Math 470: Abstract Algebra Homework 2

Chapter 1 Solutions

Proposition 1 (Exercise 1.65)**.** *Suppose that a and b are each positive integers satisfying $gcd(a, b) = 1$. If the product ab is square then each a and b are also squares.*

Proof. Suppose that $ab \leq 2$. So, $ab = 1$ or $ab = 2$. We observe that 2 is not a perfect square. So, $ab \neq 2$ by hypothesis. If $ab = 1$ then we see that both $a = 1$ and $b = 1$. Thus, $a = 1^2$ and $b = 1^2$.

Now suppose that $ab > 2$. Then there exists some positive integer, say c, satisfying $ab = c^2$, because ab is square. Note that $c \geq 2$, else we have $ab = 1 < 2$. By theorem 1.2, we can express c as a product of primes, say $c = p_1 \cdot ... \cdot p_k$. Thus,

$$ab = (p_1 \cdot ... \cdot p_k)^2 = (p_1 \cdot ... \cdot p_k)(p_1 \cdot ... \cdot p_k).$$

Using the associativity and commutativity of the integers, we can gather factors with like indices and produce the following expression for ab:

$$ab = p_1^2 \cdot ... \cdot p_k^2.$$

We observe that if $a < 2$ or $b < 2$ then $a = 1$ or $b = 1$. Then $b = ab$ or $a = ab$. But in either case, $1 = 1^2$ and ab is assumed to be square by hypothesis, so we are done. Thus, we assume that $a \geq 2$ and $b \geq 2$. By the fundamental theorem of arithmetic, we know that a and b each have a prime factorization and each $p_1, ..., p_k$ is a prime factor of a or b. Because a and b are relatively prime, each prime $p_1, ..., p_k$ is exclusively a factor of a or b. It follows that each of $p_1^2, ..., p_k^2$ exclusively belongs to the prime factorization of a or b. Since the index assignment is arbitrary, we may re-index if necessary. Then there exists some positive integer r satisfying $1 \leq r \leq k$ for which

$$a = p_1^2 \cdot ... \cdot p_r^2 \qquad \text{and} \qquad b = p_{r+1}^2 \cdot ... \cdot p_k^2.$$

After rearranging the factors we see that:

$$a = (p_1 \cdot ... \cdot p_r)^2 \qquad \text{and} \qquad b = (p_{r+1} \cdot ... \cdot p_k)^2.$$

■

Proposition 2 (Exercise 1.69)**.** *Suppose that M is some non-negative integer. Then M is the lcm of $a_1, ..., a_n$ if and only if M is a common multiple that divides every other common multiple.*

Proof. Let N be a common multiple of $a_1, ..., a_n$, throughout.

($\Leftarrow$) Since $M|N$, $M \leq N$. Since N is arbitrary, M is the smallest common multiple. Hence, M is the least common multiple.

($\Rightarrow$) Let $M = 0$. Then at least one of $a_1, ..., a_n$ is 0 by the definition of the least common multiple. Thus, $0|N$ by choice of N. So, $N = 0$, because the only number that divides 0 is 0. It follows that $M|N$.

Suppose that $M \neq 0$. By the division algorithm,

$$N = qM + r$$

for unique integers q and r such that $0 \leq r < M$. Since $a_1|M$ and $a_1|N$, it follows that $a_1|(N - qM)$. So, $a_1|r$. By a similar argument, each of $a_1, ..., a_n$ divides r. Hence, r is a common multiple. But M is the least positive common multiple, which implies that $r = 0$, since $r < M$. Then $N = qM$. Thus, $M|N$. Since N is arbitrary, M divides all common multiples.

■

Proposition 3 (Exercise 1.73)**.** *A positive integer n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.*

Proof. We first claim the following:

$$10^k \equiv \begin{cases} 1 \bmod 11, & \text{if } k \text{ is even} \\ -1 \bmod 11, & \text{if } k \text{ is odd.} \end{cases}$$

It is clear that $10^0 \equiv 1 \bmod 11$ and $10 \equiv -1 \bmod 11$. Similarly, we see that $10^2 = 100 = (9)(11) + 1$. Thus, $10^2 \equiv 1 \bmod 11$. So, assume that $k > 2$. If k is even then

$$10^k = (10^2)^{\frac{k}{2}} \equiv 1^{\frac{k}{2}} \bmod 11 \equiv 1 \bmod 11.$$

Note that $\frac{k}{2}$ is an integer, since k is even.

If k is odd then $k-1$ is even. So, we can apply the the result above. Thus, we have the following:

$$10^k = (10^{k-1})10^1 \equiv (1)10 \bmod 11 \equiv 10 \bmod 11 \equiv -1 \bmod 11.$$

This proves our claim.

