Selected exercises from Abstract Algebra by Dummit and Foote (3rd edition).

Bryan Félix

Abril 12, 2017

Section 2.1

Exercise (6). Let $G$ be an abelian group. Prove that $T = \{ g \in G | |g| < \infty \}$ is a subgroup of $G$. Give an explicit example where this set is not a subgroup when $G$ is non-abelian.

Proof.

i. $T$ is non-empty. The identity $i$ of $G$ is an element of $T$.

ii. $T$ is closed under inverses. If $x \in T$ then there exist $n < \infty$ such that $x^n = i$. Then

\[
i = x^n
\]

\[
x^{-1} = x^n x^{-1}
\]

\[
(x^{-1})^n = (x^n x^{-1})^n
\]

\[
= ix^{-n} \quad \text{since } x \text{ commutes with itself}
\]

\[
= x^n x^{-n} \quad \text{since } x^n = i
\]

\[
= i
\]

This shows that $|x^{-1}| \leq n$ and therefore $x^{-1} \in T$.

iii. $T$ is closed under products. Take arbitrary $x$ and $y$ in $T$ and let $|x| = n$ and $|y| = m$. Then

\[
(xy)^{mn} = x^{mn} y^{mn} \quad \text{since } G \text{ is an abelian group}
\]

\[
= (x^n)^m (y^m)^n
\]

\[
= i^m i^n
\]

\[
= i
\]

Therefore $|xy| \leq mn$ and $xy \in T$

We conclude that $T$ is a subgroup.

Now we exhibit an example where $T$ fails to be a subgroup when $G$ is non-abelian.

Let $G = \langle x, y | x^2 = y^2 = i \rangle$. Observe that the product $xy$ has infinite order since the product $(xy)(xy)$ is no longer reducible because we lack the commutativity of $x$ with $y$. Hence, $x, y \in T$ but $(xy) \notin T$.

Exercise (7). Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is not a subgroup of this direct product.
Solution. It easy to see that the only element of finite order in \( \mathbb{Z} \) is the identity, viz. 0. Furthermore every element of \( \mathbb{Z}/n\mathbb{Z} \) has finite order (since \( \mathbb{Z}/n\mathbb{Z} \) is a finite group). Therefore the torsion group \( T \) of \( \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z}) \) is given by \( \{0\} \times \{0,1,\ldots,n-1\} \).

Now we show the second part of the problem. Observe that \((1,1)\) and \((-1,n)\) have infinite order. The product \((1,1) + (-1,0) = (0,1)\) however, has finite order \((|(0,1)| = n\). Hence, the proposed set is not a subgroup.

Section 2.2

Exercise (7). Let \( n \in \mathbb{Z} \) with \( n \geq 3 \). Prove the following:

a) \( C(D_{2n}) = \{1\} \) if \( n \) is odd.

b) \( C(D_{2n}) = \{1, r^{\frac{n}{2}}\} \) for \( n \) even.

Proof. Observe that elements of the form \( sr^i \) do not commute with \( r \) for \( 0 \leq i < n \). Multiplying on the left yields \((sr^i)r = (s)r^{i+1}\) and, on the other hand, right multiplication gives \(r(sr^i) = s(r^{i-1})\). These expressions are equal only if \( r^{i+1} = r^{i-1} \) or equivalently \( r^2 = 1 \) which is not the case (since \( n \geq 3 \)). Now we inspect elements of the form \( r^i \). Note that:

\[
\begin{align*}
r^i s &= sr^i \\
\iff sr^{-i} &= sr^i \\
\iff r^{-i} &= r^i \\
\iff 1 &= r^{2i} \\
\iff 1 &= (r^i)^2
\end{align*}
\]

The only element in \( D_{2n} \) with this property is \( r^{\frac{n}{2}} \) for even \( n \). It is left to check that for \( n \) even \( r^{\frac{n}{2}} \) commutes with \( sr^i \) for \( 0 \leq i < n \). Observe that:

\[
\begin{align*}
r^{\frac{n}{2}} (sr^i) &= (sr^i)r^{\frac{n}{2}} \\
\iff s(r^{\frac{n}{2}} r^i) &= s(r^i r^{\frac{n}{2}}) \\
\iff r^{\frac{n}{2}} r^i &= r^i r^{\frac{n}{2}} \\
\iff r^{\frac{n}{2}} &= r^{\frac{n}{2}} \quad \text{since powers of } r \text{ commute}
\end{align*}
\]

Which is true by construction of \( n \).

Exercise (10). Let \( H \) be a group of order 2 in \( G \). Show that \( N(H) = C(H) \). Deduce that if \( N(H) = G \) then \( H \leq C(G) \).

Proof. Since \( C(H) \leq N(H) \) it is only left to show that \( N(H) \subseteq C(H) \).

