Section 4: Powers of an Element; Cyclic Groups

For elements of a semigroup $(S, *)$, the definition of positive integer exponents is clear: For x in S and n in $\mathbb{Z}^+$, $x^n = x * x * \cdots * x$, where there are n "factors", i.e., $n\ x's$ "starred together" — this n-fold "star" is meaningful because associativity says that, no matter how parentheses are put in to divide it into $n-1$ 2-fold "stars", the result will always be the same. In particular, $x^1 = x$. If the semigroup has a (two-sided) identity e, then you can probably guess what an exponent of 0 means: $x^0 = e$. If S is really a group, i.e., every element also has an inverse, then we can make sense of negative exponents; in fact, there are technically two reasonable definitions for x^{-n} when $n \in \mathbb{Z}^+$: Is it the inverse of x^n, or the n-th power of x^{-1} — is x^{-n} equal to $(x^n)^{-1}$ or is it $(x^{-1})^n$?. Fortunately, these two results turn out to be equal [the text leaves this as an exercise for the student, and so will I].

Warnings: Fractional exponents are usually meaningless in the context of groups. Also, one of the familiar rules of exponents does not hold, unless the group is abelian: If we start with $(x*y)^2 = x^2 * y^2$ (for elements x, y of some group), i.e., $x*y*x*y = x*x*y*y$, then cancellation shows that $y*x = x*y$. So for a general, not-necessarily-abelian group we can only hope to prove the other two rules of exponents:

Prop: If $(G, *)$ is a group, them for all x in G and m, n in $\mathbb{Z}$, we have $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn} = (x^n)^m$. If G is abelian, then for any x, y in G and n in $\mathbb{Z}$, we have $(x*y)^n = x^n * y^n$.

Pf: For $x^m * x^n = x^{m+n}$, suppose first that m, n are both positive. Then $x^m * x^n = (x*x*\cdots*x)*(x*x*\cdots*x)$ where the first set of parentheses has m x's and the second has n of them, so the result is "starring together" a total of $m+n$ x's, i.e., x^{m+n}. Suppose one of them is 0, say $m = 0$; then the equation to be proved is $x^0 * x^n = x0 + n$, but because $x^0 = e$ and $0 + n = n$ (no matter whether n is positive, 0 or negative), both sides are x^n and the result follows. The text does the case where both m, n are negative and where $m < 0$ and $n > 0$, so let's do the case where $m > 0$ and $n < 0$; so that $k = -n$ is a positive integer. Then $x^m * x^n = x^m * x^{-k} = x^m * (x^{-1})^k$, the value of which depends or the relative values of k, m, telescoping the "stars" $x * x^{-1}$ in the middle of the product:

if $k < m$, then $x^m * (x^{-1})^k = x^{m-k} = x^{m+n}$;
if $k = m$, then $x^m * (x^{-1})^k = e = x^0 = x^{m-k} = x^{m+n}$; and
if $k > m$, then $x^m * (x^{-1})^k = (x^{-1})^{k-m} = x^{-(k-m)} = x^{m+n}$.

Thus, in all cases, $x^m * x^n = x^{m+n}$.

The proof that $(x^m)^n = x^{mn}$ is also an exercise for the student. (It is not necessary to break up in cases for m, only for n.) Because multiplication of integers is commutative, the equality $x^{mn} = (x^n)^m$ follows from the other one.

Finally, suppose G is abelian, $x, y \in G$ and $n \in \mathbb{Z}$. Suppose first that n is positive. Then $(x*y)^n = x*y*x*y*\cdots*x*y$ is a "star" of n x's and n y's, and with the commutative property we can rearrange to put all the x's first and all the y's last, so that it becomes $x^n * y^n$. If $n = 0$, then $(x*y)^n = e$ and $x^n * y^n = e*e = e$, so they are equal. Finally, if n is negative, say $n = -k$, then $x^k * y^k = (x*y)^k$ so $e = x^{-k} * (x*y)^k * y^{-k} = x^{-k} * y^{-k} * (x*y)^k$, so $(x*y)^{-k} = x^{-k} * y^{-k}$, i.e., also in this case, $(x*y)^n = x^n * y^n$.//

Notation: From now on, a general operation will be denoted, not by $*$, but by juxtaposition, writing xy instead of $x*y$. Occasionally, if the operation is commutative, we will denote it by $+$; in this case the inverse of x is denoted by $-x$, and "powers" become multiples: $x + x + \cdots + x$ (with n terms) is denoted nx. So the rules of exponents become $(m+n)x = mx + nx$, $m(nx) =$

$(mn)x = n(mx)$, and because we are assuming commutativity, $n(x+y) = nx + ny$.

