions and equivalence relations	6
8	Cosets	7
9	Normal subgroups and homomorphisms	8

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:

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

This is often and conveniently abbreviated:

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 “ $f: S \rightarrow T$ ”, this is a function with domain S and codomain T . I will 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 $f: S \rightarrow T$ 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. In fact, we can generalize [Definition 1.6](#). Suppose $f: S \rightarrow T$ is a function.

- For any subset S' of S , the *image of S'* is the following subset of T :

$$f(S') = \{t \in T \mid \text{there exists } s \in S' \text{ such that } f(s) = t\}.$$

Note that when $S' = S$, we recover [Definition 1.6](#).

- For any subset T' of T , the *inverse image of T'* is the following subset of S :

$$f^{-1}(T') = \{s \in S \mid f(s) \in T'\}.$$

This definition is *not asserting that f is invertible*, it is just a notational choice.

Definition 1.8. 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 1.9. 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:

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

Definition 1.10. Suppose $f: S \rightarrow T$ is a function.

- We say that f is *injective* if

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

- 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 1.11. Suppose that $f: R \rightarrow S$ and $g: S \rightarrow T$ 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

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

Fact 1.1. *Function composition is associative. Specifically: if*

- $f: R \rightarrow S$,
- $g: S \rightarrow T$, and
- $h: T \rightarrow U$

are functions, then

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

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

- $g \circ f = \text{id}_S$ and
- $f \circ g = \text{id}_T$.

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

Fact 1.2. *Suppose $f: S \rightarrow T$ is a function. Then the following statement is true:*

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

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 2.1.

- 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.

2.1 Long division

Lemma 2.1 (Long division). *Suppose that $m, n \in \mathbb{Z}$ and $m \neq 0$. There is a unique pair of integers q, r such that the following two statements are true:*

- $n = qm + r$ and
- $0 \leq r < |m|$.

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.

Definition 3.6. Suppose G is a group (Definition 3.3) and $S \subseteq G$ (Definition 1.2). We say that S is a *subgroup* of G if the operation of G restricts to an operation on S that turns S into a group.

Remark 3.1. Definition 3.6 is a perfectly good definition, and gives a justification for the terminology “subgroup”. However, to prove that a subset of a group is a subgroup, we will always use Fact 3.1

Fact 3.1. Suppose G is a group with identity e and $S \subseteq G$. The subset S is a subgroup if and only if the following three statements are true:

1. $S \neq \emptyset$,
2. for all $a, b \in S$, $ab \in S$, and

3. for all $a \in S$, the inverse of a is also in S .

Fact 3.2. Suppose G is a group and $\mathcal{H}$ is a (possibly infinite) set of subgroups of G . Then $\cap_{H \in \mathcal{H}} H$ is a subgroup of G .

Definition 3.7. Suppose G is a group and $S \subseteq G$. Define $\langle S \rangle$ to be

$$\langle S \rangle = \bigcap_{\substack{\text{subgroups } H \text{ of } G \\ \text{satisfying } S \subseteq H}} H.$$

We say that $\langle S \rangle$ is the subgroup of G generated by S .

Remark 3.2. In light of [Fact 3.2](#), we know that if G is a group and $S \subseteq G$, then $\langle S \rangle$ is a subgroup (so we will never have to prove this). Moreover, [Definition 3.7](#) also tells us that no matter which subgroup H of G we choose: if $S \subseteq H$, then $\langle S \rangle \subseteq H$.

Definition 3.8. Suppose G is a group with identity e_G and a multiplicatively-written operation. For any $g \in G$ and $n \in \mathbb{Z}$, write

$$g^n = \begin{cases} \overbrace{g \cdots g}^{n \text{ times}} & \text{if } n > 0 \\ e_G & \text{if } n = 0 \\ \overbrace{g^{-1} \cdots g^{-1}}^{n \text{ times}} & \text{if } n < 0. \end{cases}$$

Now suppose the operation of G is additively-written. For any $g \in G$ and $n \in \mathbb{Z}$, write

$$ng = \begin{cases} \overbrace{g + \cdots + g}^{n \text{ times}} & \text{if } n > 0 \\ e_G & \text{if } n = 0 \\ \overbrace{(-g) + \cdots + (-g)}^{n \text{ times}} & \text{if } n < 0. \end{cases}$$

Fact 3.3 (Exponent rules). Suppose G is a group with a multiplicatively-written operation. Then for any $g \in G$ and $m, n \in \mathbb{Z}$,

- $g^{m+n} = g^m g^n$ and
- $g^{mn} = (g^m)^n$.

