

Math 331 Fall 2026, Lecture 8 and 9: Groups concluded and summarized

website: <https://www.cip.ifi.lmu.de/~grinberg/t/26fa/>
(GPT-6 was used to polish the writing that follows.)

Remark 1.12.7. The answer to the question in Example 1.12.6 in Lecture 6–7 is “no”: the only central matrices in $\mathrm{GL}_n(\mathbb{R})$ are the (nonzero scalar) multiples λI_n of the identity matrix I_n . Let us outline how it is proved. Here n is a positive integer. For $n = 1$, every invertible 1×1 -matrix already has the form λI_n , so we may assume that $n \geq 2$.

Let $A = (a_{ij})_{1 \leq i, j \leq n} \in \mathrm{GL}_n(\mathbb{R})$ be a central matrix. Thus, A commutes with any invertible $n \times n$ -matrix. In particular, A commutes with the permutation matrix $T_{1,2}$ that differs from I_n in that its first two rows (or columns) are swapped:

$$T_{1,2} = \begin{pmatrix} & 1 & & & \\ 1 & & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

(where all invisible entries are 0's). But $T_{1,2} \in \mathrm{GL}_n(\mathbb{R})$ and

$$\begin{aligned} AT_{1,2} &= (A \text{ with columns 1 and 2 swapped}) & \text{and} \\ T_{1,2}A &= (A \text{ with rows 1 and 2 swapped}). \end{aligned}$$

Since A is central, we have $AT_{1,2} = T_{1,2}A$, so these two matrices are equal. Thus, for example, by comparing the $(1,2)$ -th entries of $AT_{1,2}$ and $T_{1,2}A$, we get

$$a_{1,1} = a_{2,2}.$$

Similarly,

$$a_{i,i} = a_{j,j} \quad \text{for all } i \neq j$$

(since we can play the same game with $T_{i,j}$ instead of $T_{1,2}$, where $T_{i,j}$ is the permutation matrix obtained from the identity matrix I_n by swapping its i -th and j -th rows). In other words, all diagonal entries of A are equal.

We can also consider the $n \times n$ -matrix

$$E_{1,2} = \begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix};$$

this is the identity matrix I_n with an extra 1 in the $(1,2)$ -th cell. This matrix $E_{1,2}$ is invertible: its inverse is I_n with an extra -1 in the same cell. Thus, $E_{1,2} \in \text{GL}_n(\mathbb{R})$, and

$$\begin{aligned} AE_{1,2} &= (A \text{ with column 1 added to column 2}) & \text{and} \\ E_{1,2}A &= (A \text{ with row 2 added to row 1}). \end{aligned}$$

Since A is central, these two products are equal. Comparing their $(2,2)$ -entries, we see

$$a_{2,1} + a_{2,2} = a_{2,2}.$$

Therefore,

$$a_{2,1} = 0.$$

Similarly,

$$a_{j,i} = 0 \quad \text{for all } j \neq i$$

(since we can play the same game with the matrix $E_{i,j}$ instead of $E_{1,2}$, where $E_{i,j}$ is the identity matrix I_n with an extra 1 in cell (i,j) , and we compare the (j,j) -th entries of $AE_{i,j}$ and $E_{i,j}A$). So our matrix A is diagonal. Since all its diagonal entries are equal, it therefore has the form

$$A = \text{diag}(\lambda, \lambda, \dots, \lambda) = \lambda I_n,$$

where $\lambda \in \mathbb{R}$ is a scalar that is nonzero (since A is invertible). Conversely, each such scalar matrix is central, as shown in Example 1.12.6. So we have shown that the only central matrices in $\text{GL}_n(\mathbb{R})$ are the λI_n -matrices. Thus,

$$Z(\text{GL}_n(\mathbb{R})) = \{\lambda I_n \mid \lambda \in \mathbb{R} \setminus \{0\}\}.$$

Here is a trivial fact:

Proposition 1.12.8. The center of a semigroup is always an abelian semigroup.

Proof. The center is a subsemigroup by Theorem 1.12.3 (a). Central elements commute with everything, hence with each other; thus, the center is abelian. $\square$

1.13. Two subgroup criteria

To check that a subset H of a group G is a subgroup, we must normally verify three conditions: that it is closed under multiplication (to be precise: under the operation of G), that it contains the neutral element, and that it is closed under taking inverses. In some situations, we can get by with less work. Here are two quicker criteria.

Proposition 1.13.1 (shortcut to subgroups I). Let G be a group (written multiplicatively), and let H be a nonempty subset of G . Then, H is a subgroup of G if and only if all $a, b \in H$ satisfy $ab^{-1} \in H$.

