Groups and Symmetry HW3 Solutions

September 24, 2014

Exercise 1. 4.2

Proof. Note that the identity element in the group $\mathbb{Z}_n$ under modular addition is the element 0. For all of the groups in this problem the element 0 has order 1.

(a) Every element of $\mathbb{Z}_5$ except 0 has order five.

(b) In the group $\mathbb{Z}_9$, the elements 3 and 6 have order three. All other elements other than 0 have order 9.

(c) In the group $\mathbb{Z}_{12}$, the elements $1, 5, 7, 11$ have order 12. The elements $2, 10$ have order six. The elements $3, 9$ have order four. The elements $4, 8$ have order three. The element 6 has order two.

The general formula for the order of x in $\mathbb{Z}_n$ is $\frac{n}{\gcd(x,n)}$. Can you prove this? In particular, this says that if an element x is relatively prime to n, then it has order n, which means that every element of the group is of the form $i \cdot x$ for some i.

Also, notice that the order of any element divides the order of the group (we will prove this later on). □

Exercise 2. 4.3

Proof. Write out the multiplication table to check that the set is closed under multiplication and that each of their inverses is contained in the set.

Another way to see that all of these elements have an inverse mod 15 is by Bezout's identity which in this case says that for an element $x \mod 15$ there exist integers a, b such that $ax + b \cdot 15 = 1$ if and only if x is relatively prime to 15. But equation $ax + b \cdot 15 = 1$ is the statement $ax \equiv 1 \mod 15$, so x has an inverse $\mod 15$. And in particular, x's inverse a will also have to be relatively prime to 15. Now check that the set $\{1, 2, 4, 7, 8, 13, 14\}$ is precisely the set of numbers less than 15 that are relatively prime to 15, so they must all contain their inverses in the set.

The orders are

$$\begin{array}{cccccccc} 1 & 2 & 4 & 7 & 8 & 11 & 13 & 14 \\ 1 & 4 & 2 & 4 & 4 & 2 & 4 & 2 \end{array}.$$

Note that $14 \equiv -1 \mod 15$, and $13 \equiv -2 \mod 15$, so this may help in doing computations. □

Exercise 3. 4.4

Proof. Fix an element $g \in G$ and consider all of the products gx for all $x \in G$. Suppose two such products are the same, i.e. $gx = gy$ for some elements $x, y \in G$. Then multiplying by the inverse of g on the left gives $g^{-1}gx = g^{-1}gy$, which implies $x = y$. Therefore, the original elements x, y must have been the same, so all of the products are distinct.

Suppose that $h \in G$ is an arbitrary element of G. We need to show that there exists $x \in G$ such that $gx = h$. The element $x = g^{-1}h$ satisfies this property. Thus, the products gx fill up G. Note that you can use a counting argument here only if G is finite!

The case for the products xg is analogous. Note that this problem is really defining a map $\phi_g : G \to G$ that takes $x \in G$ to $\phi_g(x) = gx$, and we proved that this map is injective and surjective. More on this later in the course. □

Exercise 4. 4.6

Proof. We have that $x^2 = e, y^2 = e$, and $(xy)^2 = e$. The first two equations can be rewritten as $x = x^{-1}$ and $y = y^{-1}$. Then the second equation gives

$$\begin{aligned} & xyxy = e \\ \Longrightarrow\ & yxy = x^{-1} \\ \Longrightarrow\ & xy = y^{-1}x^{-1} \\ \Longrightarrow\ & xy = yx, \end{aligned}$$

where the last implications holds because $x = x^{-1}$ and $y = y^{-1}$. □

Exercise 5. 4.7

Proof. First we check that this set is closed under the operations. Given two rational numbers x, y such that $0 \leq x, y < 1$, then both expressions $x + y$ and $x + y - 1$ are rational numbers. In particular, if $0 \leq x + y < 1$, then the group operation gives the rational number $x + y$ that is contained in the desired range. It always holds that $x + y < 2$, so in the case that $1 \leq x + y$, we have $0 \leq x + y - 1 < 1$. Thus, in both cases the group operation specifies a rational number within the specified range.

