Subgroups

Contents

2.1: Definition and Examples

Exercises

1. For the sake of this problem I'll be explicit with group notation. For the proposed subgroup $(H, \cdot) \leq (G, \star)$, we want to show that $H \subset G$ and $\cdot = \star$. Then, if H is finite, we want to show that for all $x, y \in H$, $x \cdot y \in H$. If H is not finite we want to show that $x \cdot y^{-1} \in H$.

   (a) Here $H = (\{a(1+i) \mid a \in \mathbb{R}\},\ +)$ which is not finite, and $G = (\mathbb{C},\ +)$. Clearly every element of H is a complex number so $H \subset G$, and the two have the same operation. The identity is 0, so the inverse of $a(1+i)$ is $-a(1+i)$. For two arbitrary elements $x, y \in H$,

   $$x \cdot y^{-1} = a_x(1+i) + (-a_y)(1+i) = (a_x - a_y)(1+i) \in H \tag{1}$$

   so $H \leq G$.

   (b) Here $H = (\{z \mid z \in \mathbb{C},\ z^* z = 1\},\ \cdot)$ and $G = (\mathbb{C},\ \cdot)$. Again trivially $H \subset G$ and the operation is the same. The identity is 1 so $z^{-1} = \frac{1}{z}$. The subgroup H is infinite, so for $z_1, z_2 \in H$, $z_1 \cdot z_2^{-1} = \frac{z_1}{z_2}$ and

   $$\left(\frac{z_1}{z_2}\right)^* \left(\frac{z_1}{z_2}\right) = \left(\frac{z_1^*}{z_2^*}\right)\left(\frac{z_1}{z_2}\right) = \frac{z_1^* z_1}{z_2^* z_2} = \frac{1}{1} = 1 \tag{2}$$

   so $z_1 \cdot z_2^{-1} \in H$ and $H \leq G$.

   (c) For a fixed n, if $q = \frac{a}{b} \in \mathbb{Q}$ with $b|n$, then $qn \in \mathbb{Z}$. This provides an alternate characterization for H: $H = (\{q \mid q \in \mathbb{Q},\, qn \in \mathbb{Z}\},\ +)$ and $G = (\mathbb{Q}, +)$. Again $H \subset G$ and the operation being the same are trivial. The identity of G is 0, so $q^{-1} = -q$. For $q_1, q_2 \in H$, $q_1 \cdot q_2^{-1} = q_1 - q_2$, and clearly this is also an integer when multiplied by n, making $H \leq G$.

   (d) For a fixed n, $H = \left(\left\{\frac{a}{b} \mid \frac{a}{b} \in \mathbb{Q},\, (b, n) = 1\right\}, +\right)$ and $G = (\mathbb{Q}, +)$ again. The subset and operation are trivial, and the identity is 0 again with more explicit inverse $\left(\frac{a}{b}\right)^{-1} = \frac{-a}{b}$. For $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in H$,

   $$\frac{a_1}{b_1} \cdot \left(\frac{a_2}{b_2}\right)^{-1} = \frac{a_1}{b_2} + \frac{-a_2}{b_2} = \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}\ . \tag{3}$$

   If $(b_1, n) = (b_2, n) = 1$, then $(b_1 b_2, n) = 1$, and any cancellation of common factors in the numerator and denominator won't change that since none of the factors of $b_1 b_2$ are factors of n. Therefore $H \leq G$.

   (e) Here $H = (\{x \mid x \in \mathbb{R},\, x^2 \in \mathbb{Q}\}, \cdot)$ with $G = (\mathbb{Q}, \cdot)$. The subset and operation are trivial and the identity is 1 so $x^{-1} = \frac{1}{x}$. For $x, y \in H$, $x \cdot y^{-1} = \frac{x}{y}$, so

   $$(x \cdot y^{-1})^2 = \left(\frac{x}{y}\right)^2 = \frac{x^2}{y^2} \in \mathbb{Q} \tag{4}$$

   i.e. $H \leq G$.

2. Same as above, but hopefully faster and more interesting.

   (a) The identity of S_n is not a 2-cycle.

