GENERATING SETS

KEITH CONRAD

1. Introduction

In $\mathbf{R}^n$, every vector can be written as a (unique) linear combination of the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$. A notion weaker than a basis is a spanning set: a set of vectors spans $\mathbf{R}^n$ if their linear combinations fill up the whole space. The difference between a spanning set and a basis is simply that a spanning set may contain more vectors than necessary to span the space. For instance, $\{(1,0),(3,1),(2,1)\}$ is a spanning set for $\mathbf{R}^2$ but is not a basis. Omitting any vector from this spanning set will give a basis of $\mathbf{R}^2$. A basis, then, is a minimal spanning set. All bases of $\mathbf{R}^n$ have the same size, and this size is the dimension n.

In a group, the analogue of a spanning set is called a generating set.

Definition 1.1. In a group G, a subset $X \subset G$ is a *generating set* for G if every $g \in G$ can be written as a product of powers of elements taken from X:

$$g = x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}, \tag{1.1}$$

where $x_i \in X$ and $a_i \in \mathbf{Z}$. We also say that X *generates* G and write $G = \langle X \rangle$. If G has a finite generating set, we say G is a *finitely generated* group.

Instead of using integral exponents in the definition, we could write powers as the same factor repeated, and then X is a generating set for G when every element of G is a product of elements from X and inverses of elements from X. This is closer to what the idea of "generating set" sounds like: through repeated use of the group operations (multiplication and inversion) we can produce all elements of G from X.

Example 1.2. Every permutation in S_n is a product of cycles, so the cycles in S_n are a generating set of S_n. We will meet smaller generating sets for S_n later in this handout.

Example 1.3. The group $\mathbf{Z}/(m) \times \mathbf{Z}/(n)$ is generated by $(1,0)$ and $(0,1)$, since $(\overline{a}, \overline{b}) = a(1,0) + b(0,1)$

Example 1.4. A group has a one-element generating set exactly when it is a cyclic group. For instance, $\mathbf{Z}$ has the one-element generating sets $\{1\}$ and $\{-1\}$.

Example 1.5. The infinite nonabelian matrix group $\left\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a = \pm 1, b \in \mathbf{Z}\right\}$ is finitely generated. Since $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^b \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $a = \pm 1$, this group has generating set $\left\{\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\right\}$.

Example 1.6. The group $\mathbf{Q}$ is not finitely generated: a finite set of rational numbers has a common denominator, say N, and the subgroup of $\mathbf{Q}$ generated by these rational numbers (their integral multiples and sums thereof) will only give rise to rational numbers with denominators dividing N. Not all rationals have such denominators (try $1/(N+1)$), so $\mathbf{Q}$ doesn't have a finite set of generators as an additive group.

Example 1.7. A finitely generated group is at most countable, so an uncountable group is not finitely generated.

The analogue of a vector space basis in the context of groups might be a minimal generating set. That means: a generating set which is no longer a generating set when any of its elements is removed. In contrast to the case of bases for $\mathbf{R}^n$, in non-commutative groups different minimal generating sets need not have the same size.

Example 1.8. Two minimal generating sets for S_4 are $\{(12), (23), (34)\}$ and $\{(12), (1234)\}$. That these sets each generate S_4 is a special case of Theorems 2.3 and 2.6 below.

To see why the first generating set is minimal, note any two transpositions in the first set either have a common fixed point or commute. Each of these properties is preserved under multiplication, and S_4 has neither property, so two permutations in the first set do not form a generating set of S_4. In the second set, removing a permutation leaves just one, which does not generate S_4 since S_4 is not cyclic.

Because minimal generating sets in a non-abelian group need not have a common size, there is not a theory of "bases" for finitely generated groups which permits the same degree of elegance as bases for finite-dimensional vector spaces in linear algebra. In fact, finitely generated groups can fail to satisfy some natural analogues of theorems about finite-dimensional vector spaces:

- a subgroup of a finitely generated group need not be finitely generated, (!)
- even if a subgroup of a finitely generated group is finitely generated, it might require more generators than the original group. (!)

This kind of apparent pathology is an effect of noncommutativity. In a finitely generated *abelian* group, no such weirdness happens.

