Solutions to Homework #16

1. Saracino, Section 13, Problem 13.14: Let G, H be finite groups, and let $\varphi : G \to H$ be an onto homomorphism. Prove that $|H|$ divides $|G|$.

Proof. Let $K = \ker\varphi \lhd G$. By the Fundamental Theorem, we have $G/K \cong H$, and hence $|H| = [G : K]$. Therefore, by Lagrange, we have $|G| = |K| \cdot [G : K] = |K| \cdot |H|$, and hence $|H|$ divides $|G|$. QED

---

2. Saracino, Section 13, Problem 13.19: Let $\varphi : G \to K$ be a homomorphism. Prove that φ is one-to-one if and only if $\ker(\varphi) = \{e_G\}$.

Proof. ($\Rightarrow$): ($\supseteq$): We have $\varphi(e_G) = e_H$, and hence $e_G \in \ker(\varphi)$.
($\subseteq$): Given $x \in \ker(\varphi)$, we have $\varphi(x) = e_H = \varphi(e_G)$, and hence $x = e_G$ since φ is 1-1.
($\Leftarrow$): Given $g, h \in G$ with $\varphi(g) = \varphi(h)$, we have $\varphi(g)[\varphi(h)]^{-1} = e_H$, and hence $\varphi(gh^{-1}) = e_H$. Thus, $gh^{-1} \in \ker(\varphi) = \{e_G\}$ and hence $gh^{-1} = e_G$. That is, $g = h$. QED

---

3. Saracino, Section 13, Problem 13.5: Let G be the group of all real-valued functions on the real line, under addition of functions. Let $H = \{f \in G \,|\, f(0) = 0\}$.

(a) Prove that $H \lhd G$.

(b) Prove that $G/H \cong \mathbb{R}$.

Proof. Define $\varphi : G \to \mathbb{R}$ by $\varphi(f) = f(0)$.
(Homom): Given $f, g \in G$, we have $\varphi(f + g) = (f + g)(0) = f(0) + g(0) = \varphi(f) + \varphi(g)$.
(Onto): Given $y \in \mathbb{R}$, define $f(x) = y$ (the constant function with value y).
Then $f \in G$, and $\varphi(f) = f(0) = y$.
(Kernel): We have $\ker(\varphi) = \{f \in G \,|\, \varphi(f) = 0\} = \{f \in G \,|\, f(0) = 0\} = H$.
(a): By the above, we have $H = \ker(\varphi) \lhd G$ by Theorem 13.1.
(b): By the above, we have $G/H = G/\ker(\varphi) \cong \mathbb{R}$ by the Fundamental Theorem (Theorem 13.2). QED

---

4. (A useful fact for the next problem): Let $G = \mathbb{Q}^\times$, and let $H = \{a/b \,|\, a, b \text{ are odd integers}\}$. Prove that for every $x \in G$, there exist unique numbers $k \in \mathbb{Z}$ and $h \in H$ such that $x = 2^k h$.

Proof. We begin with an observation: For any nonzero integer $c \in \mathbb{Z} \smallsetminus \{0\}$, let $\ell \geq 0$ be the largest integer such that $2^\ell | c$. Then $c = 2^\ell a$, where $a \in \mathbb{Z}$ is an odd integer.
[Equivalently, factor c into primes $c = \pm 2^{e_1} p_2^{e_2} \cdots p_M^{e_M}$, where $p_2, \ldots, p_M \geq 3$ are odd primes. Then we are defining $\ell = e_1 \geq 0$ and $a = \pm p_2^{e_2} \cdots p_M^{e_M}$.]

(Existence): Given $x \in G = \mathbb{Q}^\times$, we can write $x = m/n$, where $m, n \in \mathbb{Z} \smallsetminus \{0\}$ are nonzero integers. Applying the observation above to both m and n, there are positive integers $i, j \geq 0$ and odd integers $a, b \in \mathbb{Z}$ such that $m = 2^i a$ and $n = 2^j b$.
Let $k = i - j \in \mathbb{Z}$, and let $h = a/b \in H$. Then $x = m/n = 2^k h$. QED Existence

