Problem 1: 2.52i,vii,ix
Let $G$ be a group. Are the following statements true or false, justify.

i. If $H$ is a subgroup of $K$ and $K$ is a subgroup of $G$, then $H$ is a subgroup of $G$.

Solution: By 2.68, given $x, y \in H$, then $xy^{-1} \in H$. Since inverses in $K$ must be inverses in $G$ and $G, K$ have the same operation, then $xy^{-1} \in H$ still when considered in $G$. Hence $H \leq G$ by 2.68.

vii. The intersection of two cyclic subgroup of $G$ is a cyclic subgroup.

Solution: True:
Proof. Let $H, K$ be cyclic subgroups of a group $G$. Then $H \cap K$ is again a subgroup of $G$. By proposition 2.75, every subgroup of a cyclic group is cyclic, so $H \cap K$ is cyclic. \[\square\]

ix. If $X$ is an infinite set, then:

$$F = \{\sigma \in S_X : \sigma \text{ moves only finitely many elements of } X\}$$

is a subgroup of $S_X$.

Solution: True.

Proof. Suppose $\sigma, \tau \in F$. Let $x \in X$ such that $\sigma, \tau$ fix $x$. Then $\sigma \tau(x) = x$. If $F_\sigma$ is the fixed set$^1$ of $\sigma$ and $F_\tau$ is the fixed set of $\tau$. There are only finitely many elements of $X$ which are not in $F_\sigma$ or $F_\tau$, so all but finitely many elements of $X$ are in $F_\sigma$ and $F_\tau$ because $X$ is infinite. As we showed before, every element of $F_\sigma \cap F_\tau$ is fixed by $\sigma \tau$, so $\sigma \tau \in F$.

Suppose $\sigma \in F$. If $\sigma(x) = x$, then $\sigma^{-1}(x) = x$. Hence the fixed set of $\sigma$ is contained in the fixed set of $\sigma^{-1}$, so $\sigma^{-1}$ fixes all but finitely many elements of $X$. Thus $\sigma^{-1} \in F$. We have shown that $F$ is closed under the group operation of $S_X$ and $F$ is closed under inversion, so $\sigma \sigma^{-1} = 1 \in F$ as well. Thus $F \leq S_X$ as desired. \[\square\]

Problem 2: 2.56
Let $G$ be a finite group with subgroups $H, K$. If $H \leq K$, prove that $|G : H| = |G : K||K : H|$.

Proof. By corollary 2.84:

$$|G : H| = \frac{|G|}{|H|} \quad |G : K| = \frac{|G|}{|K|} \quad |K : H| = \frac{|K|}{|H|}$$

Multiply $|G : K||K : H| = \frac{|G|}{|H|}$ and the identity is verified. \[\square\]

$^1$ i.e. $\{x \in X : \sigma(x) = x\}$
Problem 3: 2.57
If $H, K$ are subgroups of a group $G$ and if $|H|, |K|$ are relatively prime, prove that $|H \cap K| = 1$.

Proof. Observe that $H \cap K$ is a subgroup of $G$ by proposition 2.76. Then $H \cap K$ must also be a subgroup of $H, K$. Lagrange's theorem says that $|H \cap K|$ divides $|H|, |K|$. Since $|H|, |K|$ are relatively prime, their only common non-zero divisor is 1, so $|H \cap K| = 1$. □

Problem 4: 2.68
Prove a group $G$ is abelian if and only if the map $f : G \rightarrow G$ defined by $f(a) = a^{-1}$ is a group homomorphism.

Proof. Suppose $G$ is abelian and let $a, b \in A$. Then $f(ab) = b^{-1}a^{-1} = f(b)f(a) = f(a)f(b)$ since $G$ is abelian. Thus $f$ is a group homomorphism.