   (b) what

   (c)

   (d) The set isn't closed under the operation since odd + odd = even.

   (e) Again, the set isn't closed under the operation, e.g. $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$.

3. Both subsets are obviously finite subsets of D_8 with the same group operation, so we just want to check that they are closed under composition. Referring to the solution of exercise 1.5.2 for the multiplication table for D_8 confirms this for both subsets.

4. Consider $(\mathbb{N},+)$ as a possible subgroup of $(\mathbb{Z},+)$. $\mathbb{N}$ is infinite and closed under the group operation since the sum of two positive numbers is positive. However, the additive identity 0 is not in $\mathbb{N}$ (sorry if you disagree), and on top of that $(\mathbb{N},+)$ is not closed under inverses (hopefully you agree with this one).

5. Suppose $|G| = n$ and $H \leq G$ with $|H| = n-1$. Denote the single element of $G - H$ with g, and all other elements of G are in H. Then $g^{-1} \in H$, but $\left(g^{-1}\right)^{-1} = g$ is not in H, so H is not closed under inverses.

6. The torsion subgroup H is potentially infinite so we need to show that for all $g, h, \in H$, $gh^{-1} \in H$. By exercise 1.1.22, if $g, h^{-1} \in G$ and G is abelian, then $(gh^{-1})^n = g^n(h^{-1})^n$ so $\left|gh^{-1}\right| = \operatorname{lcm}(|g|, \left|h^{-1}\right|)$. By exercise 1.1.20, $\left|h^{-1}\right| = |h|$, so if g and h both have finite order then so does gh. counterexample for nonabelian?

7. For $(x,y) \in \mathbb{Z}\times(\mathbb{Z}/n\mathbb{Z})$, if $|(x,y)| = k \geq 1$, then $kx = 0$ and $ky = 0$, where the second equation is modulo n but the first one isn't. The first equation requires $x = 0$, while the second always has a solution e.g. $k = \frac{\operatorname{lcm}(y,n)}{n}$. Therefore the torsion subgroup is $\{0\} \times (\mathbb{Z}/n\mathbb{Z})$.

   The group of elements of infinite order is not a subgroup because it's not closed under addition. An element (x,y) has infinite order if and only if $x \neq 0$, then $(x,y) + (-x,z) = (0, y-z)$ for any y, z, so we have added two elements of infinite order together to get one with finite order.

8. We are given $H \leq G$ and $K \leq G$. First assume $H \cup K \leq G$. If either one of H or K is the trivial subgroup then $H \subseteq K$ or $K \subseteq H$ trivially since every subgroup contains the identity. Otherwise, let $h \in H$ and $k \in K$. For $H \cup K$ to be a subgroup, the product $x = hk$ must still be in the subgroup, so it must either be in H or K (or both). If it is in H, then $h^{-1}x = k$ must also be in H. Since k was arbitrary we see that all elements of K are in H, so $K \subseteq H$. Likewise, if $x \in K$ then $xk^{-1} = h \in K$ so $H \subseteq K$.

   In the other direction, if $H \subseteq K$ or $K \subseteq H$ then $H \cup K$ is just equal to the larger subgroup, so it is trivially a subgroup of G.

9. The structure is inherited from $GL_n(F)$ so we just need to show that, for all $X, Y \in SL_n(F)$, $M = XY^{-1} \in SL_n(F)$. This is easily seen with $\det Y^{-1} = \frac{1}{\det Y} = 1$ and $\det M = \det X \det Y^{-1} = 1$.

10. Again the subset is trivial and the group operation is the same.

    (a) If $H \leq G$ and $K \leq G$, and $x, y \in H \cap K$, then $xy^{-1} \in H$ and $xy^{-1} \in K$ so $xy^{-1} \in H \cap K$.

    (b) If you assume the collection is countable you can use the above proof and $(A \cap B) \cap C = A \cap B \cap C$. uncountable??

11. Again again the subset is trivial and the group operation is the same. Denote each subgroup as H. We use 1.1.28.c which states that $(a,b)^{-1} = (a^{-1}, b^{-1})$.