In our basic examples of operations, addition and multiplication in $\mathbb{R}$, most of the multiples nx and powers x^n (except for the identities, 0 and 1 respectively) get larger and larger as the n gets larger and larger. The counterexample is powers of -1, which alternate between 1 and -1. But in other groups, the powers (multiples) of elements can cycle through any number of other elements before repeating. For example, in $(\mathbb{Z}_5, \oplus)$, the multiples of 1 are

$$\begin{aligned} 1 \\ 1+1 &= 2 \\ 1+1+1 &= 3 \\ 1+1+1+1 &= 4 \\ 1+1+1+1+1 &= 0 \\ 1+1+1+1+1+1 &= 1 \\ 1+1+1+1+1+1+1 &= 2 \\ \text{etc.} \end{aligned}$$

Similarly, the powers of i in $(\mathbb{C} - \{0\}, \cdot)$ are

$$i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1,\ i^5 = i,\ i^6 = -1,\ \text{etc.}$$

Terminology: Let S be a subset of a group G. We say that S is *closed under the operation* on G if, for all x, y in S, xy is also in S, i.e., the restriction of the operation on G to S is an operation on S. And S is *closed under inverses* if, for all x in S, x^{-1} is also in S. If a nonempty subset S of G is closed under the operation and inverses, then S is a group in its own right, called a *subgroup* of G. We'll study more general subgroups later, but for this section we are interested in a specific kind of subgroup:

Def and Prop: Let x be an element of a group G. The set $\langle x \rangle$ of all powers of x is closed under the operation on G and under inverses, so it is a subgroup of G, called the *cyclic subgroup* generated by x.

(i) If there is no positive integer n for which $x^n = e$, then we say x has *infinite order;* in symbols, $o(x) = \infty$. In this case the function $\varphi : \mathbb{Z} \to G : n \mapsto x^n$ is a one-to-one function with range $\langle x \rangle$, and it shows that, as a group, $\langle x \rangle$ behaves just like $\mathbb{Z}$.

(ii) If there is a positive integer n for which $x^n = e$, then the smallest such n is called the *order* of x, denoted $o(x)$. In this case, for $o(x) = n$, the function $\psi : \mathbb{Z}_n \to G : k \mapsto x^k$ is a one-to-one function with range $\langle x \rangle$, and it shows that, as a group, $\langle x \rangle$ behaves just like $\mathbb{Z}_n$.

Pf of whatever isn't a definition in this statement: The subset $\langle x \rangle$ is closed under the operation because $x^m x^n = x^{m+n}$; it is closed under inverses because $(x^n)^{-1} = x^{-n}$. So it is a subgroup of G. In the case where there is no positive power of x that is equal to e, it is clear that φ has range $\langle x \rangle$. to see it is one-to-one, suppose $x^m = x^n$ where $m \geq n$; then $x^{m-n} = e$, so we must have $m - n = 0$, i.e., $m = n$. In the case where $o(x) = n < \infty$, we want to show first that ψ has range all of $\langle x \rangle$, i.e., every power of x is equal to x^r for some r between 0 and $n-1$ (inclusive): Given the power x^m, long-divide m by n: $m = qn + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$; then $x^m = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r$.

And to see that ψ is one-to-one, suppose $x^r = x^s$ where $0 \le r \le s < n$; then $x^{s-r} = e$, but $0 \le s - r < n$ and the choice of n means $s - r = 0$, i.e., $r = s$. "Behaves just like" means that adding in $\mathbb{Z}$ or $\mathbb{Z}_n$ corresponds to multiplying in G: In the case of infinite order, we have $\varphi(n+m) = x^{n+m} = x^n x^m = \varphi(n)\varphi(m)$, so the operations in the groups $\langle x \rangle$ and $\mathbb{Z}$ are essentially identical. And in the case of order n, let s, t be elements of $\mathbb{Z}_n$ and long-divide the integer $s + t$ by n: $s+t = nq+r$. Then $s \oplus t = r$, and $\psi(s)\psi(t) = x^s x^t = x^{s+t} = x^n q + r = (x^n)^q x^r = x^r = \psi(s \oplus t)$. So the operations in the groups $\langle x \rangle$ and $\mathbb{Z}_n$ are essentially identical.//

Here is a diagram of what "the operations are essentially identical" means in the infinite-order case:

$$
\begin{array}{ccccc}
\mathbb{Z} & \times & \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\
\downarrow \varphi & & \downarrow \varphi & & \downarrow \varphi \\
G & \times & G & \xrightarrow{\text{op}} & G
\end{array}
$$

If we start with any pair of integers in the upper left, going across and then going down gives the same result as going down (side-by-side) and then going across.

