Subgroups

Contents

2.1: Definition and Examples

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 $H \le G$ 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 $\left|gh^{-1}\right| = \mathrm{lcm}(|g|, \left|h^{-1}\right|)$. 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 $|(x, y)| = k \ge 1$, 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. $k = \frac{\mathrm{lcm}(y,n)}{n}$. 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 $x \ne 0$, 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 $H \le G$ and $K \le G$. First assume $H \cup K \le G$. 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 $H \le G$ and $K \le G$, 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 $(a_1, 1), (a_2, 1) \in H$,

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

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

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

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

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
$$\begin{aligned} 1 &: \text{all elements} \\ (1\ 2) &: 1,\ (1\ 2) \\ (1\ 3) &: 1,\ (1\ 3) \\ (2\ 3) &: 1,\ (2\ 3) \\ (1\ 2\ 3) &: 1,\ (1\ 2\ 3),\ (1\ 3\ 2) \\ (1\ 3\ 2) &: 1,\ (1\ 2\ 3),\ (1\ 3\ 2) \end{aligned}$$
so $Z(S_3) = \{1\}$. For D_8,
$$\begin{aligned} 1 &: \text{all elements} \\ r &: 1,\ r,\ r^2,\ r^3 \\ r^2 &: \text{all elements} \\ r^3 &: 1,\ r,\ r^2,\ r^3 \\ s &: 1,\ r^2,\ s \\ sr &: 1,\ r^2,\ sr,\ sr^3 \\ sr^2 &: 1,\ r^2,\ s,\ sr^2 \\ sr^3 &: 1,\ r^2,\ sr,\ sr^3 \end{aligned}$$
so $Z(D_8) = \{1, r^2\}$. For Q_8,

$$
\begin{aligned}
1 &: \text{all elements} \\
-1 &: \text{all elements} \\
i &: 1,\ -1,\ i,\ -i \\
-i &: 1,\ -1,\ i,\ -i \\
j &: 1,\ -1,\ j,\ -j \\
-j &: 1,\ -1,\ j,\ -j \\
k &: 1,\ -1,\ k,\ -k \\
-k &: 1,\ -1,\ k,\ -k
\end{aligned}
$$

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 $k = 0, \dots, n-1$. 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 $A = \{1, \dots, n\}$, 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!

    (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:

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

    (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 $(1\ 3\ 2\ 4)$. D8?

    (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

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

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

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.