MODEL ANSWERS TO THE THIRD HOMEWORK

1. False. Let $G = D_3$, $H = \{I, F_1\}$ and $K = \{I, F_2\}$. Then H and K are both subgroups of G but the union

$$H \cup K = \{I, F_1, F_2\},$$

is not.
2. Chapter 2, Section 4: 1. (b) Concentric circles with centre the origin.
(c) The real line union ∞, where the number $m \in \mathbb{R} \cup \{\infty\}$ represents the slope.
3. In the notation of the first question from homework 2, there are eight subgroups of D_4, up to symmetries.

$$\{I\}, \{I, R^2\}, \{I, F_1\}, \{I, D_1\}, \{I, R, R^2, R^3\}, \{I, D_1, D_2, R^2\}, \{I, F_1, F_2, R^2\}, D_4.$$

D_4 has one left and one right coset, D_4 itself. At the other extreme the left and right cosets of $\{I\}$ are the eight one element subsets of D_4,

$$\{\, \{I\}, \{R\}, \{R^2\}, \{R^3\}, \{D_1\}, \{D_2\}, \{F_1\}, \{F_2\}\}.$$

The three subgroups of order 4 have one other coset (both left and right), the complement of the subgroup:

$$\{\, \{I, R, R^2, R^3\}, \{D_1, D_2, F_1, F_2\}\,\},$$
$$\{\, \{I, D_1, D_2, R^2\}, \{R, R^3, F_1, F_2\}\,\},$$
$$\{\, \{I, F_1, F_2, R^2\}, \{R, R^3, D_1, D_2\}\,\}.$$

Now we attack the three subgroups of order 2. We are looking for four subsets of order 2.
If we start with $H = \{I, R^2\}$ then we get the partition

$$\{\, \{I, R^2\}, \{R, R^3\}, \{D_1, D_2\}, \{F_1, F_2\}\},$$

regardless of whether we look at left or right cosets.
If we start with $H = \{I, F_1\}$ then we get the two partitions

$$\{\, \{I, F_1\}, \{R, D_1\}, \{R^2, F_2\}, \{R^3, D_2\}\} \qquad \text{and} \qquad \{\, \{I, F_1\}, \{R, D_2\}, \{R^2, F_2\}, \{R^3, D_1\}\}.$$

Finally, if we start with $H = \{I, D_1\}$ then we get the two partitions

$$\{\, \{I, D_1\}, \{R, F_2\}, \{R^2, D_2\}, \{R^3, F_1\}\} \qquad \text{and} \qquad \{\, \{I, D_1\}, \{R, F_1\}, \{R^2, D_2\}, \{R^3, F_2\}\}.$$

4. Chapter 2, Section 4: 9.

$$\begin{aligned}
[0] &= 0 + H = \{[0], [4], [8], [12]\} \\
[1] &= 1 + H = \{[1], [5], [9], [13]\} \\
[2] &= 2 + H = \{[2], [6], [10], [14]\} \\
[3] &= 3 + H = \{[3], [7], [11], [15]\}.
\end{aligned}$$

4. Chapter 2, Section 4: 10. Four.

4. Chapter 2, Section 4: 12. False. Consider $G = D_3$ and $H = \{I, F\}$. Then

$$RH = \{R, F_3\} \neq \{R^2, F_2\} = F_2H.$$

But

$$HR = \{R, F_2\} = HF_2.$$

4. Chapter 2, Section 4: 16. For every i, there is a unique b_i which is the inverse of a_i. Thus the elements of G are both $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$. Now

$$\begin{aligned}
x^2 &= (a_1a_2 \dots a_n)(a_1a_2 \dots a_n) \\
&= (a_1a_2 \dots a_n)(b_1b_2 \dots b_n) \\
&= (a_1b_1)(a_2b_2)(a_3b_3) \dots (a_nb_n) \\
&= e^n \\
&= e,
\end{aligned}$$

where we used the fact that G is abelian to rearrange these products.

4. Chapter 2, Section 4: 17. As $x^2 = e$ the order of x is either 1 or 2. If the order of G is odd it cannot be 2 by Lagrange. Thus the order of x is one. But then $x = e$.

4. Chapter 2, Section 4: 26. Define

$$f\colon S \longrightarrow T$$

by the rule

$$f(Ha) = a^{-1}H.$$

The key point is to check that f is well-defined. The problem is that if $b \in Ha$, then $Ha = Hb$ and we have to check that $Ha^{-1} = Hb^{-1}$. As $b \in Ha$, we have $b = ha$. But then $b^{-1} = a^{-1}h^{-1}$. As H is a subgroup $h^{-1} \in H$. But then $b^{-1} \in a^{-1}H$ so that $a^{-1}H = b^{-1}H$ and f is well-defined.