    (a) For $(a_1, 1), (a_2, 1) \in H$,

    $$(a_1,1)\cdot(a_2,1)^{-1} = (a_1,1)\cdot(a_2^{-1},1^{-1}) = (a_1\cdot a_2^{-1}, 1\cdot 1) = (a_1a_2^{-1},1) \in H\ . \tag{5}$$

    (b) For $(1, b_1), (1, b_2) \in H$,

    $$(1,b_1)\cdot(1,b_2)^{-1} = (1,b_1)\cdot(1^{-1},b_2^{-2}) = (1\cdot 1, b_1\cdot b_2^{-1}) = (1, b_1b_2^{-1}) \in H\ . \tag{6}$$

(c) For $(a_1, a_1), (a_2, a_2) \in H$,

$$(a_1, a_1) \cdot (a_2, a_2)^{-1} = (a_1, a_1) \cdot (a_2^{-1}, a_2^{-1}) = (a_1 a_2^{-1}, a_1 a_2^{-1}) \in H \ . \tag{7}$$

12. Again again again all elements are trivially in A and the group operation is inherited. We also use exercise 1.1.20 again like we did in exercise 6. Let H denote the subgroup.

    (a) For $a^n, b^n \in H$, $a^n (b^n)^{-1} = a^n b^{-n} = (ab^{-1})^n$ where $ab^{-1} \in A$ as required. We use 1.1.24 here.

    (b) For $a, b \in H$, $(ab^{-1})^n = a^n (b^{-1})^n$. Since $|a| = n$ and $|b| = \left|b^{-1}\right| = n$, we see that $\left|ab^{-1}\right| = \text{lcm}(|a|, |b|) = n$.

13. hard

14. From 1.2.3 we know that every element of D_{2n} of the form sr^k (here $k \in [0, n-1]$ but we can just take it as any integer since $r^n = 1$) has order 2. Choose a, b such that sr^a and sr^b are distinct (so $b - a \neq 0 \bmod n$). Then

$$(sr^a)(sr^b) = (r^{-a}s)(sr^b) = r^{-a}s^2 r^b = r^{b-a} \neq 1 \tag{8}$$

    which means that this set of elements is not closed under composition and cannot be a subgroup.

15. the inductive proof is obvious but that's just an arbitrarily large finite union, I don't know what it means to extend it to a countably infinite chain of subgroups without a concrete example that I can't think of

16. The inverse of an upper triangular matrix is upper triangular; the product of two upper triangular matrices is upper triangular, so for triangular $X, Y \in GL_n(F)$, the product XY^{-1} is upper triangular as well.

17. extreme copout: heisenberg group from 1.4.11

2.2: Centralizers and Normalizers, Stabilizers and Kernels

Exercises

1. The definition is $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. If $gag^{-1} = a$, then, left-multiplying g^{-1} and right-multiplying g, we equivalently have $a = g^{-1}ag$.

2. Choose an arbitrary $x \in G$. By definition, x commutes with every element of $Z(G)$, so $xg = gx$ for all $g \in Z(G)$ and $x \in C_G(Z(G))$. Since $C_G(A) \leq N_G(A)$ for any A, in this case we also find that $N_G(Z(G)) = G$.

3. For $A \subseteq B$, every element in $C_G(B)$ must commute with every element of A, so it must also be in $C_G(A)$, i.e. $C_G(B) \subseteq C_G(A)$. Both are subgroups of G so $C_G(B) \leq C_G(A)$.

4. I'm just going to be reading off of the multiplication tables in exercise 1.5.2 for this. Lagrange's Theorem doesn't help because I already did all the manual labor for this. For S_3, the list of elements that commute are