If the operation of G is additively-written, then for any $g \in G$ and $m, n \in \mathbb{Z}$,

- $(m+n)g = mg + ng$ and
- $(mn)g = m(ng)$.

4 Some examples of groups

Definition 4.1. For any $n \in \mathbb{Z}_{\geq 3}$, the group D_n consists of the symmetries of a regular n -gon, under the operation of function composition.

Definition 4.2. For any $n \in \mathbb{Z}_{\geq 2}$, the group $\mathbb{Z}_n$ consists of the integers $\{0, 1, \dots, n-1\}$ under the operation

$$j+k := \begin{cases} j+k & \text{if } j+k < n \\ (j+k) - n & \text{if } j+k \geq n. \end{cases}$$

Definition 4.3. If A is any set, write S_A for the group of bijective functions from A to A . By [Fact 1.2](#), all such functions are invertible, so S_A is a group with the operation of function composition.

Definition 4.4. If $n \in \mathbb{Z}_{\geq 1}$, we will write S_n for the group $S_{\{1, \dots, n\}}$.

Definition 4.5. If $n \in \mathbb{Z}_{\geq 1}$ and $\pi \in S_n$, the *parity* of π is even if π can be written as an even number of permutations and *odd* if it can be written as an odd number of permutations.

Definition 4.6. If $n \in \mathbb{Z}_{\geq 1}$, define the *alternating group* as the following subgroup of S_n :

$$A_n = \{\pi \in S_n \mid \pi \text{ is even}\}.$$

5 Functions from groups to other groups

Definition 5.1. Suppose that G_1, G_2 are groups and $\phi: G_1 \rightarrow G_2$ is a function. We say that ϕ is an *isomorphism* if

- ϕ is bijective and
- for all $g, h \in G_1$: $\phi(gh) = \phi(g)\phi(h)$.

6 Group invariants

6.1 Order

Definition 6.1. For any group G and element $g \in G$, the *order* of g is

$$\text{ord}(g) = |\langle g \rangle|.$$

Remark 6.1. Similar to our definition of subgroup, we have an alternate formulation of [Definition 6.1](#)—one that is often easier to use. I will refer to both [Definition 6.1](#) and [Definition 6.2](#) as “the definition of order”.

Definition 6.2. For any group G with identity e and element $g \in G$,

- if there is a positive integer n such that $g^n = e$, write $\text{ord}(g)$ for the smallest such positive integer, and
- if there is no such positive integer n , write $\text{ord}(g) = \infty$.

Fact 6.1. Suppose G is a group with identity e . Let $g \in G$ and $n \in \mathbb{Z}_{>0}$. If $g^n = e$, then $\text{ord}(g)$ is a divisor of n .

6.2 Cyclic groups

Definition 6.3. Let G be a group. If there exists some $g \in G$ such that $G = \langle g \rangle$, we say that G is *cyclic*. Any such g is called a *generator* of G .

Fact 6.2. Let G be a group and $g \in G$. Then

$$\langle g \rangle = \{g^j \mid j \in \mathbb{Z}\}.$$

Proof. By definition, we know that $\{g^j \mid j \in \mathbb{Z}\} \subseteq \langle g \rangle$. We must show that $\{g^j \mid j \in \mathbb{Z}\}$ is a subgroup, which I leave as an exercise for you. $\square$

7 Partitions and equivalence relations

Definition 7.1. Let A be a set. A *partition* of A is another set P such that

- for all $S \in P$, $S \subseteq A$,
- for all $S \in P$, $S \neq \emptyset$,
- for all $S, T \in P$, either $S = T$ or $S \cap T = \emptyset$, and
- $\bigcup_{S \in P} S = A$.