Remark 1.9. Here's another point to watch out for when commutativity is missing. If $G = \langle x, y\rangle$ has a 2-element generating set and is abelian, then every element of G has the form $x^m y^n$ for some m and n in $\mathbf{Z}$. But if G is nonabelian, elements of G usually *can't* be written in such a condensed form, *e.g.*, $yxyx^2$ can't be written as x^3y^2.

In this handout, we look at generating sets of symmetric groups, alternating groups, and $\mathrm{SL}_2(\mathbf{Z})$. In the appendix we briefly discuss groups of prime-power order. The following table summarizes some the generating sets we will obtain for various groups, and indicates where the proofs are found.

Group	Generating Set	Size	Where
S_n, $n \geq 2$	(ij)'s	$\frac{n(n-1)}{2}$	Theorem 2.1
	$(12), (13), \ldots, (1n)$	$n-1$	Theorem 2.2
	$(12), (23), \ldots, (n-1\ n)$	$n-1$	Theorem 2.3
	$(12), (12\ldots n)$ if $n \geq 3$	2	Theorem 2.6
	$(12), (23\ldots n)$ if $n \geq 3$	2	Corollary 2.7
	$(ab), (12\ldots n)$ if $(b-a, n) = 1$	2	Theorem 2.10
A_n, $n \geq 3$	3-cycles	$\frac{n(n-1)(n-2)}{3}$	Lemma 3.1
	$(1ij)$'s	$(n-1)(n-2)$	Theorem 3.2
	$(12i)$'s	$n-2$	Theorem 3.3
	$(i\ i+1\ i+2)$'s	$n-2$	Theorem 3.4
	$(123), (12\ldots n)$ if $n \geq 4$ odd	2	Theorem 3.5
	$(123), (23\ldots n)$ if $n \geq 4$ even	2	Theorem 3.5
$\mathrm{SL}_2(\mathbf{Z})$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2	Theorem 4.1

2. Generators for S_n

The group S_n is generated by its cycles. The following theorem shows the 2-cycles (the transpositions) are enough to generate S_n.

Theorem 2.1. *For $n \geq 2$, S_n is generated by its transpositions.*

Proof. This is clear for $n = 1$ and 2. For $n \geq 3$, we note $(1) = (12)^2$ and every cycle of length > 2 is a product of transpositions:

$$(i_1 i_2 \ldots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2)$$

(Another product which works is $(i_{k-1} i_k) \cdots (i_2 i_k)(i_1 i_k)$.) Since the cycles generate S_n, and products of transpositions give us all cycles, the transpositions generate S_n. □

Since transpositions have order 2 (though *not* every element of order 2 is a transposition, *e.g.*, $(12)(34)$ in S_4), Theorem 2.1 tells us S_n is generated by certain elements of order 2.

The total number of transpositions in S_n is $\binom{n}{2} = \frac{n(n-1)}{2}$, so Theorem 2.1 provides us with a generating set of $\approx n^2/2$ transpositions. The next theorem shows we can get a generating set for S_n containing just $n-1$ transpositions.

Theorem 2.2. *For $n \geq 2$, S_n is generated by the $n-1$ transpositions*

$$(12), (13), \ldots, (1n).$$

Proof. The theorem is obvious for $n = 2$, so we take $n \geq 3$.

By Theorem 2.1, it suffices to write any transposition in S_n as a product of the transpositions involving a 1. For a transposition (ij) where i and j are not 1, check that

$$(ij) = (1i)(1j)(1i). \tag{2.1}$$

□

Here is a different generating set of $n-1$ transpositions.

Theorem 2.3. *For $n \geq 2$, S_n is generated by the $n-1$ transpositions*

$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$

Proof. By Theorem 2.1, it suffices to show any transposition in S_n is a product of transpositions of the form $(i\ i+1)$.

The transpositions in our putative generating set are those which permute a pair of consecutive integers: (ij) where $j - i = 1$. Any transposition has the form (ab) where, without loss of generality, $a < b$. We will argue by induction on $b - a \geq 1$ that (ab) is a product of the transpositions $(i\ i+1)$. This is obvious when $b - a = 1$, since (ab) then is one of the transpositions in our set. Now suppose $b - a = k > 1$ and the theorem is settled for all transpositions which permute a pair of integers with difference less than k.