(Uniqueness): Given $x \in G$, suppose we have $x = 2^k \dfrac{a}{b} = 2^\ell \dfrac{c}{d}$ with $k, \ell, a, b, c, d \in \mathbb{Z}$ with a, b, c, d odd.
Assume without loss that $k \geq \ell$.
Then we have $2^{k-\ell} ad = bc$, with both sides being integers. Since bc is an odd integer, the left side must also be odd, and hence $k - \ell = 0$. That is, $k = \ell$.
It follows that $\dfrac{a}{b} = \dfrac{c}{d}$ is the same element of H, as desired. QED

---

5. Saracino, Section 13, Problem 13.8: Let $G = \mathbb{Q}^\times$, and let $H = \{a/b \,|\, a, b \text{ are odd integers}\}$. [You may take my word for it that H is a subgroup of G.] Prove that $G/H \cong \mathbb{Z}$.

Proof. Define $\varphi : \mathbb{Q}^\times \to \mathbb{Z}$ by $\varphi\big(2^k h\big) = k$, for any $k \in \mathbb{Z}$ and $h \in H$.
By the previous problem, this formula for φ is both defined and well-defined, as each $g \in G$ may be written in one and only one way as $2^k h$ with $k \in \mathbb{Z}$ and $h \in H$.

φ **Homom:** Given $x, y \in \mathbb{Q}^\times$, we may write $x = 2^k h_1$ and $y = 2^\ell h_2$ by the previous problem, with $k, \ell \in \mathbb{Z}$ and $h_1, h_2 \in H$. Thus,

$$\varphi(xy) = \varphi\big(2^{k+\ell} h_1 h_2\big) = k + \ell = \varphi\big(2^k h_1\big) + \varphi\big(2^\ell h_2\big) = \varphi(x) + \varphi(y),$$

where the second equality is because $h_1 h_2 \in H$, since H is a subgroup of G.
[Note that the operation on $\mathbb{Q}^\times$ is multiplication, whereas the operation on $\mathbb{Z}$ is $+$, so the above is indeed the correct identity to look for.]

φ **onto:** Given $n \in \mathbb{Z}$, then $2^n \in \mathbb{Q}^\times$, and $\varphi(2^n) = \varphi(2^n \cdot 1) = n$, since $n \in \mathbb{Z}$ and $1 \in H$.

Kernel of φ: We claim $\ker \varphi = H$.

($\subseteq$): Given $x \in \ker \varphi$, write $x = 2^k h$ with $k \in \mathbb{Z}$ and $h \in H$ by the previous problem.
Then $k = \varphi(x) = 0$, since $x \in \ker \varphi$, and hence $x = 2^0 h = h \in H$.

($\supseteq$): Given $h \in H$, we have $\varphi(h) = \varphi(2^0 h) = 0$. That is, $h \in \ker \varphi$.

Thus, $\varphi : \mathbb{Q}^\times \to \mathbb{Z}$ is an onto homomorphism with kernel H, and therefore $\mathbb{Q}^\times / H \cong \mathbb{Z}$, by the Fundamental Theorem. QED

---

6. Saracino, Section 16, Problem 16.1: Let R be a ring with unity 1_R. Prove that $(-1_R)a = -a$ for all $a \in R$.

Proof. Given $a \in R$, we have $(-1_R)a = 1_R(-a) = -a$, where the first equality is by Theorem 16.1(ii). QED

Alternative Proof (from scratch). Given $a \in R$, we have

$$a + (-1_R)a = (1_R)a + (-1_R)a = (1_R - 1_R)a = 0_R a = 0_R$$

where the last equality is by Theorem 16.1(i). Since $+$ is commutative, we also have $a + (-1_R)a = 0_R$. Thus, $(-1_R)a$ is an additive inverse of a. Since $(R, +)$ is a group, and inverses in a group are unique, we therefore have $(-1_R)a = -a$. QED

---

7. Saracino, Section 16, Problem 16.13: Let R be a ring with unity.

(a) Prove that the multiplicative identity element 1_R of R is unique.

(b) Let $a \in R^\times$ be a unit. Prove that the multiplicative inverse a^{-1} of a is unique.

Proof. (a): Suppose $1_R, 1'_R \in R$ are both multiplicative identities. Then

$$1'_R = 1_R 1'_R = 1_R$$ QED (a)

(b): Given $a \in R^\times$, suppose $b, c \in R$ are both multiplicative inverses of a. Then

$$b = b1_R = b(ac) = (ba)c = 1_R c = c$$ QED (b)