Proof. $\implies$: Assume that H is a subgroup of G . We must prove that all $a, b \in H$ satisfy $ab^{-1} \in H$.

Let $a, b \in H$. Then, $b^{-1} \in H$ (since H is closed under taking inverses¹), and thus $ab^{-1} \in H$ (since H is closed under multiplication² and $a \in H$). This proves the " $\implies$ " direction of the proposition.

$\impliedby$: Assume that all $a, b \in H$ satisfy

$$ab^{-1} \in H. \quad (1)$$

We must show that H is a subgroup of G .

First, there exists some $c \in H$ (since H is nonempty). Consider this c . By our assumption (1) (applied to $a = c$ and $b = c$), we then have $cc^{-1} \in H$, that is, $1 \in H$. So H contains the neutral element of G . Therefore, each $b \in H$ satisfies $b^{-1} = 1b^{-1} \in H$ (by (1), applied to $a = 1$). So H is closed under taking inverses. Consequently, for any $a, b \in H$, we have $a(b^{-1})^{-1} \in H$ (by our assumption (1), applied to b^{-1} instead of b). Of course, this latter relation rewrites as $ab \in H$ (since $(b^{-1})^{-1} = b$), and thus we have shown that H is closed under multiplication. So H is a subgroup of G (since it satisfies all three conditions). This proves the " $\impliedby$ " direction of the proposition. $\square$

Proposition 1.13.2 (shortcut to subgroups II). Let G be a **finite** group. Then, any nonempty subsemigroup of G is a subgroup of G .

Proof. Let T be a nonempty subsemigroup of G . We must show that T is a subgroup of G .

First, T is closed under multiplication (since T is a subsemigroup).

Pick any $c \in T$ (we can do this since T is nonempty). Then, Theorem 1.7.15 (a) from Lecture 5 (applied to $a = c$) shows that there exists a positive integer n such that $c^n = 1$ (since G is a group, so $c \in G$ has an inverse in G). Consider this n . But $c^n = \underbrace{cc \cdots c}_{n \text{ times}}$ (a nonempty product of c 's because n is positive), thus

$c^n \in T$ (since T is closed under multiplication and contains c). In other words, $1 \in T$ (since $c^n = 1$). This shows that T contains the neutral element of G . Therefore, T is a submonoid of G .

What about inverses? Let $a \in T$ be arbitrary. Then, Theorem 1.7.15 (a) from Lecture 5 shows that there exists a positive integer n such that $a^n = 1$ (again because G is a group, so $a \in G$ has an inverse). Consider such an n . Then, $a^{-1} = a^{n-1}$ (since $aa^{n-1} = a^n = 1$ and $a^{n-1}a = a^n = 1$). But $n > 0$,

¹because H is a subgroup of G

²because H is a subgroup of G

thus $n - 1 \in \mathbb{N}$, and therefore a^{n-1} is a nonnegative power of a . But T is a submonoid of G (as we saw above), and thus is closed under taking nonnegative powers (since a positive power is just a product of one and the same element, while a zeroth power is just the neutral element). Thus, from $a \in T$, we obtain $a^{n-1} \in T$. Therefore, $a^{-1} = a^{n-1} \in T$.

So we have shown that $a^{-1} \in T$ for each $a \in T$. In other words, T is closed under taking inverses. Thus, T is a subgroup of G . $\square$

Don't forget that both of the above propositions require nonemptiness! The empty set is never a subgroup.

In practice, these shortcuts are rarely ever needed. They save writing, not thinking. The proof ideas are more important than the results.

1.14. A note on notation

Did you grow tired of me constantly saying “written multiplicatively” in many of the above theorems? So did I. Therefore:

Convention 1.14.1. We shall write all semigroups (thus, in particular, all monoids and groups) multiplicatively unless we either say otherwise or are forced to do otherwise (e.g., because multiplication is already taken for something else). In particular, even an abelian group will usually be written multiplicatively.

1.15. Subgroups generated by subsets

1.15.1. The semigroup case

Most subsets B of a semigroup S will usually not be subsemigroups, because there is no reason to expect them to be closed under multiplication. However, we can make them closed under multiplication by repeatedly inserting the “missing” products into them. This construction can be achieved in one step by just adding all multi-factor products of elements of B into B :

Definition 1.15.1. Let S be a semigroup. Let B be a subset of S .

