

GENERATORS OF A GROUP

Let G be a group and S be a subset of G . Then we define the *group generated by S* as the smallest subgroup of G which contains S . This is denoted by $\langle S \rangle$. Dually we say that $\langle S \rangle$ is *generated by S* . Written out, this really means three things

$$\mathbf{G1} \quad S \subset \langle S \rangle$$

$$\mathbf{G2} \quad \langle S \rangle \text{ is a subgroup of } G$$

$$\mathbf{G3} \quad \text{if } K \text{ also satisfies } (\mathbf{G1}) \text{ and } (\mathbf{G2}), \text{ then } \langle S \rangle \subset K$$

¹ This notion is well defined, i.e. there exists a unique subset of G which satisfies $(\mathbf{G1})$, $(\mathbf{G2})$, and $(\mathbf{G3})$ above (as opposed to say defining a *fraggle* as the largest state which contains the north pole or *wizzle* as the state adjacent to Washington DC which has the largest number of 'a's' in its name) since if there were two subgroups which satisfied $(\mathbf{G1})$, $(\mathbf{G2})$, and $(\mathbf{G3})$ above, then their intersection would also satisfy these three properties and would be contained inside of both. More precisely we have the following:

Lemma 1. *The intersection of all subgroups which contains S is non-empty and is equal to $\langle S \rangle$*

Proof. The intersection of all subgroups which contains S is denoted as

$$\bigcap_{\{H: S \subset H \text{ and } H < G\}} H$$

or simply $\bigcap H$. Since S is contained in all subgroups which contain S we have that $S \subset \bigcap H$ provided that there exists at least one subgroup which contains S . But this is certainly the case since S is a subset of G by assumption. In particular $\langle S \rangle$ is not empty (and not trivial provided that $S \neq \emptyset$).

Now it is easy to see that $\bigcap H$ is a subgroup of G (you actually proved in homework 3 that the intersection of two subgroups is a subgroup and the proof that the intersection of an arbitrary number of subgroups is a subgroup is the same). Thus we must have that $\langle S \rangle \subset \bigcap H$ by property $(\mathbf{G3})$ above.

We now show that $\bigcap H \subset \langle S \rangle$. Indeed since $\langle S \rangle$ is a subgroup of G which contains S we must have that one of the subgroups we are intersecting to get $\bigcap H$ is $\langle S \rangle$ itself. This implies that

$$\bigcap H \subset \bigcap H \cap \langle S \rangle \subset \langle S \rangle.$$

Thus we have proven the lemma. □

Here are some more useful facts about $\langle S \rangle$.

Lemma 2. (1) *If $S \subset T$, then $\langle S \rangle \subset \langle T \rangle$.*

(2) *$\langle H \rangle = H$ for any subgroup H of G .*

(3) *$\langle \langle S \rangle \rangle = \langle S \rangle$.*

(4) *If $S \subset T \subset \langle S \rangle$, then $\langle S \rangle = \langle T \rangle$.*

¹Typically for the set $\{s_1, \dots, s_n\}$ we denote $\langle \{s_1, \dots, s_n\} \rangle$ by $\langle s_1, \dots, s_n \rangle$. That is we drop the brackets.

- (5) Every group is generated by a set S .
 (6) $\langle S \cup T \rangle = \langle \langle S \rangle \cup \langle T \rangle \rangle$

Proof. (1) By property **(G1)** following the definition of $\langle S \rangle$ (applied to T) we have that $T \subset \langle T \rangle$. Hence $S \subset \langle T \rangle$. By **(G2)** we have that $\langle T \rangle$ is a subgroup of G . Hence we apply property **(G1)** to conclude that $\langle S \rangle \subset \langle T \rangle$ as desired.

(2) This is immediate since H clearly satisfies properties **(G1)** (H contains itself), **(G2)** (it is a subgroup of G by assumption), and **(G3)** (this is the logical tautology that H is contained in any subgroup containing H).

(3) Follows from (2) since $\langle S \rangle$ is a subgroup of G .

(4) We are assuming that $S \subset T \subset \langle S \rangle$. Thus applying (1) we have that $\langle S \rangle \subset \langle T \rangle \subset \langle \langle S \rangle \rangle$. But (3) says that $\langle \langle S \rangle \rangle = \langle S \rangle$. Hence $\langle S \rangle \subset \langle T \rangle \subset \langle S \rangle$ or $\langle S \rangle \subset \langle T \rangle$ and $\langle T \rangle \subset \langle S \rangle$ and so $\langle S \rangle = \langle T \rangle$.