Consider the formula

$$(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1).$$

The first and third transpositions on the right side lie in our set. The middle transposition permutes a pair of integers with difference $b - (a+1) = k - 1 < k$. By induction, $(a+1\ b)$ is a product of transpositions in our set, so $(a\ b)$ is as well and we are done. □

Remark 2.4. The generating sets in Theorems 2.2 and 2.3 are both minimal. Why? Well, removing a transposition $(1i)$ from the generating set in Theorem 2.2 will leave a set of transpositions with a common fixed point (and thus they can't generate all of S_n). To explain why the generating set in Theorem 2.3 is minimal is a bit more subtle. It we take out (12) or $(n-1\ n)$, then at most we will be able to generate permutations having a common fixed point (1 or n), and thus we do not get all of S_n. If we take out $(i\ i+1)$ for some i from 2 to $n-1$, then we are left with

$$(12), (23), \ldots, (i-1\ i), (i+1\ i+2), \ldots, (n-1\ n).$$

Convince yourself that these transpositions can never produce the transposition that swaps 1 and n. The "bridge" linking 1 to n through the generating set has been broken when $(i\ i+1)$ is taken out.

Now we are ready to cut down the size of a generating set for S_n to *two*.

Lemma 2.5. *For a cycle $(i_1 i_2 \ldots i_r)$ in S_n and any $\sigma \in S_n$,*

$$\sigma(i_1 i_2 \ldots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_r)).$$

Proof. Check both sides have the same (cyclic) effect on $\sigma(i_1), \ldots, \sigma(i_r)$, and neither side moves an integer other than the $\sigma(i_j)$'s. □

Theorem 2.6. *For $n \geq 2$, S_n is generated by the transposition (12) and the n-cycle $(12\ldots n)$.*

Proof. By Theorem 2.3, it suffices to show products of the permutations (12) and $(12\ldots n)$ yield all transpositions of the form $(i\ i+1)$. We may take $n \geq 3$.

Set $\sigma = (12\ldots n)$. Then

$$\sigma(12)\sigma^{-1} = (\sigma(1)\ \sigma(2)) = (23),$$

and more generally for $k = 1, 2, \ldots, n-2$,

$$\sigma^k(12)\sigma^{-k} = (\sigma^k(1)\ \sigma^k(2)) = (k+1\ k+2).$$

□

Corollary 2.7. *For $n \geq 3$, S_n is generated by (12) and the $(n-1)$-cycle $(23\ldots n)$.*

Proof. This is immediate from Theorem 2.6 since $(12\ldots n) = (12)(23\ldots n)$. □

Remark 2.8. Your prior experience with bases in linear algebra might suggest that the 2-element generating sets for S_n, being as small as possible (for $n \geq 3$), should be the most useful generating sets. In fact, the generating set of transpositions $(i\ i+1)$ in Theorem 2.3 turns out to be the most important one.

We've found a pair of generators for S_n of orders 2 and n, and then of orders 2 and $n-1$. How small can the orders of a pair of generators of S_n be?

Theorem 2.9. *For $n \geq 3$ except for $n = 5, 6, 8$, S_n is generated by an element of order 2 and an element of order 3.*

We omit the proof of this theorem. It was first proved by G. A. Miller [2] in 1901, and his proof relied on a choice of a prime between n and $n/2$, so it was not explicit in terms of n. An explicit set of generators of order 2 and 3 was given by Dey and Wiegold [1] in 1971, unaware of Miller's earlier work. As an example, S_9 is generated by

$$(14)(28)(59) \text{ and } (123)(456)(789).$$

While S_n is generated by the *particular* transposition (12) and n-cycle $(12\dots n)$, it is usually not true that S_n is generated by an *arbitrary* transposition and n-cycle. For instance, (13) and (1234) do not generate S_4. The reason is that these two permutations preserve congruences mod 2 (if two numbers in $1, 2, 3, 4$ are both even or both odd, applying either permutation to them returns values that are both even or both odd), so the subgroup they generate in S_4 has this property while S_4 does not have this property.

Theorem 2.10. *For $1 \leq a < b \leq n$, the transposition (ab) and n-cycle $(12\dots n)$ generate S_n if and only if $(b-a, n) = 1$.*

Here the transposition (ab) is general, but the n-cycle is the standard one.