Then, the **subsemigroup of S generated by B** is defined to be the subset

$$\{b_1 b_2 \cdots b_k \mid k \in \mathbb{Z}_{>0} \text{ and } b_1, b_2, \dots, b_k \in B\}$$

of S . (So it is the set of all nonempty products of elements of B , including products of 1 factor as well as products of any positive number of factors. Note that equal factors are allowed!) We denote this subset by $\langle B \rangle_{\text{semi}}$.

Proposition 1.15.2.

- (a) This subset $\langle B \rangle_{\text{semi}}$ is actually a subsemigroup of S .
- (b) It contains B as a subset.
- (c) It is the smallest subsemigroup of S that contains B as a subset. More precisely: Any subsemigroup T of S that contains B as a subset must contain $\langle B \rangle_{\text{semi}}$ as a subset.

Proof.

- (a) We must show that $\langle B \rangle_{\text{semi}}$ is closed under multiplication. But this is clear: If we multiply two products $b_1 b_2 \cdots b_k$ and $b'_1 b'_2 \cdots b'_\ell$ of elements of B , then we get $b_1 b_2 \cdots b_k b'_1 b'_2 \cdots b'_\ell$, which is still a product of elements of B .
- (b) Each $b \in B$ is a product of elements of B : namely, a 1-factor product of itself. So it belongs to $\langle B \rangle_{\text{semi}}$. Therefore, $B \subseteq \langle B \rangle_{\text{semi}}$.
- (c) Let T be a subsemigroup of S that contains B as a subset. Then, it is closed under multiplication (since it is a subsemigroup). Since it contains all elements of B (because it contains B as a subset), it must therefore also contain all nonempty products of elements of B , including products of multiple factors. That is, it must contain all elements of $\langle B \rangle_{\text{semi}}$ (since the elements of $\langle B \rangle_{\text{semi}}$ are precisely all such products). In other words, it contains $\langle B \rangle_{\text{semi}}$ as a subset. $\square$

Example 1.15.3. Let S be a semigroup, and let $a \in S$. If B is the one-element set $\{a\}$, then

$$\langle B \rangle_{\text{semi}} = \{a^1, a^2, a^3, \dots\},$$

because the nonempty products of elements of $\{a\}$ are precisely $a^1, a^2, a^3, \dots$. So in particular, we recover the fact that $\{a^1, a^2, a^3, \dots\}$ is a subsemigroup of S (see (2) in Lecture 6).

1.15.2. The monoid case

We can play the same game for monoids, but the resulting submonoid will often differ from the subsemigroup $\langle B \rangle_{\text{semi}}$ because we have to adjoin a neutral element as well:

Definition 1.15.4. Let M be a monoid. Let B be a subset of M .

Then, the **submonoid of M generated by B** is defined to be the subset

$$\{b_1 b_2 \cdots b_k \mid k \in \mathbb{N} \text{ and } b_1, b_2, \dots, b_k \in B\}$$

of M . (So it is the set of all products of elements of B , but now including the empty product, which by definition is the neutral element of M . Note that the empty product can be taken even if B is empty.) We denote it by $\langle B \rangle_{\text{monoid}}$.

Proposition 1.15.5.

- (a) This subset $\langle B \rangle_{\text{monoid}}$ is actually a submonoid of M .
- (b) It contains B as a subset.
- (c) It is the smallest submonoid of M that contains B as a subset. More precisely: Any submonoid N of M that contains B as a subset must contain $\langle B \rangle_{\text{monoid}}$ as a subset.

Proof. This is an easy adaptation of the proof of Proposition 1.15.2. In part (a), the empty product brings the neutral element into $\langle B \rangle_{\text{monoid}}$. $\square$

Example 1.15.6. Let M be a monoid, and let $a \in M$. If B is the one-element set $\{a\}$, then

$$\langle B \rangle_{\text{monoid}} = \{a^0, a^1, a^2, a^3, \dots\},$$

because the products of elements of $\{a\}$ are precisely $a^0, a^1, a^2, a^3, \dots$. Thus, we recover the fact that $\{a^0, a^1, a^2, a^3, \dots\}$ is a submonoid of M (see (3) in Lecture 6).

