

Math 113 Homework # 3, selected solutions

Fraleigh 5.13: Yes, this set of matrices, which is called $O(n)$, is a subgroup of $GL(n, \mathbb{R})$. First note that $O(n)$ is a subset of $GL(n, \mathbb{R})$ because if $A^T A = I$, then A is injective, so by the “rank-nullity” theorem in linear algebra, its range has dimension n , so A is invertible. We also note that since left inverses are unique, $A^T = A^{-1}$, so $AA^T = I$ also. Now $O(n)$ is closed under multiplication because if $A^T A = I$ and $B^T B = I$ then $(AB)^T(AB) = B^T A^T AB = B^T IB = B^T B = I$. $O(n)$ contains the identity because $I^T I = I^2 = I$. $O(n)$ is closed under inverses because if $A^T A = I$ then $(A^{-1})^T A^{-1} = (A^T)^{-1} A^{-1} = (AA^T)^{-1} = I^{-1} = I$. (Here we have used the facts that $AA^T = I$ as explained above, and also that for any invertible matrix A we have $(A^T)^{-1} = (A^{-1})^T$; this holds because $(A^{-1})^T A^T = (AA^{-1})^T = I^T = I$.)

Fraleigh 5.54: $H \cap K$ is closed under multiplication because if $x, y \in H \cap K$, then since $x, y \in H$ and H is a subgroup we have $xy \in H$; since $x, y \in K$ and K is a subgroup we have $xy \in K$; so $xy \in H \cap K$. $H \cap K$ contains the identity because since H and K are subgroups, $e \in H$ and $e \in K$, so $e \in H \cap K$. Finally, $H \cap K$ is closed under inverses because if $x \in H \cap K$, then since $x \in H$ and H is a subgroup, $x^{-1} \in H$; since $x \in K$ and K is a subgroup, $x^{-1} \in K$; so $x^{-1} \in H \cap K$.

This is not true if one replaces intersection by union. For example the union of the subgroups $\langle 2 \rangle$ and $\langle 3 \rangle$ of \mathbb{Z} is not a subgroup of \mathbb{Z} , because it contains 2 and 3 but it does not contain $2 + 3$.

6:

- (a) $Z(G)$ is closed under multiplication because if $x_1, x_2 \in Z(G)$, then for every $y \in G$, since y commutes with both x_1 and x_2 , we have

$$x_1 x_2 y = x_1 y x_2 = y x_1 x_2$$

so $x_1 x_2 \in Z(G)$. The identity is in $Z(G)$ because for all $y \in G$ we have $ey = ye = y$ by the definition of the identity. If $x \in Z(G)$ then $x^{-1} \in Z(G)$, because for any $y \in G$, since x commutes with y^{-1} we have

$$x^{-1} y = (y^{-1} x)^{-1} = (x y^{-1})^{-1} = y x^{-1}.$$

- (b) For all i we have $F_i \notin Z(D_n)$, because $F_i F_j = R_{i-j}$ while $F_j F_i = R_{j-i}$, and since $n > 2$ we can arrange for these to be unequal by taking $j = i - 1$ so that $i - j = 1$ and $i - j \neq j - i$ in \mathbb{Z}_n .

Also, as long as $2i \neq 0$ in \mathbb{Z}_n , we have $R_i \notin Z(D_n)$, because $R_i F_j = F_{i+j}$ while $F_j R_i = F_{j-i}$, and $i + j \neq j - i$ in \mathbb{Z}_n . On the other hand, if $2i = 0$ in \mathbb{Z}_n , then the above calculation shows that R_i commutes with F_j , and we also have $R_i R_j = R_j R_i = R_{i+j}$, so $R_i \in Z(D_n)$.

Thus $Z(D_n) = \{R_i \mid 2i \equiv 0 \pmod{n}\}$. To make this more explicit, we note that when n is odd, $2i = 0$ in \mathbb{Z}_n only when $i = 0$. If n is even, then $2i = 0$ in \mathbb{Z}_n for $i = 0$ and $i = n/2$.

Conclusion: if n is odd, then $Z(D_n) = \{R_0\}$; while if n is even, then $Z(D_n) = \{R_0, R_{n/2}\}$.

Fraleigh 6.32:

- a) True: any cyclic group has a generator a , and $a^m a^n = a^n a^m = a^{m+n}$.
- b) False: the Klein 4-group V_4 is abelian but not cyclic.
- c) False. Suppose $\mathbb{Q} = \langle a \rangle$. Note that $\langle a \rangle$ is the set of integer multiples of a . We can't have $a = 0$ since then $\langle a \rangle = \{0\}$, and we can't have $a \neq 0$ since then $a/2 \in \mathbb{Q}$ but $a/2 \notin \langle a \rangle$, a contradiction.
- d) False. 2 doesn't generate \mathbb{Z}_4 . 0 doesn't generate \mathbb{Z}_n for any $n > 1$.
- e) True. For any positive integer n , \mathbb{Z}_n is an abelian group of order n .
- f) False, see (b).
- g) False. 9 is a generator of \mathbb{Z}_{20} which is not prime. (The statement doesn't quite make sense anyway, because strictly speaking a generator of \mathbb{Z}_{20} is an element of \mathbb{Z}_{20} , not an integer. In general you should be careful to distinguish between integers and their equivalence classes mod n , whenever it is not clear from context what you mean.)
- h) False. G and G' might not intersect at all (so that $G \cap G'$ contains no identity element), and even if they do intersect, $G \cap G'$ may not have a well-defined binary operation on it (e.g. the group operations on G and G' might not agree on $G \cap G'$), so it doesn't even make sense to ask whether or not $G \cap G'$ is a group.
- i) True, by section 5 exercise 54.

j) True. Any finite cyclic group of order > 2 is isomorphic to \mathbb{Z}_n where $n > 2$, and 1 and -1 are both generators of \mathbb{Z}_n which are distinct by our assumption that $n > 2$. (For most n there are lots of other generators too.) Any infinite cyclic group is isomorphic to \mathbb{Z} which also has 1 and -1 as generators.