To differentiate between usual addition (+) and the operation that defines the group operation we use the new notation $+_G$ for addition in the group. The identity element is the rational number 0 that is contained in the range $0 \leq x < 1$, and for any such x the group law says $0 +_G x = x +_G 0 = x$ because $0 + x = x + 0 < 1$ always holds.

Check that associativity holds, i.e. no matter which order you apply the group operation to three numbers, the number of times you subtract 1 is the same.

As is the case in any group, the inverse of the identity element, 0, is itself. The inverse of a rational number x in the range $0 < x < 1$ is a rational number y in the range $0 < y < 1$ such that $x +_G y = 0$. This can only happen if $x + y = 1$, so that $x +_G y = x + y - 1 = 0$. Therefore, the inverse to x is $1 - x$, which satisfies $0 < 1 - x < 1$ when $0 < x < 1$. Thus, the group operation turns this set into a group, and since addition is abelian, the group is abelian.

Every rational number $0 \leq x < 1$ can be written in the form $x = a/b$ where $a, b \in \mathbb{Z}$ and $a < b$. Furthermore, we may assume that a/b is in simplest form, i.e. if a, b share a prime factor p then divide both of them by p to get new integers a', b' such that $x = a/b = a'/b'$. Continuing on in this way we can get rid of all common factors, so we may assume from the beginning that $x = a/b$ where $a < b$ and a, b are relatively prime. Let k be the smallest integer such that $ka > b$. Then applying the group operation repeatedly gives $a/b +_G a/b = 2a/b$, $2a/b +_G a/b = 3a/b$, and so forth, until we reach the point $(k-1)a/b + a/b = ka/b > 1$, in which case $(k-1)a/b +_G a/b = (ka - b)/b$, which is the same as reducing $ka \mod b$ (note that $ka \geq 2b$ could never hold since $a < b$). Therefore, repeatedly adding the same rational number a/b under this group operation is equivalent to repeatedly adding the number a to itself mod b. Since a and b are relatively prime, we know from previous exercises that a has finite order. In fact, it's order is b. □

Exercise 6. 4.8

Proof. We prove by induction that $(gxg^{-1})^n = gx^ng^{-1}$. For the base case when $n = 2$, compute $(gxg^{-1})^2 = gxg^{-1}gxg^{-1} = gxxg^{-1} = gx^2g^{-1}$, as desired. Now suppose that the result holds for $n - 1$, i.e. $(gxg^{-1})^{n-1} = gx^{n-1}g^{-1}$. Then

$$\begin{aligned}(gxg^{-1})^n &= (gxg^{-1})^{n-1}gxg^{-1} \\ &= gx^{n-1}g^{-1}gxg^{-1} \text{ by the inductive hypothesis} \\ &= gx^ng^{-1},\end{aligned}$$

as desired. Suppose that $x^k = e$, then $(gxg^{-1})^k = gx^kg^{-1} = gg^{-1} = e$. Notice that this has only proved that the order of gxg^{-1} is at most the order of x! Now we prove the other direction, i.e. that the order of x is at most the order of x. If $(gxg^{-1})^k = e$, then $e = (gxg^{-1})^k = gx^kg^{-1} \implies g^{-1}g = x^k \implies e = x^k$. Thus, x^k is the identity exactly when $(gxg^{-1})^k$ is the identity, so their orders coincide.

To see that xy and yx have the same order, observe that $x(yx)x^{-1} = xy$ and apply the previous part of the exercise. □

Exercise 7. 5.1

Proof. Each example contains the trivial subgroup consisting of only the identity element. I am being brief here, but you are expected to prove that the subgroups you find are indeed subgroups and to prove that there are no others. If you don't convince yourself with a proof, then you will probably miss some subgroups or identify ones that aren't subgroups.