    1 : all elements
    $(1\ 2)$: 1, $(1\ 2)$
    $(1\ 3)$: 1, $(1\ 3)$
    $(2\ 3)$: 1, $(2\ 3)$
    $(1\ 2\ 3)$: 1, $(1\ 2\ 3)$, $(1\ 3\ 2)$
    $(1\ 3\ 2)$: 1, $(1\ 2\ 3)$, $(1\ 3\ 2)$

    so $Z(S_3) = \{1\}$. For D_8,

    1 : all elements
    r : 1, r, r^2, r^3
    r^2 : all elements
    r^3 : 1, r, r^2, r^3
    s : 1, r^2, s
    sr : 1, r^2, sr, sr^3

sr^2 : 1, r^2, s, sr^2

sr^3 : 1, r^2, sr, sr^3

so $Z(D_8) = \{1, r^2\}$. For Q_8,

1 : all elements

-1 : all elements

i : 1, -1, i, $-i$

$-i$: 1, -1, i, $-i$

j : 1, -1, j, $-j$

$-j$: 1, -1, j, $-j$

k : 1, -1, k, $-k$

$-k$: 1, -1, k, $-k$

so $Z(Q_8) = \{1, -1\}$.

5. More reusing previous results.

   (a) The set of elements of S_3 that commute with all elements of A is exactly A as seen in the previous exercise. That $N_G(A) = S_3$ can be seen by following the multiplication table in exercise 1.5.2 again.

   (b) Same as above.

   (c) All elements D_{10} are either powers of r (and are in A) or are of the form sr^k. Since $rs \neq sr$, none of those elements commute with every element of A, and the only elements of D_{10} that commute with powers of r are other powers or r so $C_G(A) = A$. To see how conjugation acts on A consider conjugation by an arbitrary element not in A:

$$(sr^k)r^n(sr^k)^{-1} = (sr^k)r^n(sr^k) = sr^{k+n}sr^k = ssr^{k+n}r^k = r^{2k+n} \tag{9}$$

   so the exponents in A are just shifted up by $2k$ and $A \mapsto A$. Conjugation by an element of the form r^k trivially preserves A, so $N_G(A) = G$.

6. We are given $H \leq G$.

   (a) Since H is closed under inverses and multiplication, for any $g, h \in H$, $hgh^{-1} \in H$. Therefore $hHh^{-1} = H$. counterexample

   (b) If $H \leq C_G(H)$, then, for all $g, h \in H$, $ghg^{-1} = h$ i.e. $gh = hg$ so H is abelian. The other direction is the argument in reverse.

7. (a) All elements of D_{2n} are r^k and sr^k for $k = 0, \ldots, n-1$. We just need to show that every nonidentity element has at least one other element it doesn't commute with. Consider the multiplication of r^k and sr^l:

$$r^k \cdot sr^l = r^k \cdot r^{-l}s = r^{k-l}s \tag{10}$$

$$sr^l \cdot r^k = sr^{k+l} = r^{-k-l}s\ . \tag{11}$$

   These products are only the same if $r^{2k} = 1$. Since n is odd, that means $r^k = 1$, in which case we were working with $r^k = 1$ and $sr^k = s$. We still need to show that s is not in the center; this is obvious because it doesn't commute with r. We have now explicitly shown that every nonidentity element fails to commute.

   (b) If n is even then $r^{2k} = 1$ has another solution: $k = \frac{n}{2}$. Then this r^k commutes with all sr^l, and it also trivially commutes with powers of r, so it is in the center of the group.

8. The group $G = S_n$ acts on the set $A = \{1, \ldots, n\}$, and $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ all keep i fixed. The identity permutation has $\sigma(k) = k$ for all k, not just i, so $1 \in G_i$. If $\sigma_1, \sigma_2 \in G_i$, then $\sigma_1 \circ \sigma_2$ is as well since $(\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i)) = \sigma_1(i) = i$. Also, $\sigma_1^{-1}(i) = i$ as well, so G_i is a group. If we send $i \mapsto i$ then there are only $n-1$ elements of A to permute, so $|G_i| = (n-1)!$.

9. By definition, $N_H(A)$ is the same as $N_G(A)$ but the conjugating elements come from H instead. All of these elements have to be in H (duh), but since $H \leq G$, all of these elements are also in G, so $N_H(A)$ is exactly the subset of $N_G(A)$ that is in H, i.e. $N_H(A) = N_G(A) \cap H$. subgroup of H follows?