Often we are given an indexed sets of subsets of A . That is, some other set I (the indexing set) along with a subset of A for every $i \in I$, which we will call A_i for this definition. Then $\{A_i \mid i \in I\}$ is a *partition* of A if

- for all $i \in I$, there exists $a \in A_i$,
- for all $i, j \in I$, if there exists $a \in A_i \cap A_j$, then $i = j$.
- for all $a \in A$, there exists $i \in I$ with $a \in A_i$.

Definition 7.2. Suppose A is a set. A *relation* on A is any subset of $A \times A$.

Remark 7.1. Suppose that R is a relation on a set A . We will adopt the following notational convention for any $a, b \in A$:

instead of writing $(a, b) \in R$, we will instead write aRb .

(This is meant to mimic relations like “ $\leq$ ” on $\mathbb{R}$. For real number $x, y \in \mathbb{R}$, if it so happens that x is less than or equal to y , we write “ $x \leq y$ ” and we don’t write “ $(x, y) \in \mathbb{R}$ ”.)

Definition 7.3. Suppose that R is a relation on a set A .

1. We say R is *reflexive* if

$$\text{for all } a \in A, aRa.$$

2. We say R is *symmetric* if

$$\text{for all } a, b \in A, \text{ if } aRb, \text{ then } bRa.$$

3. We say R is *transitive* if

$$\text{for all } a, b, c \in A, \text{ if } aRb \text{ and } bRc, \text{ then } aRc.$$

4. We say R is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Definition 7.4. Suppose that R is an equivalence relation on a set A . For any $a \in A$, the *equivalence class* of a is the set

$$[a] = \{b \in A \mid bRa\}.$$

If $E \subseteq A$ is an equivalence class, then any $e \in E$ is called an *equivalence class representative* of E . I might refer to the set of equivalence classes as A/R . That is,

$$A/R = \{[a] \mid a \in A\}.$$

Fact 7.1. Let A be a set.

- If P is a partition on A , define a relation R_P on A via the condition: for all $a, b \in A \times A$,
 $aR_P b$ if and only if there exists $S \in P$ such that $a \in S$ and $b \in S$.

This is an equivalence relation on A .

- If R is an equivalence relation on A , then A/R is a partition of A .

Moreover,

- for any partition P of A , $A/(R_P) = P$ and
- for any equivalence relation R on A , $R_{A/R} = R$.

That is, these procedures of turning a partition into an equivalence relation and vice-versa are inverses of each other.

8 Cosets

Definition 8.1. Suppose G is a group and H is a subgroup of G . If $g \in G$, write

$$Hg = \{hg \mid h \in H\} \quad \text{and} \quad gH = \{gh \mid h \in H\}.$$

We say Hg is a *right coset* of H and gH is a *left coset* of H . We will write

$$G/H = \{Hg \mid g \in G\} \quad \text{and} \quad (G : H) = |G/H|.$$

We refer to the first set as “ $G \bmod H$ ” and the second quantity as “the index of H in G ”.

Fact 8.1. Suppose G is a group and H is a subgroup of G . Then:

1. G/H is a partition of G ,
2. for any $g \in G$, $g \in Hg$,
3. for any $g_1, g_2 \in G$: $Hg_1 = Hg_2$ if and only if $g_1(g_2)^{-1} \in H$, and
4. for any $g_1, g_2 \in G$, the function

$$\begin{aligned} Hg_1 &\rightarrow Hg_2 \\ hg_1 &\mapsto hg_2 \end{aligned}$$

is well-defined and bijective.

Theorem 8.1 (Lagrange’s Theorem). Suppose that H is a subgroup of a finite group G . Then $|H|$ is a divisor of $|G|$. (Which means that $(G : H)$ is a divisor of $|G|$ as well).