(a) The only nontrivial proper subgroup of $\mathbb{Z}_4$ is the group generated by the element 2, which is just the set $\{0, 2\}$.

(b) There are no nontrivial proper subgroups of $\mathbb{Z}_7$ because each element other than 0 generates the group.

(c) There is one subgroup of order 6 generated by 2, one subgroup of order 3 generated by 4, one subgroup of order 4 generated by 3, and one subgroup of order 2 generated by 6.

(d) The dihedral group D_4 has five subgroups of order 2 each generated respectively by s, r^2, rs, r^2s, r^3s. There are also three subgroups of order 4, one a cyclic subgroup generated by r. The second was is generated by s and r^2. The third and final one is generated by rs and r^2.

(e) The dihedral group D_5 has a single subgroup of order 5 generated by r (also generated by r^2, or r^3, or r^4). It also contains 5 distinct subgroups of order 2, each one generated respectively by s, rs, r^2s, r^3s, r^4s.

□

Exercise 8. 5.2

Proof. If m is a divisor of n, then we may write $n = m \cdot a$ (where $a = n/m$). The order of the element a in $\mathbb{Z}_n$ is m (recall the general formula is $n/\gcd(n, m)$ where in this case $\gcd(n, m) = m$). The m elements $\{a, 2a, 3a, \ldots, (m-1)a, ma = 0\}$ form a subgroup of $\mathbb{Z}^n$, and the elements are all distinct because the order of a is m. The inverse of $k \cdot a$ is $(m - k) \cdot a$, which is in the set, the set contains the identity, and adding any two elements in the set again gives an element of the set. Thus, this is a subgroup of order m.

Suppose there is some other subgroup of order m. Then by Theorem 5.3 (a) this subgroup must be cyclic, i.e. it is generated by some element x, and the subgroup consists of the m elements $\{x, 2x, \ldots, (m - 1)x, mx = 0\}$. Since $mx \equiv 0 \mod n$, it follows that $mx = nk$ for some integer k. Then $mx = nk = mak$, implies $x = ak$. Thus, a divides x, so $ab = x$ for some number b, which implies that x is contained in the subgroup generated by a, $\{a, 2a, \cdots, (m - 1)a, ma = 0\}$. Since x also generates a subgroup of m elements all of which must be contained in the subgroup generated by a, these two subgroups coincide. □

Exercise 9. 5.3

Proof. Recall the identity $sr = r^{n-1}s$ or equivalently $srs = r^{n-1}$. Then $(r^2s)(rs) = rr(srs) = r^2r^{n-1} = r$, so we can get r using the two specified elements, and therefore also r^{n-1}. Then using the two elements also gives $r^{n-1}(rs) = s$, so the two elements generate both r and s so they generate the Dihedral group D_n. □

Exercise 10. 5.5

Proof. ($\Longrightarrow$) If H is a subgroup then xy belongs to H whenever $x, y \in H$. ($\Longleftarrow$) Suppose that H is finite and nonempty subset of G such that for all $x, y \in H$ we have that $xy \in H$. Since H is nonempty there exists an element $x \in H$. Since $x \in H$, $xx = x^2 \in H$. Likewise, taking x and $y = x^2$ both in H, we have that $x^3 \in H$. Consider the powers $x, x^2, x^3, x^4, \ldots$ all of which are in H. Since H is finite, this list cannot have infinitely many distinct elements. Let n be the smallest number such that $x^n = x^k$ for some $k < n$. Then taking inverses gives $x^{n-k} = e$, but x^{n-k} appears in the list because $n - k > 0$. Thus the list, and hence H, contains e. Furthermore, $x(x^{n-k-1}) = e$, so x has an inverse in the list, and hence x has an inverse in H. Since x was an arbitrary element of H, the same reasoning can be applied to any element to show that it has an inverse. Therefore, H is closed under the group operation, contains the identity and contains inverses, so is itself a subgroup. □