10. If H is a subgroup of order 2, then $H = \{1, x\}$ for some $x \in G$ where $x^2 = 1$. The difference between $N_G(H)$ and $C_G(H)$ in general is that conjugation by an element in C_G sends every element of H to itself, while conjugation by an element of N_G can permute different elements of H. In this case, conjugation always maps the identity to itself ($g1g^{-1} = 1$ for any g), so if we want all of H to be in the image of the conjugation we require $x \mapsto x$. We see that the only possible conjugation actions of G sending H to H sends every element to itself, so $C_G(H) = N_G(H)$. If $N_G(H) = G$, then $C_G(H) = G$, meaning the elements of H commute with all elements of G and $H \leq Z(G)$.

11. We want to show that if $g \in Z(G)$, then $g \in N_G(A)$ for any subset A of G. If $g \in Z(G)$ then g commutes with all elements of G, so $gag^{-1} = gg^{-1}a = a$ for any element $a \in A$. We then see that $gAg^{-1} = A$, so $g \in N_G(A)$. The shorter version is $Z(G) \leq C_G(A)$ for any subset A, and $C_G(A) \leq N_G(A)$ by definition.

12. Oh boy! (in retrospect this problem was interesting and I retract this statement)

    (a) Given $\sigma = (1\ 2\ 3\ 4)$ and $\tau = (1\ 2\ 3)$, $\sigma \circ \tau = (1\ 3\ 2\ 4)$ and $\tau \circ \sigma = (1\ 3\ 4\ 2)$. I'm not writing the polynomial out because it's what you find in the dictionary when you look up the word "arbitrary". The original is $p(x_1, x_2, x_3, x_4)$.

    i. $\sigma \cdot p = p(x_2, x_3, x_4, x_1)$
    ii. $\tau \cdot (\sigma \cdot p) = \tau \cdot p(x_2, x_3, x_4, x_1) = p(x_3, x_1, x_4, x_2)$
    iii. $(\tau \circ \sigma) \cdot p = p(x_3, x_1, x_4, x_2)$ by associativity
    iv. $(\sigma \circ \tau) \cdot p = p(x_3, x_4, x_2, x_1)$

    (b) The identity permutation sends each $p \in R$ to itself. The inverse of a permutation is a permutation, and the composition of two permutations is another permutation:

    $$(\sigma_2 \circ \sigma_1) \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma_2(\sigma_1(1))}, x_{\sigma_2(\sigma_1(2))}, x_{\sigma_2(\sigma_1(3))}, x_{\sigma_2(\sigma_1(4))}) = \sigma_2 \cdot (\sigma_1 \cdot p(x_1, x_2, x_3, x_4)) \quad (12)$$

    (c) The permutations that stabilize x_4 are the ones with no "4" in the cycle decomposition: 1, (1 2), (1 3), (2 3), (1 2 3), and (1 3 2). These are trivially isomorphic to S_3, I think I remember a sentence saying that the whole point of cycle notation being how it is is so that we could see that $S_n \leq S_m$ for $n < m$.

    (d) To stabilize the polynomial $x_1 + x_2$, we can either do nothing (duh), swap the labels $1 \leftrightarrow 2$, permute the remaining labels 3 and 4, or some mix. The permutations are 1, (1 2), (3 4), and (1 2)(3 4). Since (1 2) and (3 4) are disjoint cycles that square to the identity, this is an abelian subgroup.

    (e) To stabilize $x_1x_2 + x_3x_4$, we either swap $1 \leftrightarrow 2$, $3 \leftrightarrow 4$, or both as before, or we can also swap the two terms with $(1, 2) \leftrightarrow (3, 4)$. The explicit permutations are 1, (1 2), (3 4), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 4 2 3), and (1 3 2 4). Let $r = (1\ 4\ 2\ 3)$ and $s = (1\ 2)$, then $r^4 = s^2 = 1$ and $rs = sr^{-1}$, which is the usual presentation of D_8. The explicit representation of each element I listed is, in order, 1, s, sr^2, r^2, sr^3, sr, r, r^3.,

    (f) To stabilize $(x_1 + x_2)(x_3 + x_4)$ we can perform the same swaps as the previous example. It's the same structure since 1 and 2 are grouped in a way where order doesn't matter, 3 and 4 are grouped in a way order doesn't matter, and the order of the two terms doesn't matter.