1.15.3. The group case

Finally, we define the subgroup of a group G generated by a given subset B . The idea is the same as for semigroups and for monoids, but the execution would get a bit tricky if we tried to blindly follow the previous method: in addition to just taking products of elements of B , we would have to take their inverses, as well as products of their inverses (and of original elements of B), but also inverses of such products, and products of such inverses, and so on, ad infinitum. In principle, such constructions can be made, but here we can find a much easier way. Indeed, any “inverse-product matryoshka” such as $(ab)^{-1}(cd^{-1}e)^{-1}f(g^{-1}h)^{-1}ij^{-1}$ can be unravelled into a single product (in this example, into $b^{-1}a^{-1}e^{-1}dc^{-1}fh^{-1}gij^{-1}$) using Theorem 1.4.3 and Theorem 1.3.5. Thus, all we need are the elements of B , their inverses, and the products of these. This suggests the following simple definition of the subgroup we are looking for:

Definition 1.15.7. Let G be a group. Let B be a subset of G . Then, we define the subset

$$B^{-1} := \{b^{-1} \mid b \in B\}$$

of G . Subsequently, the **subgroup of G generated by B** is defined to be the submonoid of G generated by $B \cup B^{-1}$. We denote it by $\langle B \rangle$. Thus,

$$\langle B \rangle := \langle B \cup B^{-1} \rangle_{\text{monoid}}. \quad (2)$$

Proposition 1.15.8.

- (a) This subset $\langle B \rangle$ is actually a subgroup of G .
- (b) It contains B as a subset.
- (c) It is the smallest subgroup of G that contains B as a subset. More precisely: Any subgroup H of G that contains B as a subset must contain $\langle B \rangle$ as a subset.

Proof.

- (a) We defined $\langle B \rangle$ as $\langle B \cup B^{-1} \rangle_{\text{monoid}}$, so we know it is a submonoid of G (by Proposition 1.15.5 (a), applied to $B \cup B^{-1}$ instead of B). It remains to prove that it is closed under taking inverses.

First, we observe that

$$a^{-1} \in B \cup B^{-1} \text{ for each } a \in B \cup B^{-1}. \quad (3)$$

(*Proof:* Let $a \in B \cup B^{-1}$. Thus, $a \in B$ or $a \in B^{-1}$. If $a \in B$, then the definition of B^{-1} yields $a^{-1} \in B^{-1} \subseteq B \cup B^{-1}$, so that (3) is proved in this case. Thus, only the case $a \in B^{-1}$ remains to be handled. In this case, we have $a = b^{-1}$ for some $b \in B$ (since $a \in B^{-1} = \{b^{-1} \mid b \in B\}$). Thus, for this b , we have $a^{-1} = (b^{-1})^{-1} = b$ (by Theorem 1.3.5 (a)) and thus $a^{-1} = b \in B \subseteq B \cup B^{-1}$. So we have proved (3) in both cases.)

Now, let $b \in \langle B \rangle$. Then, $b \in \langle B \rangle = \langle B \cup B^{-1} \rangle_{\text{monoid}}$. By Definition 1.15.4, this shows that b is a product $a_1 a_2 \cdots a_k$ of some elements $a_1, a_2, \dots, a_k$ of $B \cup B^{-1}$, where $k \in \mathbb{N}$. Consider these elements $a_1, a_2, \dots, a_k$. Then, from $b = a_1 a_2 \cdots a_k$, we obtain

$$b^{-1} = (a_1 a_2 \cdots a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1} \quad (\text{by Theorem 1.4.3}).$$

But all of the factors $a_k^{-1}, a_{k-1}^{-1}, \dots, a_1^{-1}$ belong to $B \cup B^{-1}$ (by (3), since $a_k, a_{k-1}, \dots, a_1$ belong to $B \cup B^{-1}$). Hence, $a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1}$ is a product of elements of $B \cup B^{-1}$, and therefore belongs to $\langle B \cup B^{-1} \rangle_{\text{monoid}}$ (by Definition

1.15.4). Thus,

$$b^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1} \in \langle B \cup B^{-1} \rangle_{\text{monoid}} = \langle B \rangle.$$

So we have proved that $b^{-1} \in \langle B \rangle$ for each $b \in \langle B \rangle$. In other words, $\langle B \rangle$ is closed under taking inverses. Thus it is a subgroup of G ; this proves part (a).

- (b) Proposition 1.15.5 (b) shows that the submonoid $\langle B \cup B^{-1} \rangle_{\text{monoid}}$ contains $B \cup B^{-1}$ as a subset; hence, it also contains B as a subset. In other words, $\langle B \rangle$ contains B as a subset.
- (c) Let H be a subgroup of G that contains B as a subset. Since H is closed under taking inverses, it therefore also contains B^{-1} , and hence contains the union $B \cup B^{-1}$. Moreover, H is a submonoid of G (being a subgroup of G). Proposition 1.15.5 (c) (applied to G , H and $B \cup B^{-1}$ instead of M , N and B) thus shows that H must contain $\langle B \cup B^{-1} \rangle_{\text{monoid}}$ as a subset. In other words, H contains $\langle B \rangle$ as a subset (since $\langle B \rangle = \langle B \cup B^{-1} \rangle_{\text{monoid}}$). This proves part (c). $\square$

