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 $H \leq G$ 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 $\left|gh^{-1}\right| = \text{lcm}(|g|, \left|h^{-1}\right|)$. 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. $k = \frac{\text{lcm}(y,n)}{n}$. 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 $(a_1, 1), (a_2, 1) \in H$,

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

    (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 $\left|ab^{-1}\right| = \mathrm{lcm}(|a|, |b|) = n$.

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