13. See part b of the previous exercise.

14. We want to find the conditions for an element of $H(F)$ to commute with all other elements. The matrix bashing is

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix} \quad (13)$$

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+xc+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix}. \quad (14)$$

If we want this to be true for all a, b, c, then $x = z = 0$, so

$$Z(H(F)) = \left\{ \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mid y \in F \right\} \tag{15}$$

which has an obvious isomorphism to F itself.

2.3: Cyclic Groups and Cyclic Subgroups

Exercises

1. Theorem 7 lets us list the subgroups by finding the gcd of $(n, 45)$ for all $n < 45$:
   (a) $Z_{45} = \langle x \rangle = \langle x^2 \rangle = \langle x^4 \rangle = \langle x^7 \rangle = \langle x^8 \rangle$ and all other x^n for n coprime to 45, which is (I'm just padding so the set goes on the next line) $n \in \{11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44\}$
   (b) $Z_{15} = \langle x^3 \rangle = \langle x^6 \rangle = \langle x^{12} \rangle = \langle x^{21} \rangle = \langle x^{24} \rangle = \langle x^{33} \rangle = \langle x^{39} \rangle = \langle x^{42} \rangle$
   (c) $Z_9 = \langle x^5 \rangle = \langle x^{10} \rangle = \langle x^{20} \rangle = \langle x^{25} \rangle = \langle x^{35} \rangle = \langle x^{40} \rangle$
   (d) $Z_5 = \langle x^9 \rangle = \langle x^{18} \rangle = \langle x^{27} \rangle = \langle x^{36} \rangle$
   (e) $Z_3 = \langle x^{15} \rangle = \langle x^{30} \rangle$
   (f) $1 = \langle 1 \rangle$
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16. y
17. Isn't this just $Z_n = \langle x \mid x^n = 1 \rangle$?
18. Let Z_n be generated by x, and $h^n = 1$ in H. For a homomorphism $\phi : Z_n \to H$ with $\phi(x) = h$ then

$$1 = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = h\phi(x^{-1}) \tag{16}$$

so $\phi(x^{-1}) = h^{-1}$. By induction,

$$\phi(x^n) = \phi(x)\phi(x^{n-1}) = hh^{n-1} = h^n \tag{17}$$

$$\phi(x^{-n}) = \phi(x^{-1})\phi(x^{-(n-1)}) = h^{-1}h^{-(n-1)} = h^{-n} \tag{18}$$

and $\phi(1) = 1$, so $\phi(x^k) = h^k$ for any $k \in \mathbb{Z}$. This is well-defined since $x^n = 1$ and $\phi(x^n) = h^n = 1$. By the division algorithm we have a unique map sending x^k to h^k for $k = 0, \ldots, n$.

19. This is very similar to the previous exercise. $(\mathbb{Z}, +)$ is generated by the number 1, so for a homomorphism $\phi : \mathbb{Z} \to H$ with $\phi(1) = h$,

$$\phi(2) = \phi(1+1) = \phi(1)\phi(1) = hh = h^2 \tag{19}$$

so $\phi(n) = h^n$ for all positive n by induction. For negative exponents, since $\phi(0) = 1_H$,

$$1_H = \phi(0) = \phi(-1+1) = \phi(-1)\phi(1) = \phi(-1)h \tag{20}$$

so $\phi(-1) = h^{-1}$. Then $\phi(-2) = h^{-2}$, and $\phi(-n) = h^{-n}$ by induction again. We have completely specified ϕ.

20. First we prove that, if for some $x \in G$, $|x| = k$, and $x^m = 1$ for some $m > 0$, then $k \mid m$. Assume that this is not true; that $|x| = k$, $x^m = 1$, and $m = pk + r$ for some integers p, r where $1 \leq r < k$ (the remainder is nonzero). Then

$$1 = x^m = x^{pk+r} = \left(x^k\right)^p x^r = 1^p x^r = x^r \tag{21}$$

which is a contradiction since $|x| = k$ means that x^r is not the identity.