Example 1.15.9. Let G be a group, and let $a \in G$. If B is the one-element set $\{a\}$, then

$$\langle B \rangle = \{a^n \mid n \in \mathbb{Z}\}. \quad (4)$$

One way to see this is by observing that $B \cup B^{-1} = \{a, a^{-1}\}$, and that the products of a 's and a^{-1} 's are simply the integer powers a^n of a : for example, $aaa^{-1}aa^{-1}a^{-1}aaa^{-1}a = a^2$. Thus, in particular, we recover the fact that $\{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G . Alternatively, if we take this fact as a given, we can use Proposition 1.15.8 (c) to show that $\langle B \rangle \subseteq \{a^n \mid n \in \mathbb{Z}\}$, whereas Proposition 1.15.8 (a), (b) yields the converse inclusion $\{a^n \mid n \in \mathbb{Z}\} \subseteq \langle B \rangle$ (since $\langle B \rangle$ is a subgroup containing a , so it contains all integer powers of a); thus (4) follows.

Definition 1.15.10. Let $a_1, a_2, \dots, a_k$ be k elements of a group G . Then, the subgroup $\langle \{a_1, a_2, \dots, a_k\} \rangle$ of G will be simply denoted by $\langle a_1, a_2, \dots, a_k \rangle$. That is, we drop the set-braces and simply write down the elements themselves inside the angular brackets.

In particular, $\langle a \rangle = \langle \{a\} \rangle = \{a^n \mid n \in \mathbb{Z}\}$ for any $a \in G$. (This subgroup $\langle a \rangle$ is called a **cyclic subgroup** of G , though a proper definition of a cyclic group will have to wait until the next chapter.)

Similar notations will be used for semigroups and monoids: e.g., we write $\langle a \rangle_{\text{monoid}}$ for $\langle \{a\} \rangle_{\text{monoid}}$.

1.15.4. Assorted examples

Example 1.15.11. Recall the abelian group $(\mathbb{Q}, +)$. Keep in mind that it is written additively, so all products in the general definitions above must be read as sums when working in this group.

We have the subsemigroup

$$\begin{aligned} \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{semi}} &= \left\{ b_1 + b_2 + \cdots + b_k \mid \begin{array}{l} k \in \mathbb{Z}_{>0}, \\ b_1, b_2, \dots, b_k \in \left\{ \frac{1}{2}, \frac{1}{3} \right\} \end{array} \right\} \\ &= \left\{ \text{all nonempty sums of } \frac{1}{2}\text{'s and } \frac{1}{3}\text{'s} \right\} \\ &= \left\{ n \cdot \frac{1}{2} + m \cdot \frac{1}{3} \mid n, m \in \mathbb{N} \text{ with } n + m > 0 \right\} \end{aligned}$$

and the submonoid

$$\begin{aligned} \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{monoid}} &= \left\{ b_1 + b_2 + \cdots + b_k \mid \begin{array}{l} k \in \mathbb{N}, \\ b_1, b_2, \dots, b_k \in \left\{ \frac{1}{2}, \frac{1}{3} \right\} \end{array} \right\} \\ &= \left\{ \text{all sums of } \frac{1}{2}\text{'s and } \frac{1}{3}\text{'s including the empty sum} \right\} \\ &= \left\{ n \cdot \frac{1}{2} + m \cdot \frac{1}{3} \mid n, m \in \mathbb{N} \right\} \\ &= \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{semi}} \cup \{0\} \end{aligned}$$

and the subgroup

$$\begin{aligned} \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle &= \left\langle \frac{1}{2}, \frac{1}{3}, -\frac{1}{2}, -\frac{1}{3} \right\rangle_{\text{monoid}} \quad \left(\begin{array}{l} \text{since the inverse of } b \\ \text{in our group is } -b \end{array} \right) \\ &= \left\{ b_1 + b_2 + \cdots + b_k \mid \begin{array}{l} k \in \mathbb{N}, \\ b_1, b_2, \dots, b_k \in \left\{ \frac{1}{2}, \frac{1}{3}, -\frac{1}{2}, -\frac{1}{3} \right\} \end{array} \right\} \\ &= \left\{ n \cdot \frac{1}{2} + m \cdot \frac{1}{3} \mid n, m \in \mathbb{Z} \right\}. \end{aligned}$$

In the last equality, we collect the positive and negative copies of each fraction to obtain an integer multiple of this fraction. Note that we have used the commutativity of $+$ to normalize arbitrarily ordered sums such as $\frac{1}{2} + \frac{1}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{2}$ into simple linear combinations of the form $n \cdot \frac{1}{2} + m \cdot \frac{1}{3}$; this would not work for a non-abelian group!