In particular, for any $g \in G$, we know that $\text{ord}(g)$ is a divisor of $|G|$ because $\text{ord}(g) = |\langle g \rangle|$ by [Definition 6.1](#).

9 Normal subgroups and homomorphisms

Definition 9.1. Suppose that ϕ is a function from a group G to a group H . We say that ϕ is a *homomorphism* if

$$\text{for all } g_1, g_2 \in G, \quad \phi(g_1g_2) = \phi(g_1)\phi(g_2).$$

Fact 9.1. Suppose that G, H are groups and $\psi: G \rightarrow H$ is a homomorphism. The notation we use below is from [Definition 1.7](#).

- If G' is a subgroup of G , then $\psi(G')$ is a subgroup of H .
- If H' is a subgroup of H , then $\psi^{-1}(H')$ is a subgroup of G .

Fact 9.2. Suppose G, H are groups with identities e_G, e_H , respectively. For any homomorphism $\phi: G \rightarrow H$,

- $\phi(e_G) = e_H$ and

- for all $g \in G$: $\phi(g)^{-1} = \phi(g^{-1})$.

Definition 9.2. Suppose G, H are groups with identities e_G, e_H , respectively. For any homomorphism $\phi: G \rightarrow H$, the kernel of ϕ is

$$\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}.$$

Definition 9.3. Suppose G is a group and H is a subgroup of G . We say that H is a normal subgroup when

$$\text{for all } g \in G \text{ and } h \in H, \quad ghg^{-1} \in H.$$

Fact 9.3. Suppose G is a group and H is a subgroup of G . It turns out that H is a normal subgroup of G if and only if

$$\text{for all } g \in G, \quad gH = Hg.$$

Fact 9.4. Suppose that G, H are groups and $\phi: G \rightarrow H$ is a homomorphism. Then $\ker(\phi)$ is a normal subgroup of G .

Fact 9.5. Suppose G, H are groups with identities e_G, e_H , respectively, and suppose ϕ is a homomorphism from G to H . Let's write $K = \ker(\phi)$.

- The subgroup K is normal in G .

- For all $g_1, g_2 \in G$:

$$\phi(g_1) = \phi(g_2) \quad \text{if and only if} \quad Kg_1 = Kg_2.$$

- The homomorphism ϕ is injective if and only if $K = \{e_G\}$. In other words: ϕ is injective if and only if

$$\text{for all } g \in G: \quad \text{if } \phi(g) = e_H, \text{ then } g = e_G.$$

Theorem 9.1. Suppose that G is a group and H is a subgroup of G . If H is a normal subgroup of G , then G/H is a subgroup, with the operation:

$$\text{for all } g_1, g_2 \in G: \quad (Hg_1)(Hg_2) = H(g_1g_2).$$

Fact 9.6. Suppose that G is a group and H a normal subgroup of G . Define

$$\begin{aligned} \pi: G &\rightarrow G/H \\ g &\mapsto Hg. \end{aligned}$$

Then π is a surjective homomorphism of groups.

Theorem 9.2. Suppose that G is a group and N is a normal subgroup of G . For all

- groups H and
- homomorphisms $\phi: G \rightarrow H$,

if $\ker(\phi) \supseteq N$, then the following is a well-defined homomorphism of groups:

$$\begin{aligned} \bar{\phi}: G/N &\rightarrow H \\ Ng &\mapsto \phi(g). \end{aligned}$$

Corollary 9.1 (Fundamental Homomorphism Theorem). Suppose that G, H are groups and $\phi: G \rightarrow H$ is a homomorphism, say with kernel K . Then the following is an isomorphism of groups:

$$\begin{aligned} \bar{\phi}: G/K &\rightarrow \phi(G) \\ Kg &\mapsto \phi(g). \end{aligned}$$

Proof. The fact that $\bar{\phi}$ is a homomorphism of groups follows from [Theorem 9.2](#). The fact that $\bar{\phi}$ is surjective follows from the fact that we have restricted the domain of ϕ to $\phi(G)$. The fact that $\bar{\phi}$ is injective follows from [Fact 9.5](#). $\square$