Proof. Let $d = (b-a, n)$. We will show every $g \in \langle (ab), (12\dots n)\rangle$ preserves mod d congruences among $\{1, 2, \dots, n\}$:

$$i \equiv j \bmod d \Longrightarrow g(i) \equiv g(j) \bmod d. \tag{2.2}$$

It suffices to check this when $g = (ab)$ and when $g = (12\dots n)$. For $i \neq a$ or b, $(ab)(i) = i$. Also $(ab)(a) = b \equiv a \bmod d$ and $(ab)(b) = a \equiv b \bmod d$, so $(ab)(i) \equiv i \bmod d$ for all i. Thus (2.2) holds for $g = (ab)$. As for $g = (12\dots n)$, $(12\dots n)(i) = i+1$, so from

$$i \equiv j \bmod d \Longrightarrow i+1 \equiv j+1 \bmod d$$

we see (2.2) holds for $g = (12\dots n)$.

For $d > 1$, the group S_n does not preserve mod d congruences: pick $i \not\equiv j \bmod d$ and consider the transposition (ij). So if $\langle (ab), (12\dots n)\rangle = S_n$ then we must have $d = 1$.

Now we prove the converse direction: if $(b-a, n) = 1$ then $\langle (ab), (12\dots n)\rangle = S_n$. Let $\sigma = (12\dots n)$, so $\sigma^i(a) = a + i$. So $\sigma^{b-a}(a) = b$. Since $(b-a, n) = 1$, $\langle \sigma\rangle = \langle \sigma^{b-a}\rangle$ and σ^{b-a} is an n-cycle sending a to b, so $\sigma^{b-a} = (ab\dots)$ where the dots are other numbers in the range $\{1, 2\dots, n\}$. Then

$$\langle (ab), \sigma\rangle = \langle (ab), \sigma^{b-a}\rangle = \langle (ab), (ab\dots)\rangle.$$

A suitable relabeling of the numbers $1, 2\dots, n$ (that is, making an overall conjugation on S_n) turns (ab) into (12) and $(ab\dots)$ into $(12\dots n)$, so $\langle (ab), \sigma\rangle$ is conjugate to $\langle (12), (12\dots n)\rangle$, which is S_n by Theorem 2.6. Therefore $\langle (ab), \sigma\rangle = S_n$. □

Corollary 2.11. *For any transposition $\tau = (ab)$ and n-cycle σ in S_n, $\langle \tau, \sigma \rangle = S_n$ if and only if $(k, n) = 1$, where $\sigma^k(a) = b$.*

Proof. Exercise. □

Corollary 2.12. *For a prime number p, S_p is generated by any transposition and any p-cycle.*

Proof. Any p-cycle can be written as $(12 \dots p)$ by relabeling the objects being permuted (that means by applying an overall conjugation on S_p), so to show any transposition and any p-cycle generate S_p it suffices to show any transposition and the standard p-cycle $(12 \dots p)$ generate S_p. For any transposition (ab) where $1 \leq a < b \leq p$, $(b - a, p) = 1$, so $\langle (ab), (12 \dots p) \rangle = S_p$ by Theorem 2.10. □

3. Generators for A_n

We now look for generating sets of A_n, where $n \geq 3$. (For $n = 1$ and 2, A_n is trivial.) Our development will parallel in large part what we did for S_n. In particular, we will see that A_n can be generated by two permutations.

Within S_n, every element of A_n is a product of transpositions, but the transpositions themselves do *not* lie in A_n. The smallest cycles in A_n (excluding the trivial 1-cycle) are the 3-cycles. Do these generate A_n? Yes.

Lemma 3.1. *For $n \geq 3$, any element of A_n is a product of 3-cycles. Therefore the 3-cycles generate A_n.*

Proof. The identity is $(123)^3$, a product of 3-cycles. Now pick a non-trivial element of A_n, say σ. Write it as a product of transpositions in S_n:

$$\sigma = \tau_1 \tau_2 \cdots \tau_r.$$

The number of terms, r, is even. Without loss of generality, adjacent τ's are not equal.