(5) Follows from (2) since (2) says that the group generated by any given group is the group itself. Thus, if by “some set” we can take the group itself.

(6) Ok, this one doesn’t really fit in here, but its proof allows us to understand the formal properties of $\langle \rangle$ a little bit better. For starters we have

$$\begin{aligned} S \subset \langle S \rangle, T \subset \langle T \rangle &\Rightarrow S \cup T \subset \langle S \rangle \cup \langle T \rangle && \text{(definition of union)} \\ &\Rightarrow \langle S \cup T \rangle \subset \langle \langle S \rangle \cup \langle T \rangle \rangle && \text{(by (1) of this Lemma)} \end{aligned}$$

and on the other hand we have

$$\begin{aligned} S \subset S \cup T \text{ and } T \subset S \cup T &\Rightarrow \langle S \rangle \subset \langle S \cup T \rangle \text{ and } \langle T \rangle \subset \langle S \cup T \rangle && \text{(part (1) of lemma again)} \\ &\Rightarrow \langle S \rangle \cup \langle T \rangle \subset \langle S \cup T \rangle && \text{(property of union)} \\ &\Rightarrow \langle \langle S \rangle \cup \langle T \rangle \rangle \subset \langle \langle S \cup T \rangle \rangle && \text{(part (1) again)} \\ &\Rightarrow \langle \langle S \rangle \cup \langle T \rangle \rangle \subset \langle S \cup T \rangle && \text{(part (2) with } H = \langle S \cup T \rangle) \quad \square \end{aligned}$$

Properties (1) and (2) listed above can be stated as $\langle \rangle$ is a projection from the set of all subsets of a group to the set of subgroup of a group.

Example 1. As usual we let A_4 be the alternating group on 4 letters (this group has order 12). We show that two elements σ, τ generate A_4 if and only they do not commute, so for instance $\langle (123), (234) \rangle = A_4$. Indeed by Lagrange’s theorem every subgroup of A_4 has order a divisor of 12. Hence if $\langle \sigma, \tau \rangle \neq A_4$, then $|\langle \sigma, \tau \rangle| = 6, 4, 3$ or 2. In homework assignment 7 you showed that no subgroup of A_4 has order 6. Thus $|\langle \sigma, \tau \rangle| = 4, 3$ or 2, but all groups of these orders are abelian and hence σ and τ must commute.

Proposition 1. Suppose $g \in G$ has finite order n , then

$$\langle g \rangle = \{1, g, \dots, g^{n-1}\} = \{g^i : i \in \mathbb{Z}, 0 \leq i < n\}$$

or if g has infinite order

$$\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$$

²note that in both cases this set really equals the second set, but in the case that the order of g is finite, this second set will have many redundancies.

Proof. These are simply done by noting that $\{g^i : i \in \mathbb{Z}\}$ is a subgroup of G and any subgroup which contains g must contain all powers of g and its inverse. \square

Corollary 1. *The order of the group generated by g is equal to the order of g .*

Proof. In the case that the order of g is finite we see this from the previous proposition since $\{g^i : i \in \mathbb{Z}\}$ has $|g|$ elements in it and no redundancies since if $g^i = g^j$ for some pair of distinct integers i and j greater than or equal to 0 but less than $|g|$, then WLOG assuming that $i < j$ we have that $j - i < |g|$ and $g^{j-i} = 1_G$ which contradicts the definition of the order of an element. \square

For S a non-empty subset of G , we define $S^{-1} := \{s^{-1} : s \in S\}$ and $S^\pm := S \cup S^{-1}$. A word in S is (finite) product of elements in S^\pm , i.e. w is a word in S if and only if there exists elements s_1, \dots, s_n so that $w = s_1 \cdots s_n$ (notice that the identity is a word in S since for an element $s \in S$ we have $ss^{-1} = 1$). Said in another way we can define the set of words in S inductively by stating that

- (1) The identity is a word in S .
- (2) If w is a word in S , and $s \in S^\pm$, then ws is a word in S .

In practice this definition makes it fairly straight forward to find words in S , but unfortunately it very difficult to show something is *not* a word in S .