We now show that the proposition holds. Suppose that k is even. By the claim above, the following holds:

$$d_k 10^k + ... + d_0 \bmod 11 \equiv d_k - d_{k-1} + ... - d_1 + d_0 \bmod 11.$$

Similarly, when k is odd the congruence below is true.

$$d_k 10^k + ... + d_0 \bmod 11 \equiv -d_k + d_{k-1} + ... - d_1 + d_0 \bmod 11$$

In either case, if one side is congruent to $0 \bmod 11$ then the other side is also congruent to $0 \bmod 11$ by the transitivity of congruence modulo 11. It follows that n is divisible by 11 if and only if the alternating sum of the digits of n is congruent modulo 11.

■

Chapter 2 Solutions

Proposition 4 (Exercise 2.3i-iii)**.** *If A and B are subsets of a set X, define their symmetric difference by*

$$A + B = (A - B) \cup (B - A)$$

Then the following hold:

(i) $A + B = (A \cup B) - (A \cap B)$

(ii) $A + A = \emptyset$

(iii) $A + \emptyset = A$.

Proof. (i) Let $x \in A+B$. Then $x \in (A-B)\cup(B-A)$, by the definition of $A+B$. So, $x \in (A-B)$ or $x \in (B-A)$, by the definition of a union.

Suppose that $x \in (A-B)$. Then, $x \in A$ and $x \notin B$. It then follows that $x \in A \cup B$, by the definition of a union and $x \notin A \cap B$, by the definition of an intersection. But this implies $x \in (A\cup B)-(A\cap B)$, by the definition of a set difference. The argument for when $x \in (B-A)$ is similar. Since x is an arbitrary element, this will hold for all $x \in A+B$. Thus,

$$A + B \subseteq (A \cap B) - (A \cap B).$$

Let $x \in (A \cup B) - (A \cap B)$, by the definition of a set difference. Then $x \in (A \cup B)$ and $x \notin (A \cap B)$. Since $x \in A \cup B$, it follows that $x \in A$ or $x \in B$. However, because $x \notin A \cap B$ this "or" is exclusive.

So, if we assume that $x \in A$ then $x \notin B$. Following this line of thought, we see that $x \in (A - B)$. So, $x \in (A - B) \cup (B - A)$, by the definition of a union. If we assume that $x \in B$ then it follows that $x \in (A - B) \cup (B - A)$ by similar reasoning. Thus,

$$A + B \supseteq (A \cap B) - (A \cap B).$$

Therefore, the claim of (i) holds, by the definition of set equality.
(ii) We observe that $A - A = \{x \in A | x \notin A\}$, by the definition of a set difference. Since $x \in A$ or $x \notin A$ exclusively, there are no elements in $A - A$. Thus, $A - A = \emptyset$. Then

$$A + A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset.$$

(iii) Observe that $A - \emptyset = \{x \in A | x \notin \emptyset\}$. Since the empty set has no elements at all, it shares no elements with A. Thus, $x \in A - \emptyset$ if and only if $x \in A$. $A - \emptyset = A$.

Also, $(\emptyset - A) = \{x \in \emptyset | x \notin A\}$. Since there are, by definition of the emptyset, no elements $x \in \emptyset$, then there are no $x \in \emptyset$ such that $x \in A$. It follows that $(\emptyset - A) = \emptyset$.

Using the definition of $A + B$ and the definition of a union, we conclude that

$$A + \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A.$$

■

Proposition 5 (Exercise 2.13)**.** *Let $f : X \to Y$ and $g : Y \to Z$ be functions.Then the following are true:*

(i) If both f and g are injective, prove that $g \circ f$ is injective.

(ii) If both f and g are surjective, prove that $g \circ f$ is surjective.

(iii) If both f and g are bijective, prove that $g \circ f$ is bijective.

(iv) If $g \circ f$ is a bijection, then f is an injection and g is a surjection.

Proof. (i) Let $x_1, x_2 \in X$. Then observe that $(g \circ f)(x_1), (g \circ f)(x_2) \in Z$. Suppose

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

Thus,

$$g(f(x_1)) = g(f(x_2)).$$

By the injectivity of g,

$$f(x_1) = f(x_2).$$

Then by the injectivity of f,

$$x_1 = x_2.$$

So, $(g \circ f)$ is injective.

(ii) Let $z \in Z$. By the surjectivity of g, there exists some $y \in Y$ such that $g(y) = z$. By the surjectivity of f, there exists some $x \in X$ such that $f(x) = y$. Hence, $(g \circ f)(x) = z$. As z is arbitrary, this holds for all $z \in Z$. Thus, $(g \circ f)$ is surjective.

(iii) By definition of bijectivity, f and g are each injective. So we can see that, by (i), $(g \circ f)$ is injective. Similarly, it follows from (ii) that $(g \circ f)$ is surjective. Thus, $(g \circ f)$ is bijective.

