Solutions to Homework #3

1. Saracino, Section 3, Problem 3.9: Let $(G, *)$ be a group. Prove that $(G, *)$ is abelian if and only if:

$$(x * y)^{-1} = x^{-1} * y^{-1} \quad \text{for all } x, y \in G.$$

Proof. ($\Rightarrow$) Given $x, y \in G$, we have $(x * y)^{-1} = (y * x)^{-1} = x^{-1}y^{-1}$, where the first equality is by the assumption that G is abelian, and the second is by Theorem 3.4.

($\Leftarrow$) Given $x, y \in G$, then $x^{-1}, y^{-1} \in G$, so by hypothesis we have

$$\left(x^{-1} * y^{-1}\right)^{-1} = \left(x^{-1}\right)^{-1} * \left(y^{-1}\right)^{-1} = x * y.$$

However, by Theorem 3.4, the left side above is

$$\left(x^{-1} * y^{-1}\right)^{-1} = \left(y^{-1}\right)^{-1} * \left(x^{-1}\right)^{-1} = y * x.$$

Combining the two above equations, we have $x * y = y * x$. QED

---

2. Saracino, Section 3, Problem 3.11: Let $(G, *)$ be a group such that $x^2 = e$ for all $x \in G$. Prove that G is abelian.

Proof. Given $x, y \in G$, we have $x * y \in G$, so by hypothesis we have $(x * y)^2 = e$, i.e., $(x * y) * (x * y) = e$. Multiply this equation on the left by x and on the right by y, and we get

$$\Big(x * \big((x * y) * (x * y)\big)\Big) * y = (x * e) * y.$$

Applying associativity on the LHS and the identity axiom on the RHS, we get

$$\big((x * x) * (y * x)\big) * (y * y) = x * y.$$

But by hypothesis, we have $x * x = e$ and $y * y = e$, so the above equation becomes $\big(e * (y * x)\big) * e = x * y$, i.e., $y * x = x * y$. QED

---

3. Saracino, Section 3, Problem 3.12: Let $(G, *)$ be a group. Prove that G is abelian if and only if $(x * y)^2 = x^2 * y^2$ for all $x, y \in G$.

Proof. ($\Rightarrow$) Given $x, y \in G$, we have

$$(x * y)^2 = (x * y) * (x * y) = x * (y * x) * y = x * (x * y) * y = (x * x) * (y * y) = x^2 * y^2,$$

where the second and fourth equalities are by associativity, and the third is by our assumption that G is abelian.

($\Leftarrow$) Given $x, y \in G$, we have $x*(y*x)*y = (x*y)*(x*y) = (x*y)^2 = x^2*y^2 = (x*x)*(y*y) = x*(x*y)*y$, where the first and fifth equalities are by associativity, and the third is by assumption. Multiplying on the left by x^{-1} and on the right by y^{-1}, we get $e*(y*x)*e = e*(x*y)*e$, and hence $y*x = x*y$. QED

---

4. Saracino, Section 4, Problem 4.8: It is a fact [which you may assume without proof] that the set $2\mathbb{Z}$ of even integers forms a group under addition. Is this group cyclic? Prove or disprove.

Answer/Proof. YES

In fact, we claim $2\mathbb{Z}$ is generated by 2. That is, we must prove the set equality $2\mathbb{Z} = \langle 2 \rangle$. Here goes:

($\subseteq$): Given $x \in 2\mathbb{Z}$, we have $x = 2m$ for some $m \in \mathbb{Z}$ [by definition of $2\mathbb{Z}$; or, if you like, by the definition of "even integer"]. Then $x = 2m = m2 \in \langle 2 \rangle$. QED ($\subseteq$)

($\supseteq$): Given $x \in \langle 2 \rangle$, we have $x = n2$ for some $n \in \mathbb{Z}$. Therefore, $x = 2n \in 2\mathbb{Z}$. QED

[**Note**: -2 is also a generator; that is, $2\mathbb{Z} = \langle -2 \rangle$. No other element of $2\mathbb{Z}$ is a generator, though.]