Lemma 3. (1) *The set of words in S forms a subgroup of G .*
 (2) *If w is a word in S , then $w \in \langle S \rangle$.*

Proof. (1) We temporarily denote the set of words in S by $W(S)$. Any $s \in S$ is a word in S so $W(S)$ is non-empty. Now if $w = s_1 \cdots s_n$ is a word in S , then each of $s_1, \dots, s_n \in S^\pm \Rightarrow s_1^{-1}, \dots, s_n^{-1} \in S^\pm$ which implies that $s_n^{-1} \cdots s_1^{-1}$ is a word in S . Since this last word is the inverse of w we have that the set of words is closed under inversion. Finally for $w_1, w_2 \in W(S)$ we can inductively assume that $w_2 \in S^\pm$. Thus by the inductive definition of words in S we have that $w_1 w_2 \in W(S)$.

(2) We must show that any word w is in any subgroup H which contains S . Indeed if H contains S , then H contains S^\pm and hence it must contain any product of elements of S^\pm . But these are precisely the set of words in S . \square

Theorem 1. *For any nonempty subset S of G we have that $\langle S \rangle$ is equal to the set of words in S .*

Proof. We maintain the notation $W(S)$ for the set of words in S that we used in the lemma. Since $S \subset W(S)$ and $W(S)$ is a group by the lemma we have that $\langle S \rangle \subset W(S)$. On the other hand, by the second part of the lemma we have that every word in S is an element of $\langle S \rangle$. Thus $W(S) \subset \langle S \rangle$. \square

Theorem 2. *Given to subsets S and T of G we have that $\langle S \rangle \subset \langle T \rangle$ if and only if every element of S can be written as a word in T .*

Proof. Since $\langle T \rangle$ is the set of words in T we have that an element $g \in G$ is in $\langle T \rangle$ if and only if g can be written as a word in T . Hence $S \subset \langle T \rangle$ if and only if every element of S can be written as word in T which happens if and only if $\langle S \rangle \subset \langle T \rangle$. \square

You should think of this lemma as saying that words in S can be rewritten in terms of words in T .

Corollary 2. *Given to subsets S and T of G we have that $\langle S \rangle = \langle T \rangle$ if and only if every element of S can be written as a word in T and every element of T can be rewritten as a word in S .*

Example 2. *Let G be A_n , the alternating group in n letters. We showed that every element of S_n can be written as a product of transpositions of the form $\sigma_i := (i, i+1)$. We also showed that a permutation is in A_n if and only if it can be written as a product of an even number of 2-cycles. Hence we have that products $\sigma_i \sigma_j$ generate A_n .*

In general a proof that uses words is not considered elegant because the proof often comes down to a calculation as opposed to a concept.

Theorem 3. *Let $f : G \rightarrow H$ be a homomorphism between two groups G and H . Then for any subset $S \subset G$ we have that $f(\langle S \rangle) = \langle f(S) \rangle$.*

Proof. Since $\langle S \rangle$ is a group containing S we have that $f(\langle S \rangle)$ is subgroup of H which contains $f(S)$. Hence we have that $f(\langle S \rangle) \subset \langle f(S) \rangle$. On the other hand we have that $f^{-1}(\langle f(S) \rangle)$ is a subgroup of G which contains S (since $f(S) \subset \langle f(S) \rangle$) hence we have that $\langle S \rangle \subset f^{-1}(\langle f(S) \rangle)$ and so $f(\langle S \rangle) \subset f(f^{-1}(\langle f(S) \rangle)) \subset \langle f(S) \rangle$. \square

Or for a more concrete but uglier proof using words

Another Proof. Let $w \in \langle S \rangle$. Then w is a word in S . That is $w = s_1 \cdots s_n$ for some $s_i \in S^\pm$. Hence $f(w) = f(s_1 \cdots s_n) = f(s_1) \cdots f(s_n)$ which implies that $f(w)$ is a word in $f(S)$. Thus $f(w) \in \langle f(S) \rangle$. Hence we have shown that $f(\langle S \rangle) \subset \langle f(S) \rangle$. On the other hand if $w' \in \langle f(S) \rangle$ then w' is a word in $f(S)$. Hence $w' = f(s_1)^{\pm 1} \cdots f(s_n)^{\pm 1} = f(s_1^{\pm 1} \cdots s_n^{\pm 1})$ for some $s_1, \dots, s_n \in S$. But since $s_i \in S^\pm$ we have that $s_1^{\pm 1} \cdots s_n^{\pm 1}$ is a word in S . Thus we have that the element $s_1^{\pm 1} \cdots s_n^{\pm 1} \in \langle S \rangle$ gets mapped to w' under f and this is exactly what the definition of $f(\langle S \rangle)$ is. So $w' \in f(\langle S \rangle)$ and hence $\langle f(S) \rangle \subset f(\langle S \rangle)$. \square