Conversely suppose that $f$ is a homomorphism. Observe that $b^{-1}a^{-1} = f(ab) = f(a)f(b) = a^{-1}b^{-1}$. Inverting both sides, we obtain $ab = ba$, so $G$ is abelian. □

Problem 5: 2.75
If $G$ is a group and $a, b \in G$, prove that $ab$ and $ba$ have the same order.

Proof. Observe that:

$$ba = a^{-1}(ab)a$$

i.e. $ba$ is a conjugate of $ab$. Thus by proposition 2.94, they have the same order (conjugate elements have the same order). □

Problem 6: 2.76
Prove the following:

i. Let $f : G \rightarrow H$ be a homomorphism and $x \in G$ have order $k$. Prove that $f(x) \in H$ has order $m$ where $m|k$.

Proof. Observe first that if $(f(x))^k = f(x^k) = f(1) = 1$, so $f(x)$ has finite order $\leq k$. Let $m = |f(x)|$ and suppose that $m \nmid k$. Then there exists a non-zero remainder $r \in \mathbb{Z}$, $0 < r < k$ such that $k = qm + r$ for some $q \in \mathbb{Z}$. Thus $f(x)^k = (f(x)^m)^q f(x)^r = f(x)^r$ because $f(x)^m = 1$, but $f(x)^r \neq 1$ because $r < k < |f(x)|$, so we have a contradiction to the fact that $f(x)^k = 1$. Thus $m|k$. □

ii. Show that if $|G|, |H|$ are relatively prime, then the image of $f$ is trivial.
Proof. Let \( x \in G \) so that \( f(x) \in H \) is an arbitrary element of the image of \( f \). Observe that \( \langle x \rangle \leq G \), so \( |x| = |\langle x \rangle| \) divides \( |G| \) by Lagrange’s theorem. By the preceding part, \( |f(x)| \) divides \( |x| \), so \( |f(x)| \) divides \( |G| \).

On the other hand, \( (f(x)) \leq H \), so \( |f(x)| \) divides \( |H| \) by Lagrange’s theorem. Therefore \( |f(x)| \) divides both \( |G|, |H| \), so \( |f(x)| = 1 \) because \( |G|, |H| \) are relatively prime so that their only common divisor is 1. Thus \( f(x) = 1 \) because only the identity element has order 1. □

Problem 7:
Let \( G \) be an abelian group and \( f : S_3 \to G \) a homomorphism. Prove that \( \text{Im } f \leq 2 \).

Proof. Observe that if \( G \) is abelian with \( a, b \in G \), then \( ab = ba \iff aba^{-1}b^{-1} = 1_G \).\(^2\) Hence if \( x \in S_3 \) is of the form \( x = \alpha\beta\alpha^{-1}\beta^{-1} \) for \( \alpha, \beta \in S_3 \), we see that:
\[
f(\alpha\beta\alpha^{-1}\beta^{-1}) = f(\alpha)f(\beta)f(\alpha)^{-1}f(\beta)^{-1} = 1_G
\]
by properties of a homomorphism and the above mentioned property of the abelian group \( G \).

Observe now that:
\[
\]
so by the preceding, \( (123), (132) \in \ker f \) and that \( (1) \in \ker f \) by default, so \( |\ker f| = 3 \). At this point, you can check that \( (12)(123) = (23) \) and \( (12)(132) = (13) \) so that \( f(12) = f(23) \) and \( f(12) = f(13) \) because \( (123), (132) \in \ker f \) and applying the properties of a homomorphism, so \( \text{Im } f \) consists exactly of \( \{1, f(12)\} \) which means that it must contain at most 2 elements.

A more elegant, motivated solution uses the first isomorphism theorem (2.116) which states that:
\[
\text{Im } f \cong S_3/\ker f
\]
so that by a corollary to Lagrange’s theorem:
\[
|\text{Im } f| = |S_3|/|\ker f| = 6/|\ker f| \leq 2
\]
because \( |\ker f| \geq 3 \). □

\(^2\)Note that we are using \( 1_G \) to explicitly identify the identity in \( G \).