---

5. Saracino, Section 4, Problem 4.9: Prove that the group $(\mathbb{Q}_{>0}, \cdot)$ is not cyclic.

[**Note**: there are several ways to prove this. Here are two.]

Proof 1. Suppose $a \in \mathbb{Q}^+$ is a generator. Then there are integers $m, n \geq 1$ such that $a = m/n$ and such that $(m, n) = 1$. Let p be a prime number not dividing m or n; for example, take p to be any prime divisor of $mn + 1 \geq 2$. Note $p \in \mathbb{Q}_{>0}$. We'll show that $p \notin \langle a \rangle$, thus giving a contradiction.

If $p \in \langle a \rangle$, then there is an integer $k \in \mathbb{Z}$ such that $m^k/n^k = p$. If $k = 0$, that means $p = 1$, a contradiction. If $k \geq 1$, then $m^k = pn^k$, so $p|m^k$, and hence $p|m$, contradicting our choice of p. Finally, if $k \leq -1$, then $n^{-k} = pm^{-k}$, and by the same reasoning we get $p|n$, another contradiction. QED

Proof 2. Suppose $a \in \mathbb{Q}_{>0}$ is a generator. If $a = 1$, then $\langle a \rangle = \{1\} \subsetneq \mathbb{Q}^+$ (for example, $2 \in \mathbb{Q}^+ \smallsetminus \{1\}$), a contradiction. Thus, we may assume $a \neq 1$.
If $a > 1$, pick a rational number b such that $1 < b < a$. (For example, let $b = (a+1)/2$.) Then for any integer $k \geq 1$, we have $a^k \geq a > b$, so $b \neq a^k$. On the other hand, for any integer $k \leq 0$, we have $a^k \leq 1 < b$, so again, $b \neq a^k$. Thus, $b \notin \langle a \rangle$, giving our contradiction.
If $a < 1$, let $b = (a+1)/2$ again, so that $a < b < 1$. The proof in this case is similar to the previous paragraph. QED

---

6. [Not from Saracino, but may be useful on HW 4.]
Fix a positive integer $n \geq 1$. Let $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ be integers such that $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$. Prove that $x_1 y_1 \equiv x_2 y_2 \pmod{n}$.

Proof. By hypothesis, there are integers $s, t \in \mathbb{Z}$ such that

$$x_1 - x_2 = xn \qquad \text{and} \qquad y_1 - y_2 = tn.$$

Thus,

$$x_1y_1 - x_2y_2 = x_1y_1 - x_1y_2 + x_1y_2 - x_2y_2 = x_1(y_1 - y_2) + (x_1 - x_2)y_2 = x_1(tn) + (sn)y_2 = (tx_1 + xy_2)n.$$

Since $tx_1 + xy_2 \in \mathbb{Z}$, this means that $x_1 y_1 \equiv x_2 y_2 \pmod{n}$. QED

---

7. [Not from Saracino, but may be useful on HW 4.]
Let G be a group, and let $a, x \in G$. Use induction to prove that for any integer $n \geq 1$, we have $(xax^{-1})^n = xa^n x^{-1}$.

Proof. **Base Case**: For $n = 1$, we have $(xax^{-1})^1 = xax^{-1} = xa^1x^{-1}$.

Inductive Step: Given the statement for a particular n, we have

$$(xax^{-1})^{n+1} = (xax^{-1})^n(xax^{-1}) = xa^nx^{-1}xax^{-1} = xa^nax^{-1} = xa^{n+1}x^{-1},$$

proving the statement for $n + 1$. QED

[**Note**: This is actually true for *all* integers n, not just $n \geq 1$. One way to prove it for $n \leq 0$ is by "backwards" induction (given it's true for n, prove it for $n - 1$). Another way is to prove that for any $c \in G$, $(xcx^{-1})^{-1} = xc^{-1}x^{-1}$. (By Theorem 3.4, for example.) So then for any $n \leq -1$, we have $(xax^{-1})^n = [(xax^{-1})^{-n}]^{-1} = [xa^{-n}x^{-1}]^{-1} = xa^nx^{-1}$. Finish by proving the formula by hand for $n = 0$.]