Theorem 4. *Suppose that ϕ, ψ are two homomorphisms from $\langle S \rangle \rightarrow H$ with $\phi(s) = \psi(s)$ for every $s \in S$. Then $\phi = \psi$. (That is homomorphisms are uniquely determined by what they do to a generating set).*

Proof. For a homomorphism ϕ we define $\Lambda(\phi)$ as the set $\{(g, h) \in G \times H : \phi(g) = h\}$ (this is the *graph* of ϕ).

- It uniquely determines the map ϕ in the sense that if we can show that $\Lambda(\phi) = \Lambda(\psi)$ then we would have $\phi = \psi$. This is because $(g, h) \in \Lambda(\phi)$ if and only if $h = \phi(g)$.
- $\iota_\phi : g \mapsto (g, f(g))$ is an isomorphism from G onto $\Lambda(\phi)$. We need to check that ι_ϕ is a homomorphism, that it is one-to-one, and that it is onto. Indeed if $k, h \in G$, then $\iota_\phi(kh) = (kh, \phi(kh)) = (kh, \phi(k)\phi(h)) = (k, \phi(k))(h, \phi(h)) = \iota_\phi(k)\iota_\phi(h)$. It is one to one since $(g, \phi(g)) = \iota_\phi(g) = (1_G, 1_H)$ implies that $g = 1_G$. Finally it is onto since every element of $\Lambda(\phi)$ has the form $(g, \phi(g))$ which equals $\iota_\phi(g)$.
- $\Lambda(\phi)$ is a subgroup of $G \times H$ since it is the image of G under a homomorphism.
- We have for all $s \in S$, $\iota_\phi(s) = (s, \phi(s)) = (s, \psi(s)) = \iota_\psi(s)$.

Thus we have that

$$\Lambda(\phi) = \iota_\phi(G) = \langle \iota_\phi(S) \rangle = \langle \iota_\psi(S) \rangle = \Lambda(\psi).$$

Thus the graph of ϕ equals the graph of ψ and $\phi = \psi$. \square

Ok, even I'll admit this theorem is much easier using words:

Another Proof. Suppose that ϕ is defined on generators. Then ϕ is uniquely determined by $\phi(s_1 \cdots s_n) := \phi(s_1) \cdots \phi(s_n)$. In more detail we have for every $w = s_1 \cdots s_n \in G$

$$\begin{aligned} (1) \quad & \phi(w) = \phi(s_1 \cdots s_n) \\ (2) \quad & = \phi(s_1) \cdots \phi(s_n) \quad (\text{since } \phi \text{ is a homomorphism}) \\ (3) \quad & = \psi(s_1) \cdots \psi(s_n) \quad (\psi|_{S^\pm} = \phi|_{S^\pm}) \\ (4) \quad & = \psi(s_1 \cdots s_n) \quad (\text{since } \psi \text{ is a homomorphism}) \\ (5) \quad & = \psi(w). \quad (\text{since } w = s_1 \cdots s_n) \end{aligned}$$

\square

Now the next logical question is whether or not a given function from S to a group G extends to a homomorphism. In other words suppose we have a function f from S to a group H . Is there a homomorphism $\phi : G \rightarrow H$ so that $\phi(s) = f(s)$ for every $s \in S$. Clearly one cannot hope that such a ϕ always exists since for example if we take the function from $\mathbb{Z}_3 \rightarrow \mathbb{Z}$ given by $f(1 \pmod 3) := 1$ we can not get a homomorphism since if it did we would have

$$\phi(3 \pmod 3) = 3\phi(1 \pmod 3) = 3f(1 \pmod 3) = 3 \cdot 1 = 3 \neq 0.$$

If on the other hand if we had a word that was equal to the identity in G getting mapped to the identity of H via the extension of f , then it is easy to see that ϕ would indeed be a well defined homomorphism. It turns out we have the following (proof omitted since we never defined what a set of relations actually are)

Theorem 5. *Suppose $\langle S, R \rangle$ is a presentation of G . Then a function $f : S \rightarrow H$ extends to a homomorphism of G into H if and only if $f(r) = 1_H$ for every $r \in R$. \square*