If the transpositions τ_i and τ_{i+1} have one element in common, then

$$\tau_i \tau_{i+1} = (ab)(ac) = (acb)$$

is a 3-cycle. If τ_i and τ_{i+1} are disjoint, then $n \geq 4$ and

$$\tau_i \tau_{i+1} = (ab)(cd) = (ab)(bc)(bc)(cd) = (bca)(cdb) = (abc)(bcd)$$

is a product of two 3-cycles. □

Let's reduce the number of 3-cycles needed.

Theorem 3.2. *For $n \geq 3$, the group A_n is generated by 3-cycles of the form $(1ij)$.*

Proof. For any 3-cycle (abc) not containing a 1, we have $(abc) = (1ab)(1bc)$. Now use Lemma 3.1. □

Theorem 3.2 is an analogue for alternating groups (on at least 3 letters) of Theorem 2.2 for symmetric groups (on at least 2 letters): each theorem says there is a generating set of cycles which contain 1 and have the smallest length consistent with the parity allowed in the group. The 3-cycles containing a 1 leave two undetermined terms, so our generating set for A_n in Theorem 3.2 is quite a bit larger than the generating set for S_n in Theorem 2.2. Here is a sharper analogue of Theorem 2.2 for A_n, where we only allow one undetermined entry in the 3-cycles.

Theorem 3.3. *For $n \geq 3$, the group A_n is generated by 3-cycles of the form $(12i)$.*

Proof. For $n = 3$, the only such 3-cycle is (123), and we know $A_3 = \{(1), (123), (132)\}$ is generated by (123). We now take $n \geq 4$.

Since $(12i)^{-1} = (1i2)$, any 3-cycle in A_n containing 1 and 2 is generated by the 3-cycles of the form $(12i)$. For a 3-cycle containing 1 but not 2, say $(1ij)$, check

$$(1ij) = (12j)(12j)(12i)(12j).$$

By Theorem 3.2, we're done. □

We can describe Theorem 3.3 in a "coordinate-free" manner as follows: A_n is generated by the 3-cycles moving a common pair of terms.

Here is an A_n-analogue of Theorem 2.3.

Theorem 3.4. *For $n \geq 3$, the consecutive 3-cycles $(i\ i+1\ i+2)$, with $1 \leq i \leq n-2$, generate A_n.*

Proof. This is true for $n = 3$ since $A_3 = \{(1), (123), (132)\}$ is cyclic with generator (123).

We know by Theorem 3.3 that A_4 is generated by (123) and (124). Since

$$(124) = (123)(123)(234)(123), \tag{3.1}$$

we see (123) and (234) also generate A_4.

Now take $n \geq 5$. Theorem 3.3 says a generating set for A_n is the set of 3-cycles $(12i)$. We argue by induction on i that these particular 3-cycles can be produced from products of consecutive 3-cycles. This is obvious for $i = 3$, and is shown in (3.1) for $i = 4$. For $i \geq 5$, assume $(12j)$ is a product of consecutive 3-cycles for $3 \leq j < i$. Then the equation

$$(1\ 2\ i) = (1\ 2\ i-2)(1\ 2\ i-1)(i-2\ i-1\ i)(1\ 2\ i-2)(1\ 2\ i-1)$$

and the inductive hypothesis show $(12i)$ can be written as a product of consecutive 3-cycles. □

Here is an analogue of Theorem 2.6.

Theorem 3.5. *For $n \geq 4$, A_n is generated by two elements:*

$$(123) \text{ and } \begin{cases} (12\dots n), & \text{if } n \text{ is odd,} \\ (23\dots n), & \text{if } n \text{ is even.} \end{cases}$$

The theorem is true in a redundant sense when $n = 3$.

Proof. It suffices, by Theorem 3.4, to obtain the 3-cycles $(i\ i{+}1\ i{+}2)$ from the two indicated permutations.

First suppose n is odd. Let $\sigma = (12\dots n)$, so $\sigma \in A_n$. Then, for $1 \leq k \leq n-3$.

$$\sigma^k(123)\sigma^{-k} = (\sigma^k(1)\sigma^k(2)\sigma^k(3)) = (k+1\ k+2\ k+3).$$

Now suppose n is even. Let $\sigma = (23\dots n)$, so $\sigma \in A_n$. Then, for $1 \leq k \leq n-3$,

$$\sigma^k(123)\sigma^{-k} = (\sigma^k(1)\sigma^k(2)\sigma^k(3)) = (1\ k+2\ k+3).$$

This does not give us the consecutive 3-cycles right away, but we can obtain them from what we now have, since

$$(k\ k+1\ k+2) = (1\ k\ k+1)(1\ k+1\ k+2).$$

□

There is an analogue of Theorem 2.9 for alternating groups, with a slightly different set of exceptions.