First, note that since \( |H| = 2 \), \( H = \{1, h\} \) where \( h \) is an element of order 2. Now let \( g \in N(H) \), then \( gHg^{-1} = H \). Since \( g1g^{-1} = 1 \), it must be the case that \( ghg^{-1} = h \). Therefore \( g \) commutes with \( H \) and \( g \in C(H) \) as desired. In particular if \( N(H) = G \) every element of \( G \) commutes with \( h \). Therefore \( h \in C(G) \) and hence \( H \leq C(G) \).
Section 2.3

Exercise (5). Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Solution. An element $z \in \mathbb{Z}/49000\mathbb{Z}$ is a generator of the group if and only if $\gcd(z, 49000) = 1$. Therefore we compute the number of relative prime numbers of 49000 by mean of the Euler $\phi$ function. i.e.

$$\phi(49000) = \phi(2^3 \cdot 5^3 \cdot 7^2) = (2^3 - 2^2)(5^3 - 5^2)(7^2 - 7) = 16800$$

Exercise (16). Assume $|x| = n$ and $|y| = m$. Suppose $x$ and $y$ commute. Prove that $|xy|$ divides the least common multiple of $m$ and $n$. Need this to be true if $x$ and $y$ do not commute?

Proof. Observe that $(xy)^{\text{lcm}(m,n)} = 1$. Why?! because

$$(xy)^{\text{lcm}(m,n)} = x^{\text{lcm}(m,n)}y^{\text{lcm}(m,n)} \quad \text{since } x \text{ and } y \text{ commute}$$

$$= 1 \cdot 1 \quad \text{since } n, m | \text{lcm}(n,m).$$

Therefore $|xy|$ divides $\text{lcm}(m,n)$ by Proposition 3. $\square$

Observe that this is not the case for elements that do not commute. We exhibited such a case at the end of problem 6 in section 2.1. Also, the order of $xy$ need not to be $\text{lcm}(m,n)$ take, for example, the subgroups $\langle r \rangle$ and $\langle r^2 \rangle$ in $D_{12}$. Clearly $|r| = 6$, $|r^2| = 3$, $\text{lcm}(6, 3) = 6$, but $|r \cdot r^2| = |r^3| = 2$.

Exercise (23). Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$.

Proof. We follow the hint and we exhibit two distinct subgroups of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ with order 2. For $n \geq 3$ take the subgroups generated by $2^n - 1$ and $2^{n-1} + 1$. It’s easy to see that the former has order 2 since $2^n - 1 \equiv -1 \mod 2^n$. For the latter note that

$$(2^{n-1} + 1)^2 \equiv (2^{n-1} + 1)(2^{n-1} + 1) \mod 2^n$$

$$\equiv 2^{2n-2} + 2^n + 1 \mod 2^n$$

$$\equiv 2^{2n-2} + 1 \mod 2^n$$

$$\equiv 1 \mod 2^n$$

since $2^n$ divides $2^{2n-2}$ for $n \geq 3$. Hence $\langle 2^{n-1} + 1 \rangle$ has order 2 as desired. $\square$

Section 2.4

Exercise (11). Prove that $SL_2(\mathbb{F}_3)$ and $S_4$ are two nonisomorphic groups of order 24.

Proof. Note that \[
\begin{pmatrix}
2 & 1 \\
0 & 2
\end{pmatrix}
\in SL_2(\mathbb{F}_3)
\] has order 6. However, the representative elements of $S_4$ (up to relabeling)

$$\begin{pmatrix}
1 \\
(12) \\
(12)(34) \\
(123) \\
(12)(34)
\end{pmatrix}$$

have orders 1, 2, 3, and 4. Thus $SL_2(\mathbb{F}_3)$ is not isomorphic to $S_4$. $\square$
Exercise (14).

A group \( H \) is called finitely generated if there is a finite set \( A \) such that \( H = \langle A \rangle \).

a) Prove that every finite group is finitely generated.

\textbf{Proof.} For a finite group \( G \) let \( A = G \). Then \( G = \langle A \rangle \).

\( \square \)

b) Prove that \( \mathbb{Z} \) is finitely generated.

\textbf{Proof.} Observe that \( \mathbb{Z} = \langle -1, 1 \rangle \).

\( \square \)

c) Prove that every finitely generated subgroup of the additive group \( \mathbb{Q} \) is cyclic.