Example 3. *A presentation of $D_n = \langle a, b \mid a^n, b^2, abab \rangle$. Suppose that $m \mid n$. Then I claim that the function $f(a) = a$ and $f(b) = b$ extends to a homomorphism from $D_n \rightarrow D_m$. Indeed $f(a^n) = a^n = (a^m)^x = 1_{D_m}$, $f(b^2) = b^2 = 1_{D_m}$, and finally $f(abab) = abab = 1_{D_n}$ so by the theorem we have that f extends to a homomorphism. Also note that f is surjective since the image contains a generating set of D_m (namely a and b).*

Example 4. *In this example we show that the only index 2 subgroup of S_n is A_n . Let H be an index 2 subgroup of S_n . Then H is the kernel of the quotient map $S_n \rightarrow S_n/H \approx \mathbb{Z}_2$. Hence we need only show that there exists a unique surjective map from S_n to \mathbb{Z}_2 which we identify with $\{\pm 1\}$. From the above we need to show that every surjection from $S_n \rightarrow \{\pm 1\}$, which we call ϕ , does the same thing to every two cycle, namely takes it to its sign, -1 . Indeed if ϕ of some two cycle did not equal -1 , we would have that a two cycle was in the kernel of ϕ , which is a proper (since we are assuming ϕ is surjective, in particular non-trivial), normal subgroup of S_n . However in exercise 2d of homework assignment 4 you showed that such a subgroup of S_n did not exist.*

The nice thing about generators is that it makes many calculations much easier since it allows us to simply check the calculation on generators.

Remark 1. *The center of a group by definition is the set of elements that commute with every element of G while the centralizer of an element is the set of elements which commute with that given element. Both are subgroups of G and an element $g \in G$ is in the center if and only if the centralizer of g is equal to G .*

Theorem 6. *Let $H = \langle S \rangle$ and $G = \langle T \rangle$. Then*

- (1) *If G is finite, then H is normal in G if and only if the conjugate of every element S by every element of T not in S is in H . (if G is infinite then you need to try every element of T^{-1} as well)*
- (2) *An element w is in the center of G if and only if w commutes with every element in T .*

Proof. (1) The condition is clearly necessary by definition of normality. We show that it is sufficient. If we can show that $\langle T \rangle \subset N_G(H)$, then we can conclude that $G = N_G(H)$ and hence H is normal in G . Since $S \subset H$ we do not need to check it for elements of T that happen to be in S . Now an element $g \in N_G(H)$ by definition means that the automorphism $c_g : g' \mapsto gg'g^{-1}$ maps H to itself, or written suggestively, $gHg^{-1} \subset H$. However the assumption is that $tSt^{-1} \subset H$ for every element in $T \setminus S$, so we have $tHt^{-1} = t(\langle S \rangle)t^{-1} = \langle tSt^{-1} \rangle \subset \langle S \rangle = H$ as desired.

(2) Again the condition is clearly necessary and we simply show that it is sufficient. To show that an element $g \in G$ is in the center of G means that the centralizer of g has got to equal all of G . But the assumption is that the centralizer of g contains all elements of a generating set of H and this means that it contains G . □

Exercise 1. *Show that we only need to check that $tst^{-1} \in S$ for a single s in every conjugacy class of s which meets S .*

Exercise 2. *Prove Theorem 6 (at least in your head) by using words. Notice how easy it is to prove it to yourself and how ugly it is to write down on paper?*

Example 5. *In Quiz 8 I had you show that $\langle a \rangle$ was a normal subgroup of D_4 . In that quiz you needed to show that $a^n b^\epsilon a^m (a^n b^\epsilon)^{-1}$ was equal to some power of a to get full credit. However using our shortcut above we need only verify that $bab^{-1} \in \langle a \rangle$ which it is since $bab^{-1} = a^{-1}$.*

Example 6. *We show that the group $K_4 := \langle a := (12)(34), b := (13)(24) \rangle$ is a normal subgroup of S_4 . Recall that S_4 is generated by the 2-cycles $x := (12)$, $y := (23)$ and $z := (34)$. Moreover a and b are conjugate (via $yay^{-1} = b$) so by Exercise 1 we need only do the following three calculations: $axa^{-1} = x \in K_4$, $yay^{-1} = b \in K_4$, and $zaz^{-1} = a \in K_4$.*