Theorem 3.6. *For $n \geq 3$ except for $n = 6, 7, 8$, A_n is generated by an element of order 2 and an element of order 3.*

We omit the proof. As an example, A_9 is generated by

$$(14)(29)(37)(56) \text{ and } (123)(456)(789).$$

4. $\mathrm{SL}_2(\mathbf{Z})$

The group $\mathrm{SL}_2(\mathbf{Z})$ consists of 2×2 integer matrices with determinant 1 (under multiplication). For instance, $\left(\begin{smallmatrix} 26 & 7 \\ 11 & 3 \end{smallmatrix}\right)$ is in $\mathrm{SL}_2(\mathbf{Z})$. There are two important matrices in this group:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

It is left to the reader to check that $S^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $S^4 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so S has order 4, while $T^k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ for any $k \in \mathbf{Z}$, so T has infinite order.

Theorem 4.1. *The group $\mathrm{SL}_2(\mathbf{Z})$ is generated by S and T.*

Proof. As the proof will reveal, this theorem is essentially the Euclidean algorithm in disguise. If the reader finds the proof hard to follow, consult the example following the proof and then re-read the proof.

First we check how S and a power of T change the entries in a matrix. Verify that

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix},$$

and

$$T^k\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + ck & b + dk \\ c & d \end{pmatrix}.$$

Thus, up to a sign change, multiplying by S on the left interchanges the rows. Multiplying by a power of T on the left adds a multiple of the second row to the first row and does not change the second row. Given a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$, we can carry out the Euclidean algorithm on a and c by using left multiplication by S and powers of T. We use the power of T to carry out the division (if $a = cq + r$, use $k = -q$) and use S to interchange the roles of a and c to guarantee that the larger of the two numbers (in absolute value) is in the upper-left corner. Multiplication by S will cause a sign change in the upper row, but this has no serious effect on the algorithm.

Since $ad - bc = 1$, a and c are relatively prime, so the last step of Euclid's algorithm will have a remainder of 1. This means, after suitable multiplication by S's and T's, we will have transformed the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ into one with first column $\binom{\pm 1}{0}$ or $\binom{0}{\pm 1}$. Left-multiplying by S interchanges the rows up to a sign, so we can suppose the first column is $\binom{\pm 1}{0}$. Any matrix of the form $\left(\begin{smallmatrix} 1 & x \\ 0 & y \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$ must have $y = 1$ (the determinant is 1), and then it is $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) = T^x$. A matrix $\left(\begin{smallmatrix} -1 & x \\ 0 & y \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{Z})$ must have $y = -1$, so the matrix is $\left(\begin{smallmatrix} -1 & x \\ 0 & -1 \end{smallmatrix}\right) = -T^{-x} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)T^x$. Since $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = S^2$, we can finally unwind and express our original matrix in terms of S's and T's. □

Example 4.2. Take $A = \left(\begin{smallmatrix} 26 & 7 \\ 11 & 3 \end{smallmatrix}\right)$. Since $26 = 11 \cdot 2 + 4$, we want to subtract $11 \cdot 2$ from 26:

$$T^{-2}A = \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}.$$

Now we want to switch the roles of 4 and 11. Multiply by S:

$$ST^{-2}A = \begin{pmatrix} -11 & -3 \\ 4 & 1 \end{pmatrix}.$$

Dividing -11 by 4, we have $-11 = 4 \cdot (-3) + 1$, so we want to add $4 \cdot 3$ to -11. Multiply by T^3:

$$T^3ST^{-2}A = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Once again, multiply by S to switch the entries of the first column (up to sign):

$$ST^3ST^{-2}A = \begin{pmatrix} -4 & -1 \\ 1 & 0 \end{pmatrix}.$$

Our final division is: $-4 = 1(-4) + 0$. We want to add 4 to -4, so multiply by T^4:

$$T^4ST^3ST^{-2}A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S.$$

Thus, left-multiplying by the inverses of all the S's and T's on the left side, we obtain

$$A = T^2S^{-1}T^{-3}S^{-1}T^{-4}S.$$

Since S has order 4, we can write S^{-1} as S^3 if we wish to use a positive exponent on S. However, a similar idea does not apply to the negative powers of T.