Ex: In the group $GL(3, \mathbb{R})$, let

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} .$$

Then

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} , \qquad A^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I$$

so $\langle A \rangle = \{A, A^2, I\}$ behaves just like $\mathbb{Z}_3$:

$$\varphi : \mathbb{Z}_3 \to \langle A \rangle : \qquad 0 \mapsto I , \qquad 1 \mapsto A , \qquad 2 \mapsto A^2$$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

	I	A	A^2
I	I	A	A^2
A	A	A^2	I
A^2	A^2	I	A

If $x^n = e$, then $(x^{-1})^n = (x^n)^{-1} = e^{-1} = e$, and vice versa, so $o(x)$, the smallest n for which $x^n = e$, is the same as $o(x^{-1})$, and if one is infinite, so is the other. We can say more when we are talking about finite orders, but the proofs suddenly involve a lot of Math 250 results. Before we give the proof, let's take an example, looking at the orders of the elements of $\mathbb{Z}_{12}$:

- 0 has order 1 — the identity in any group is the only element of order 1.
- 1 has order 12: we need to add 12 copies of 1 to get 0.
- 2 has order 6: $2(2) = 4$, $3(2) = 6$, $4(2) = 8$, $5(2) = 10$, $6(2) = 0$.
- The idea that works for 2 also works for the other divisors of 12: 3 has order 4, 4 has order 3, 6 has order 2.
- How many copies of 5 will we need to add to get 0? I.e., in $\mathbb{Z}$, how many 5's will we need to add to get a multiple of 12? Well, because 5 has no factor in common with 12, we only get $n(5) = m(12)$ if n is divisible by 12; so 5 has order 12. The same is true of the other numbers less than 12 and relatively prime to it: 7 and 11.

- $1(8) = 8$, $2(8) = 4$, $3(8) = 0$; i.e., in $\mathbb{Z}$, a multiple of 8, $n(8)$, is a multiple of 12 only if n makes up the factor 3 of 12 that is not in 8. In the equation $n(8) = m(12)$, divide both sides by the gcd of 12 and 8: $n(2) = m(3)$; because 3 is relatively prime to 2, it must divide n. So $o(8) = 3 = 12/4 = 12/\gcd(12, 8)$.

- And the same idea works for 9 and 10: In $\mathbb{Z}$, $1(9) = 9$, $2(9) = 18$, $3(9) = 27$, $4(9) = 36$, a multiple of 12: $o(9) = 4 = 12/3 = 12/\gcd(12, 9)$; and $6(10) = 60$ is the smallest common multiple of 10 and 12: $o(10) = 6 = 12/2 = 12/\gcd(12, 10)$.

So the idea seems to be that, in $\mathbb{Z}_n$, the order of an element k is $n/\gcd(n, k)$. If this is right, it should translate to any cyclic group $\langle x\rangle$ where $o(x) = n$.

We need two things from Math 250, i.e., from arithmetic in $\mathbb{Z}$: the idea of long division, and the fact that, if a divides a product bc and $\gcd(a, b) = 1$, then $a|c$. The text proves these in great detail, but because they are now done in Math 250, I will assume we know them.

Prop: Suppose the group element x has finite order n. Then:

(i) For any integer m, $x^m = e$ if and only if $n|m$; and

(ii) For any integer k, $o(x^k) = n/\gcd(n, k)$.

Pf: (i) Of course if $n|m$, say $m = nd$, then $x^m = (x^n)^d = e^d = e$. Conversely, suppose $x^m = e$, and long-divide m by n: $m = qn + r$ where $q, r \in \mathbb{Z}$ with $0 \le r < n$. Then we have $e = x^m = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r$. But n was the smallest positive power of x that is e, so r, which is less than n, cannot be positive, i.e., it must be 0. Thus, n divides $m = qn$.

(ii) Because $\gcd(n, k)$ is a factor of k, $k/\gcd(n, k)$ is an integer, so $(x^k)^{n/\gcd(n,k)} = (x^n)^{k/\gcd(n,k)} = e^{k/\gcd(n,k)} = e$. So suppose there is an integer m for which $(x^k)^m = e$; in view of (i), it is enough to show that $n/\gcd(n, k)$ divides m: We know that $x^{km} = e$, so $n|km$, say $km = ns$ where $s \in \mathbb{Z}$. Dividing both sides by $\gcd(n, k)$ gives $(k/\gcd(n, k))m = (n/\gcd(n, k))s$. But $k/\gcd(n, k)$ and $n/\gcd(n, k)$ have no factors in common — we have divided out all the common factors — so they are relatively prime; so the fact that $n/\gcd(n, k)$ divides the product $(k/\gcd(n, k))m$ but is relatively prime to the first factor means that it must divide the second factor. Thus, $n/\gcd(n, k)$ divides m, as required.//

Def: If a group G includes an element x for which all the elements of G are powers of x, i.e., $\langle x\rangle = G$, then G is called a *cyclic group,* and x is called a *generator* of G.

If $o(x) = \infty$, we still call $\langle x\rangle$ a cyclic group, even though nothing is "cycling". For any group G, the cardinality $|G|$ is called the *order.* If $G = \langle x\rangle$ is cyclic, then $|G| = o(x)$.

Because the powers of an element all commute with each other, a cyclic group is abelian. But there are abelian groups that are not cyclic: The text gives the examples of $(\mathbb{Q}, +)$ (assume x is a generator; then $x/2$ is in $\mathbb{Q}$, but it is not an integral multiple — power — of x, a contradiction) and the "Klein Four-Group" $V = \{e, a, b, c\}$ with the operation [inspired by $\mathbb{Z}_2^2$ under addition modulo 2]

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

[

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

] .

Every element is its own inverse, so no element has order 4.