We have a chain of inclusions

$$\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{semi}} \subseteq \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{monoid}} \subseteq \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle \subseteq \mathbb{Q}.$$

All these inclusions are proper, i.e., each set contains an element not in the previous set. For example:

- We have $\frac{5}{6} \in \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{semi}}$ because $\frac{5}{6} = \frac{1}{2} + \frac{1}{3}$.
- We have $0 \in \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{monoid}} \setminus \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{semi}}$.
- Both $-\frac{1}{2}$ and $\frac{1}{6}$ belong to $\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle \setminus \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{monoid}}$. In fact, $\frac{1}{6} = \frac{1}{2} - \frac{1}{3} \in \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle$ but $\frac{1}{6} \notin \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle_{\text{monoid}}$ (since any sum $n \cdot \frac{1}{2} + m \cdot \frac{1}{3}$ with $n, m \in \mathbb{N}$ is either 0 or $\geq \frac{1}{3}$).
- We have $\frac{1}{4}, \frac{1}{5} \in \mathbb{Q} \setminus \left\langle \frac{1}{2}, \frac{1}{3} \right\rangle$. Indeed, any $n \cdot \frac{1}{2} + m \cdot \frac{1}{3}$ with $n, m \in \mathbb{Z}$ can be rewritten as $\frac{3n+2m}{6}$, so it becomes an integer when multiplied by 6. But neither $\frac{1}{4}$ nor $\frac{1}{5}$ becomes an integer when multiplied by 6.

The subgroup $\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle$ can be described in a simpler way:

$$\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle = \left\{ \frac{k}{6} \mid k \in \mathbb{Z} \right\}.$$

Indeed, as we just saw, every element $n \cdot \frac{1}{2} + m \cdot \frac{1}{3}$ of $\left\langle \frac{1}{2}, \frac{1}{3} \right\rangle$ has the form $\frac{k}{6}$ for $k = 3n + 2m$; conversely, any $\frac{k}{6}$ can be written as $k \cdot \frac{1}{2} + (-k) \cdot \frac{1}{3}$.

So we see that the same subset of a group generates a subsemigroup, a submonoid and a subgroup, and these are generally not the same.

However, they are the same when the group is finite and the subset is nonempty:

Proposition 1.15.12. Let G be a **finite** group. Let $B \subseteq G$ be nonempty. Then,

$$\langle B \rangle_{\text{semi}} = \langle B \rangle_{\text{monoid}} = \langle B \rangle.$$

Proof. We know that $\langle B \rangle_{\text{semi}}$ is a subsemigroup of G , and furthermore is nonempty (since it contains B as a subset, but B is nonempty). But we also know (Proposition 1.13.2) that every nonempty subsemigroup of a finite group is already a subgroup. So $\langle B \rangle_{\text{semi}}$ is a subgroup of G .

But $\langle B \rangle$ is the smallest subgroup of G that contains B as a subset (by Proposition 1.15.8 (c)). Since $\langle B \rangle_{\text{semi}}$ is such a subgroup, we thus conclude that $\langle B \rangle \subseteq \langle B \rangle_{\text{semi}}$.

On the other hand, $\langle B \rangle_{\text{semi}} \subseteq \langle B \rangle$, because products of elements of B clearly belong to $\langle B \rangle$.

Combining these two inclusions, we obtain $\langle B \rangle_{\text{semi}} = \langle B \rangle$.

An analogous argument (now including the empty product) shows that $\langle B \rangle_{\text{monoid}} = \langle B \rangle$ (since submonoids are subsemigroups).

Thus, Proposition 1.15.12 is proved. $\square$

The nonemptiness assumption in Proposition 1.15.12 is needed: if $B = \emptyset$, then $\langle B \rangle_{\text{semi}} = \emptyset$, whereas $\langle B \rangle_{\text{monoid}} = \langle B \rangle = \{1\}$.