In this example, we wrote a matrix in terms of S and T, but not in the condensed form S^aT^b or T^bS^a. It is generally *not* possible to write elements of $\mathrm{SL}_2(\mathbf{Z})$ in either of those ways, because a matrix S^aT^b or T^bS^a has a 0 in one of its entries (Since S has order 4, this can be checked by writing $T^b = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ and then computing $S^a\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)S^a$ for $a = 0, 1, 2, 3$.)

Since $\mathrm{SL}_2(\mathbf{Z}) = \langle S, T\rangle$, we can also say $\mathrm{SL}_2(\mathbf{Z}) = \langle S, ST\rangle$. This is interesting because S has order 4 and $ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ has order 6. In other words, $\mathrm{SL}_2(\mathbf{Z})$ is an infinite group which can be generated by two elements of finite order. Moreover, in the quotient group[1] $\mathrm{PSL}_2(\mathbf{Z}) := \mathrm{SL}_2(\mathbf{Z})/\{\pm I_2\} = \langle \overline{S}, \overline{ST}\rangle$, $\overline{S}$ has order 2 and $\overline{ST}$ has order 3. This quotient group is "universal" for the property of being generated by elements of order dividing 2 and 3: if $G = \langle x, y\rangle$ is any group generated by elements x and y where $x^2 = e$ and $y^3 = e$, there is a unique group homomorphism $\mathrm{PSL}_2(\mathbf{Z}) \to G$ sending $\overline{S}$ to x and $\overline{ST}$ to y, so G is isomorphic to a quotient group of $\mathrm{PSL}_2(\mathbf{Z})$. For example, A_n and S_n are generated by elements of order 2 and 3 when $n \geq 9$, so all these groups are quotient groups of the single group $\mathrm{PSL}_2(\mathbf{Z})$.

[1]The group $\{\pm I_2\}$ is the center of $\mathrm{SL}_2(\mathbf{Z})$.

Appendix A. Groups of prime-power order

For a finite group G, let $d(G)$ denote the smallest possible size of a generating set for G. (With analogies to linear algebra in mind, we might naively think of $d(G)$ as a "dimension," hence the notation.) For instance, $d(G) = 1$ precisely when G is a cyclic group. Theorems 2.6 and 3.5 tell us $d(S_n)$ and $d(A_n)$ equal 2 when these groups are non-abelian (that is, except for very small n). Consider the following questions about $d(G)$ for a general finite group G, motivated by an analogy with bases in vector spaces:

- Do all minimal generating sets for G have $d(G)$ terms?
- Let X be any generating set for G. Is there a generating set of $d(G)$ elements inside of X?
- If $H \subset G$ is a subgroup, is $d(H) \leq d(G)$?

The answer to all three questions, in the context of all finite groups, is *no*. Indeed, the symmetric groups S_n for $n \geq 4$ answer the first two questions in the negative by Remark 2.4, using the minimal generating set in Theorem 2.2 or 2.3. The symmetric groups also provide examples which negate the third question, as follows. Let H be the subgroup of S_n generated by the transpositions $(12), (34), \ldots, (2j-1\ 2j), \ldots$. While $d(S_n) = 2$, it can be shown that $d(H) = [n/2]$. In particular, $d(H) > d(S_n)$ for $n \geq 6$.

Despite this bad news, something remarkable happens if we restrict our attention to finite groups G of prime-power order. The answers to all three questions become *yes*: all minimal generating sets of G have the same size, any generating set of G contains a generating set with that minimal size, and the size of a minimal generating set drops when passing to subgroups. The main result in this direction is called the Burnside Basis Theorem. You can find a discussion of this theorem in any advanced text on group theory.

References

[1] I. M. S. Dey and J. Wiegold, "Generators for alternating and symmetric groups," *J. Australian Math. Soc.* **12** (1971), 63–68.

[2] G. A. Miller, "On the groups generated by 2 operators," *Bull. Amer. Math. Soc.* **7** (1901), 14–32.