Solutions to Homework #6

1. [Not from Saracino, but useful on the next problem]
Let G be a group, let $H \subseteq G$ be a subgroup, and let $x \in G$. If $x \in H$, prove that $\langle x \rangle \subseteq H$.

Proof. Given $y \in \langle x \rangle$, there is some integer $n \in \mathbb{Z}$ such that $y = x^n$. Whether n is positive, negative, or zero, the fact that H is closed under multiplication and inverses (and contains the identity) implies that $x^n \in H$. QED

---

2. Saracino, Section 5, Problem 5.5(a): Find all the subgroups of Q_8.
Find all the subgroups of Q_8. Make sure to explain why each set in your list actually is a subgroup, **and** prove that your list must be complete.

You may assume the following fact: that all the subgroups of Q_8 have order dividing 8, i.e., order 1, 2, 4, or 8. (This is due an upcoming result known as **Lagrange's Theorem**.)

Answer/Proof. I claim that the following is a complete list of subgroups of $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$:

$$\boxed{Q_8, \quad \langle 1 \rangle = \{1\}, \quad \langle -1 \rangle = \{1, -1\}, \quad \langle i \rangle = \langle -i \rangle = \{\pm 1, \pm i\},}$$

$$\boxed{\langle j \rangle = \langle -j \rangle = \{\pm 1, \pm j\}, \quad \langle k \rangle = \langle -k \rangle = \{\pm 1, \pm k\}}$$

Certainly each of the sets listed above is a subgroup, as each is either the subgroup generated by some element or else the improper subgroup Q_8 itself. So it suffices to show that any subgroup of Q_8 does indeed appear above.
Given a subgroup $H \subseteq Q_8$, by Lagrange's Theorem, we must have $|H| = 1, 2, 4$, or 8.
If $|H| = 8$, then H contains all 8 elements of Q_8, so $H = Q_8$.
For the rest of the proof, then, we may assume $|H|$ is 1, 2, or 4.
If $i \in H$, then by Problem 1, H contains $\langle i \rangle = \{\pm 1, \pm i\}$, which is already 4 elements. So $H = \langle i \rangle$.
Similarly, if $-i \in H$, then by Problem 1, H contains $\langle -i \rangle = \langle i \rangle = \{\pm 1, \pm i\}$, which is already 4 elements. So again, $H = \langle i \rangle$.
Similarly, if either $j \in H$ or $-j \in H$, then $H = \langle j \rangle = \langle -j \rangle$.
And if either $k \in H$ or $-k \in H$, then $H = \langle k \rangle = \langle -k \rangle$.
If none of the above happen, then $\pm i, \pm j, \pm k \notin H$, so $H \subseteq \{\pm 1\}$.
Since H is a subgroup, however, it must contain the identity element 1. Hence, we have either $H = \{1\}$ (the trivial subgroup) or $H = \{\pm 1\}$, which is the subgroup $\langle -1 \rangle$. QED

---

3. Saracino, Section 5, Problem 5.7: Let $G = \langle x \rangle$ be a cyclic group of order n. Show that for any integer $m \in \mathbb{Z}$, the element x^m is a generator of G if and only if $(m, n) = 1$.

Proof. ($\Rightarrow$): Since x^m generates G, we have $\langle x^m \rangle = G$, so in particular $|\langle x^m \rangle| = |G| = n$. However, by Theorem 4.5 we have $|\langle x^m \rangle| = o(x^m)$, and by Theorem 4.4(iii), we have $o(x^m) = n/(m, n)$.
That is, $n = |G| = |\langle x^m \rangle| = o(x^m) = n/(m, n)$. Thus, $(m, n) = 1$.

($\Leftarrow$): Again by Theorems 4.5 and 4.4(iii), we have $|\langle x^m \rangle| = o(x^m) = n/(m, n) = n$, where the last equality is by the assumption that $(m, n) = 1$. Thus, $\langle x^m \rangle$ is a subgroup of G of order n, and hence it must contain all n elements of G. That is, $\langle x^m \rangle = G$, or equivalently, x^m generates G. QED

---

4. Saracino, Section 5, Problem 5.8: Let $G = \langle x \rangle$ be a cyclic group of order 144. How many elements are there in the subgroup $\langle x^{26} \rangle$?

Solution. Observe that 26 has prime factorization $26 = 2 \cdot 13$ and $13 \nmid 144$, so that $(144, 26) = 2$.

Since $o(x) = |\langle x \rangle| = |G| = 144$, Theorem 4.4(iii) tells us that $o(x^{26}) = \dfrac{144}{(144, 26)} = \dfrac{144}{2} = 72$.

By Theorem 4.5, then, the subgroup $\langle x^{26} \rangle$ contains exactly $\boxed{72 \text{ elements}}$

---

5. Saracino, Section 5, Problem 5.11: Let G be an abelian group, and let $n \geq 1$ be a positive integer. Let $H = \{x \in G \,|\, x^n = e\}$. Prove that H is a subgroup of G.

Proof. [Clearly $H \subseteq G$.]
(**Nonempty**). We have $e^n = e$, so $e \in H$.
(**Closure**). Given $x, y \in H$, we have $(xy)^n = x^n y^n = ee = e$, where the first equality is because G is abelian. Thus, $xy \in H$.
(**Inverses**). Given $x \in H$, we have $(x^{-1})^n = x^{-n} = (x^n)^{-1} = e^{-1} = e$. Thus, $x^{-1} \in H$. QED

[**Note**: In the Closure step, technically we need induction on n to show that $(xy)^n = x^n y^n$ for every $n \geq 1$, but never mind. On the other hand, it's important to say explicitly that we are using the abelian hypothesis to deduce this equality.]

---

6. Saracino, Section 5, Problem 5.14: Let H, K be subgroups of a group G. Prove that $H \cap K$ is also a subgroup of G.

Proof. [Clearly $H \cap K \subseteq H \subseteq G$.]
Nonempty: We have $e \in H$ and $e \in K$, because they are subgroups. Thus, $e \in H \cap K$.
Closure: Given $x, y \in H \cap K$, then $x, y \in H$, so $xy \in H$ because H is a subgroup. Similarly, $xy \in K$, since K is a subgroup. Thus, $xy \in H \cap K$.
Inverses: Given $x \in H \cap K$, then $x \in H$, so $x^{-1} \in H$ because H is a subgroup. Similarly, $x^{-1} \in K$, since K is a subgroup. Thus, $x^{-1} \in H \cap K$. QED