\textbf{Proof.} Let \( H \) be a finitely generated subgroup of \( \mathbb{Q} \); i.e. \( H = \langle \pm \frac{p_1}{q_1}, \pm \frac{p_2}{q_2}, \ldots, \pm \frac{p_n}{q_n} \rangle \) where each \( p_i \) and \( q_i \) are elements of \( \mathbb{Z} \). Observe that \( \frac{p_i}{q_i} = \frac{p_i}{q_i q_2 \cdots q_n} \cdot \frac{q_i q_2 \cdots q_n}{q_i} \) where the latter factor is an element of \( \mathbb{Z} \). Therefore the group \( H \) is a subset (and a subgroup, by construction) of \( \langle \pm \frac{1}{q_i q_2 \cdots q_n} \rangle \). Since the latter is a cyclic group, it is isomorphic to \( \mathbb{Z} \). We have proved earlier that any subgroup of \( \mathbb{Z} \) is cyclic. Hence, \( H \) is a cyclic group.

\( \square \)

d) Prove that \( \mathbb{Q} \) is not finitely generated.

\textbf{Proof.} We proceed by contradiction. Assume \( \mathbb{Q} \) is finitely generated. Then, by the previous exercise \( \mathbb{Q} \) is cyclic and has a generator \( \frac{p}{q} \) where \( p, q \in \mathbb{Z} \). We will show that \( \frac{p}{q+1} \notin \langle \frac{p}{q} \rangle \).

If \( \frac{p}{q} \in \langle \frac{p}{q} \rangle \) then there exist \( z \in \mathbb{Z} \) such that \( z \frac{p}{q} = \frac{p}{q+1} \). Thus, we arrive at a contradiction.

\( \square \)

Exercise (15). Exhibit a proper subgroup of \( \mathbb{Q} \) which is not cyclic.

\textbf{Exhibit.} For any prime \( p \) let \( \tilde{Q}_p = \langle \frac{1}{p^r} | z \in \mathbb{Z} \rangle \). It is easy to check that \( \tilde{Q}_p \) is a group. Associativity is inherited form \( \mathbb{Q} \). The identity, namely 0, is a member of the set. Inverses have the form \( (-1) \cdot \frac{n}{p^r} \). Lastly, it is closed under addition \( \frac{n}{p^r} + \frac{m}{p^r} = \frac{np^r + np^r}{p^r} \).

Exercise (19). A nontrivial group is called divisible if for each element \( a \in A \) and each nonzero integer \( k \) there is an element \( x \in A \) such that \( x^k = a \), i.e., each element has a \( k^{th} \) root in \( A \).

a) Prove that the additive group of rational numbers, \( \mathbb{Q} \), is divisible.

\textbf{Proof.} For any non-zero integer \( k \) and any \( q \in \mathbb{Q} \) let \( q' = \frac{q}{k} \). Observe that \( q' \in \mathbb{Q} \) an that \( kq' = q \).

\( \square \)

b) Prove that no finite abelian group is divisible.

\textbf{Proof.} Observe that any element in a finite abelian group \( A \) has finite order. Let \( \{a_i\}_n \) be an enumeration of the elements in \( A \) and let \( d = \text{lcm}\{\|a_i\|^n\} \); i.e. the least common multiple of the order of all the elements in \( A \). We prove that no element (other than the identity) has a \( d \) root.

We proceed by contradiction. Let \( a \in A \) be a non-identity element, and assume there exist \( \tilde{a} \) such that \( \tilde{a}^d = a \). Since \( A \) is abelian, \( \tilde{a} \) has the form

\[
a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n}
\]

Therefore

\[
\tilde{a}^d = a_1^{dp_1} a_2^{dp_2} \cdots a_n^{dp_n}
\]

Since the order of any element divides \( d \) we have that \( a_i^{dp_i} = 1 \) for all \( i \). Hence \( \tilde{a}^d = 1 \), and we arrive at the much desired contradiction.

\( \square \)
Section 2.5

Exercise (8). In each of the following groups find the normalizer of each subgroup

a) $S_3$.  
*Solution.* For any of the subgroups generated by a permutation of length 2, the element $(1 2 3)$ does not preserve the group under conjugation, therefore the normalizer can not be the entire group $S_3$. Hence

\[
N(\langle (1 2) \rangle) = \langle (1 2) \rangle \\
N(\langle (1 3) \rangle) = \langle (1 3) \rangle \\
N(\langle (2 3) \rangle) = \langle (1 2) \rangle
\]

For the element $(1 2 3)$, we note that the conjugation by $(1 2)$ preserves the group. Therefore $(1 2) \in N(\langle (1 2 3) \rangle)$ and the only possible choice is that $N(\langle (1 2 3) \rangle) = S_3$.

b) $Q_8$.  
*Solution.* We easily check that conjugation by any of the elements $i, j, k$ preserves the group $\langle -1 \rangle$, therefore $N(\langle -1 \rangle) = Q_8$. Similarly we easily check that $i \in N(\langle j \rangle), j \in N(\langle k \rangle)$ and $k \in N(\langle i \rangle)$. Therefore

\[
N(\langle i \rangle) = N(\langle j \rangle) = N(\langle k \rangle) = Q_8.
\]