Example 1.15.13. Consider the symmetric group S_3 . For any two distinct elements i and j of $\{1, 2, 3\}$, we let $t_{i,j}$ denote the permutation that swaps i with j while keeping all the other elements unchanged. Set $s_1 = t_{1,2}$ and $s_2 = t_{2,3}$ and $w_0 = t_{1,3}$. Let c be the cycle $1 \mapsto 2 \mapsto 3 \mapsto 1$. As we know,

$$S_3 = \{\text{id}, s_1, s_2, w_0, c, c^2\}.$$

Then,

$$\langle c \rangle = \{c^n \mid n \in \mathbb{Z}\} = \{\text{id}, c, c^2\} \quad (\text{since } o(c) = 3),$$

$$\langle s_1 \rangle = \{\text{id}, s_1\} \quad (\text{since } o(s_1) = 2),$$

$$\langle s_2 \rangle = \{\text{id}, s_2\},$$

and

$$\langle s_1, s_2 \rangle = \{\text{id}, s_1, s_2, w_0, c, c^2\}$$

(since $w_0 = s_1 s_2 s_1$ and $c = s_1 s_2$ and $c^2 = s_2 s_1$). Thus, every one of the six elements of S_3 belongs to $\langle s_1, s_2 \rangle$; the reverse inclusion holds because this is a subgroup of S_3 . The latter equality, of course, says that $\langle s_1, s_2 \rangle = S_3$. We can say this as follows: the elements s_1 and s_2 **generate** the group S_3 .

More generally:

Definition 1.15.14. Let $a_1, a_2, \dots, a_k$ be some elements of a group G . We say that these elements **generate** the group G if $\langle a_1, a_2, \dots, a_k \rangle = G$.

Similarly we can define what it means for some elements of a monoid to generate the monoid, or for some elements of a semigroup to generate the

semigroup; however, it should be kept in mind that the three notions are not equivalent in the case of a group, so a careful writer must signal which one is meant. (That is, if there is any possibility for confusion, do not say “ $a_1, a_2, \dots, a_k$ generate G ”; always say “ $a_1, a_2, \dots, a_k$ generate the group G ” or “... the monoid G ” or “... the semigroup G ”.)

1.16. A group-focused summary

We will mostly be dealing with groups in this course, not semigroups or monoids. However, I have been stating everything in maximum possible generality so far. Let us summarize the most important results specialized to the case of groups.

1.16.1. The main definitions and notations

- A **group** is a set G equipped with a binary operation $*$ that is associative, such that G has a neutral element and each element of G has an inverse (under $*$). (Definition 1.1.1 (**g**), Lecture 2–3.) Keep in mind that a “binary operation” on G in our definition of this word has to be a map from $G \times G$ to G .
- A **subgroup** of a group $(G, *)$ is a subset H of G that is closed under $*$, contains the neutral element of G and is closed under taking inverses. We write $H \leq G$ for this. (Definition 1.11.3, Lecture 6–7.)
- A group $(G, *)$ is said to be **abelian** if all its elements commute (i.e., if $a * b = b * a$ for all $a, b \in G$). (Definition 1.10.3, Lecture 6–7.)
- To write a group $(G, *)$ in **multiplicative notation** means that we write ab for $a * b$, write 1 for the neutral element, and write a^{-1} for the inverse of a . (Definition 1.5.1, Lecture 4, and Definition 1.3.4, Lecture 2–3.)

We use multiplicative notation by default when nothing speaks against it.

- To write an abelian group $(G, *)$ in **additive notation** means that we write $a + b$ for $a * b$, write 0 for the neutral element, and write $-a$ for the inverse of a . (Definition 1.10.4, Lecture 6–7.)
- The **powers** of an element a in a group G (written multiplicatively) are defined by

$$a^n := \begin{cases} \underbrace{aa \cdots a}_{n \text{ times}}, & \text{if } n > 0; \\ 1, & \text{if } n = 0; \\ (a^{-1})^{-n}, & \text{if } n < 0 \end{cases} \quad \text{for all } n \in \mathbb{Z}.$$

If we write G additively, then we write na instead of a^n . (Definition 1.7.1, Lecture 5, and Definition 1.10.4, Lecture 6–7.)

- The **order** $o(a)$ of an element a in a group G is the smallest positive integer n such that $a^n = 1$ if such an n exists; otherwise it is ∞ . (Definition 1.8.1, Lecture 6–7.)
- The **subgroup generated by** a subset $B \subseteq G$, denoted by $\langle B \rangle$, consists of all finite products of elements of B and their inverses, including the empty product. It is the smallest subgroup of G containing B . (Definition 1.15.7 and Proposition 1.15.8 above.)

1.16.2. The main examples

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups (but $(\mathbb{N}, +)$ is not). They form a chain of subgroups:

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +).$$

(§1.2, Lecture 2–3, and §1.11, Lecture 6–7.)

- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are abelian groups (but $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group). They also form a chain of subgroups. (§1.2, Lecture 2–3; the subgroup conditions are checked just as for the additive groups above.)
- Two very small groups are the trivial group $(\{1\}, \cdot)$ and the group $(\{1, -1\}, \cdot)$ with two elements. (§1.2, Lecture 2–3.)
- For any set A , the permutations of A form a group S_A under composition (§1.2, Lecture 2–3). This group is called the **symmetric group** of A . If A is finite of size n , then S_A is finite of size $|S_A| = n!$ (see Math 222 or Math 221).
- If A is any set, then $(\mathcal{P}(A), \triangle)$ is a group, in which all elements have order 1 or 2. If A is finite of size n , then $|\mathcal{P}(A)| = 2^n$ (see Math 222 or Math 221). (The operation $\triangle$ is defined by $X \triangle Y = (X \cup Y) \setminus (X \cap Y)$. See §1.2 in Lecture 2–3; for the orders, see Example 1.8.7 in Lecture 6–7.)
- All $n \times m$ -matrices with real entries form a group $(\mathbb{R}^{n \times m}, +)$. All invertible $n \times n$ -matrices form a group $(GL_n(\mathbb{R}), \cdot)$. (§1.2, Lecture 2–3³.)

³The addition example there is stated for square matrices, but the same argument applies to rectangular ones.

1.16.3. The main theorems

Let G be a group, written multiplicatively. All elements below belong to G .

- Generalized associativity (Theorem 1.4.2 **(b)**, Lecture 4): Products of the form $a_1 a_2 \cdots a_n$ are well-defined without specifying the parenthesization; they can be parenthesized at will:

$$a_1 a_2 \cdots a_n = (a_1 a_2 \cdots a_k) (a_{k+1} a_{k+2} \cdots a_n).$$

Here $0 \leq k \leq n$ are integers, and an empty product is 1.

- Inverses satisfy (Theorem 1.3.5, Lecture 2–3)

$$(ab)^{-1} = b^{-1} a^{-1} \quad \text{and} \quad (a^{-1})^{-1} = a.$$

- Solving equations (Theorem 1.6.1 **(a)**, **(b)**, Lecture 4):

$$ab = c \iff b = a^{-1}c$$

and

$$ba = c \iff b = ca^{-1}.$$

- Cancellation (Theorem 1.6.1 **(c)**, **(d)**, Lecture 4):

$$ab = ac \iff b = c$$

and

$$ba = ca \iff b = c.$$

- For any $a \in G$, the maps L_a (left multiplication by a) and R_a (right multiplication by a) are bijective. (Corollary 1.6.4, Lecture 4.)
- Rules of exponents: For all $a \in G$ and all $n, m \in \mathbb{Z}$, we have

$$\begin{aligned} a^n a^m &= a^{n+m}, \\ (a^n)^m &= a^{nm}, \\ a^{-n} &= (a^{-1})^n = (a^n)^{-1} \end{aligned}$$

(Theorems 1.7.9, 1.7.11 and 1.7.7, and Lemma 1.7.10, Lecture 5). Moreover, if $a, b \in G$ commute, then $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$ (Theorem 1.7.12, Lecture 5).

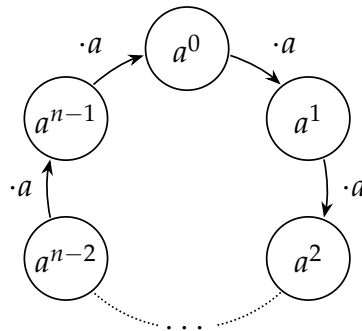
(The integer-exponent version of $(a^n)^m = a^{nm}$ and the rule $(ab)^n = a^n b^n$ for commuting a and b are on homework set #2; don't use them without proof yet.)

- If G is finite, then each $a \in G$ has finite order $o(a)$ (Theorem 1.7.15 (a), Lecture 5). Denoting this order by n , we have

$$\{\text{all powers of } a\} = \{a^0, a^1, \dots, a^{n-1}\},$$

and furthermore, these n powers $a^0, a^1, \dots, a^{n-1}$ are distinct. (Theorem 1.8.5 (a), (c), Lecture 6–7.)

The powers form a cycle under right multiplication by a , since $a^{n-1}a = a^n = 1 = a^0$. Its shape is shown schematically in the following picture:



(Note that if $a = 1$, then this cycle consists of just a single node a^0 with a single loop back to it.)

- Any subgroup H of a group G becomes a group itself if we restrict the multiplication of G to H (Theorem 1.11.7, Lecture 6–7).