Now, if $x^{p^n} = 1$, then $|x| \mid p^n$. By the Fundamental Theorem of Arithmetic (is this overkill?) the only divisors of p^n are p^m for $m = 1, \ldots, n$.

21.

22.

23.

24. G is a finite group here.

(a) If $g \in N_g(\langle x \rangle)$ then by definition there exists an n such that $gx^m g^{-1} = x^n$ for all m. Just choose $m = 1$ here.

(b) If $gxg^{-1} = x^a$, then $x^{2a} = gxg^{-1} \cdot gxg^{-1} = gxxg^{-1} = gx^2g^{-1}$ and by induction $x^{ka} = gx^k g^{-1}$. Therefore all powers of x get sent to some (possibly other) power of x under conjugation by g. We just need to show that the map is surjective. G being finite means that x has finite order, call it n. If $gx^a g^{-1} = gx^b g^{-1}$, then, left-canceling g and right canceling g^{-1}, $x^a = x^b$, so conjugation by g sends each power of x to a different element of G. Therefore $\left|g \langle x \rangle g^{-1}\right| = n = |\langle x \rangle|$ so the two sets are equal and $g \in N_g(\langle x \rangle)$.

25. The first part of this is pretty obvious once written out in excruciating detail. Here $G = Z_n$, $(k, n) = 1$, and we want to show that $x \mapsto x^n$ is surjective. That means that for all $a \in \{0, 1, \ldots, n-1\}$, we want to show that there exists an element of G, namely x^m, that gets mapped to x^a, i.e. $x^a = (x^m)^k$ or $a = km$ where equality is modulo n. Since $(k, n) = 1$, $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ and there exists a k^{-1} so that $m = k^{-1}a$. This identifies m for a given a. lagrange?

26. Let Z_n be generated by x.

(a) If $(a, n) = 1$, then we showed in the previous exercise that σ_a is surjective. To show it is injective, suppose $\sigma_a(x^b) = \sigma_a(x^c)$. Then $x^{ab} = x^{ac}$ so $1 = x^{ac}x^{-(ab)} = x^{a(c-b)}$ and we see that either $a = 0$, in which case (a, n) couldn't be 1, or $b = c$ (modulo n) so the preimages are equal. The homomorphism part is just

$$\sigma_a(x^b) \cdot \sigma_a(x^c) = x^{ab}x^{ac} = x^{a(b+c)} = \sigma_a(x^{b+c}) = \sigma_a(x^b \cdot x^c)\ . \tag{22}$$

opposite direction?

(b) If $\sigma_a = \sigma_b$, then, for all $y \in Z_n$, $y^a = y^b$. Since $y = x^k$ for some k, that means $x^{ak} = x^{bk}$ or $x^{k(a-b)} = 1$. Since this is true for all k, we see that we must have $a = b$ (modulo n). In the other direction, if $a = b$ modulo n, let c be the representative of the equivalence class on $[0, n-1]$. Then $a = m_a n + c$ and $b = m_b n + c$ (I am totally not running out of letters). For any $y = x^k$,

$$\sigma_a(y) = x^{ak} = x^{k(m_a n + c)} = x^{km_a n}x^{kc} = x^{kc} \tag{23}$$

$$\sigma_b(y) = x^{bk} = x^{k(m_b n + c)} = x^{km_b n}x^{kc} = x^{kc} \tag{24}$$

so $\sigma_a = \sigma_b$.

(c)

(d) Follow the image of an arbitrary element $y = x^k$:

$$\sigma_a(\sigma_b(y)) = \sigma_a(y^b) = (y^b)^a = y^{ab} = \sigma_{ab}(y) \ . \tag{25}$$

Parts a and c showed that all automorphisms of Z_n are given by some σ_a where $(a, n) = 1$. Part b showed that these maps can be defined modulo n, so we can say that $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ without loss of generality. Therefore there is a bijection between elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ and automorphisms of Z_n, where σ_a corresponds to $\bar{a}$. The homomorphism part is shown above, so we have an isomorphism between $(\mathbb{Z}/n\mathbb{Z})^\times$ and $\mathrm{Aut}(Z_n)$.