To show that f is a bijection, we will show that it has an inverse. Define

$$g\colon T \longrightarrow S$$

by the rule

$$g(aH) = Ha^{-1}.$$

We have to show that g is well-defined. This follows, exactly as in the proof that f is well-defined. Then $g(f(aH)) = g(Ha^{-1}) = aH$ and similarly fg is the identity. It follows that f is a bijection.
4. Chapter 2, Section 4: 27. Let $[a]_L$ denote the left-coset generated by a and let $[a]_R$ denote the right-coset generated by a. Suppose that $b \in [a]_L$. Then $[a]_L = [b]_L$ and so $aH = bH$. By assumption $Ha = Hb$. But then $[a]_R = [b]_R$ and so $b \in [a]_R$.
As b is an arbitrary element of $[a]_L$, it follows that $[a]_L \subset [a]_R$. In other words $aH \subset Ha$. Multiplying both sets on the right by a^{-1} we get the inclusion

$$aHa^{-1} \subset H.$$

Now this is valid for any $a \in G$, so that

$$bHb^{-1} \subset H.$$

for all $b \in G$. Take $b = a^{-1}$. Then

$$a^{-1}Ha \subset H,$$

so that multipying on the left by a, we get

$$Ha \subset aH.$$

Thus $Ha = aH$ and $aHa^{-1} = H$.
4. Chapter 2, Section 4: 29. We first prove that

$$ab^ja^{-1} = b^{ij}.$$

We proceed by induction on j. The case $j = 1$ follows by hypothesis. We have

$$\begin{aligned} ab^{j+1}a^{-1} &= a(bb^j)a^{-1} \\ &= (aba^{-1})(ab^ja^{-1}) \\ &= b^ib^{ij} \\ &= b^{i+ij} \\ &= b^{i(j+1)}. \end{aligned}$$

This completes the proof that

$$ab^ja^{-1} = b^{ij}.$$

Now we prove that if

$$a^rba^{-r} = b^{i^r}.$$

We proceed by induction on r. The case $r = 1$ follows by hypothesis. We have

$$\begin{aligned} a^{r+1}ba^{-r-1} &= a(a^r ba^{-r})a^{-1} \\ &= a(b^{i^r})a^{-1} \\ &= b^{i^r \cdot i} \\ &= b^{i^{r+1}}. \end{aligned}$$

4. Chapter 2, Section 4: 30. We have

$$\begin{aligned} b &= a^5 ba^{-5} \\ &= b^{2^5} \\ &= b^{32}. \end{aligned}$$

It follows that

$$b^{31} = e.$$

Thus the order of b divides 31. As 31 is prime this means the order is either 1 or 31. But if the order is one then $b = e$, which we are supposing does not happen.
Thus the order of b is 31.
5. **Challenge Problems** Chapter 2, Section 4: 43.
We have already seen that the set H of elements of G whose square is the identity is a subset of G. If $a \in G \setminus H$ then the inverse of a is also an element of $G \setminus H$, distinct from a. Thus we may assume that a_1 and b_1, a_2 and b_2, ..., a_m and b_m are inverses of each other, where $a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_m$ are all the elements of $G \setminus H$.
In this case

$$\begin{aligned} a_1 a_2 \dots a_{n-2} &= (a_1 a_2 \dots a_m)(b_1 b_2 \dots b_m) \\ &= (a_1 b_1)(a_2 b_2)(a_3 b_3) \dots (a_m b_m) \\ &= e^m \\ &= e. \end{aligned}$$

Let y be the product of the elements of H. Then

$$\begin{aligned} x &= a_1 a_2 \dots a_n \\ &= ey \\ &= y. \end{aligned}$$

Replacing G by H we may therefore assume that the square of every element of H is the identity.
(a) In this case $G = \{e, b\}$ and so

$$x = be = b.$$

(b) We show that G contains a subgroup of index 2.
Let H be any subgroup of G. Suppose that the index of H is not two. Then H has at least three left cosets. Pick a left coset aH that does not contain either e or x. Consider the union K of H and aH.
I claim that K is a subgroup of G. It is certainly non-empty and is it certainly finite. We just need to prove it is closed under products.
Suppose that u and v belong to K. If u and v belong to H then the product belongs to H and so the product certainly belongs to K. Suppose that u belongs to H and v belongs to K. Then $v = ah$, where $h \in H$. But then the product

$$\begin{aligned} uv &= u(ah) \\ &= a(uh) \in aH \end{aligned}$$

belongs to aH, so that is certainly belongs to K. Finally suppose that u and v both belong to aH. Then $u = ah$ and $v = ak$, where h and $k \in H$. In this case

$$\begin{aligned} uv &= (ah)(ak) \\ &= a^2(hk) \\ &= hk \in H, \end{aligned}$$

belongs to H, so that it certainly belongs to K.
Thus K is a subgroup of G. It is then clear that any maximal (with respect to inclusion) proper subgroup H of G has index 2.
Pick $a \notin H$. Then the left cosets of H are H and aH. As we are supposing that G has at least three elements, H has order m greater than one. As every element of H squares to the identity, m is even by Lagrange.
Let y be the product of the elements of H. Then the product of the elements of aH is $a^m y = y$, as m is even and $a^2 = e$. But then the product of the elements of G is

$$x = y^2 = e.$$

(c) As $x^2 = e$, x has order 1 or 2. If n is odd then the order is not 2. Thus the order of x is one and so $x = e$.
6. **Challenge Problems** Consider the rational numbers under addition. $\mathbb{Q}$ is certainly countable. Suppose that $g_1, g_2, \dots, g_k$ were a finite set of generators. Each g_i is a rational number, say of the form $\frac{a_i}{b_i}$. Now let b be the least common multiple of the $b_1, b_2, \dots, b_k$. Then any element which is a finite sum or difference of the $g_1, g_2, \dots, g_k$ will be of the form $\frac{a}{b}$, for some integer a. But most rationals are not of this form. Thus $\mathbb{Q}$ is not finitely generated.