(iv) There are really two claims to prove here. First we show that f is injective. Let $x_1, x_2 \in X$ such that $f(x_1), f(x_2) \in Y$. Suppose that

$$f(x_1) = f(x_2).$$

Thus,

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

By the injectivity of $(g \circ f)$,

$$x_1 = x_2.$$

Thus, f is injective.

We now show that g is surjective. Let $z \in Z$. By the surjectivity of $(g \circ f)$, there exists some $x \in X$ such that $(g \circ f)(x) = z$. Thus, $g(f(x)) = z$ where $f(x) \in Y$. Since z is arbitrary, it follows that g is surjective. ■

Proposition 6 (Exercise 2.15)**.** *(i) Let $f : X \to Y$ be a function, and let $\{S_i : i \in I\}$ be a family of subsets of X. Then*

$$f\left(\bigcup_{i \in I} S_i\right) = \bigcup_{i \in I} f(S_i).$$

(ii) If S_1 and S_2 are subsets of a set X, and if $f : X \to Y$ is a function, then $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$. There is an example for which $f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$.

(iii) If S_1 and S_2 are subsets of a set X, and if $f : X \to Y$ is an injection, then $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$.

Proof. (i) Let $y \in f\left(\bigcup_{i \in I} S_i\right)$. Then there exists some $x \in \bigcup_{i \in I} S_i$ such that $f(x) = y$, by definition of the image of f. So, $x \in S_i$ for some index $i \in I$. Thus, $y = f(x) \in f(S_i)$. By the definition of a union, we see that $y \in \bigcup_{i \in I} f(S_i)$. Since y is arbitrary, the same is true of all $y \in \bigcup_{i \in I} S_i$. Thus,

$$f\left(\bigcup_{i\in I} S_i\right) \subseteq \bigcup_{i\in I} f(S_i).$$

Let $y \in \bigcup_{i\in I} f(S_i)$. Then $y \in f(S_i)$ for some $i \in I$. By definition of the image of f, it follows that there exists some element $x \in S_i$ such that $f(x) = y$. Thus, $x \in \bigcup_{i\in I} S_i$. So, $y = f(x) \in f\left(\bigcup_{i\in I} S_i\right)$. Since y is arbitrary, this holds for all $y \in \bigcup_{i\in I} f(S_i)$. Thus,

$$f\left(\bigcup_{i\in I} S_i\right) \supseteq \bigcup_{i\in I} f(S_i).$$

Therefore, set equality follows.

(ii) There are two claims to address for this item. First, fix some element $y \in f(S_1 \cap S_2)$. Thus, there exists some $x \in S_1 \cap S_2$ such that $f(x) = y$, by the definition of a function image. The intersection implies that $x \in S_1$ and $x \in S_2$. Thus, $y = f(x) \in f(S_1)$ and $y \in f(S_2)$. By definition of an intersection, $y \in f(S_1) \cap f(S_2)$. Since y is arbitrary, this holds for all y. So,

$$f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2).$$

Second, we find an example that shows the opposite subset inclusion does not necessarily hold. Let $X, Y = \mathbb{R}$, $S_1 = (-2, 1)$ and $S_2 = (-1, 2)$, where S_1 and S_2 are intervals on the real line. It's clear that $S_1, S_2 \subseteq X$. Choose your function to be $f : \mathbb{R} \to \mathbb{R}$ defined by the rule $f(x) = x^2$. Then $f(S_1) = [0, 4)$ and $f(S_2) = [0, 4)$. So,

$$f(S_1) \cap f(S_2) = [0, 4).$$

Note that $S_1 \cap S_2 = (-1, 1)$. Thus,

$$f(S_1 \cap S_2) = [0, 1).$$

So, we see that

$$f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2).$$

(iii) From part (ii), we know that $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$. So, it suffices to show the opposite inclusion. Let $y \in f(S_1) \cap f(S_2)$. By the definition of an intersection, $y \in f(S_1)$ and $y \in f(S_2)$. From which we can see that there exists some $x_1 \in S_1$ and some $x_2 \in S_2$ such that $f(x_1) = y$ and $f(x_2) = y$. Hence, $f(x_1) = f(x_2)$. By the injectivity of f, $x_1 = x_2$. Then it suffices to only consider x_1. From above, it follows that $x_1 \in S_1 \cap S_2$. Thus, $y = f(x_1) \in f(S_1 \cap S_2)$. Since y is arbitrary, this holds for all $y \in f(S_1) \cap f(S_2)$. We conclude that

$$f(S_1 \cap S_2) \supseteq f(S_1) \cap f(S_2).$$

Therefore, set equality holds. ■

Proposition 7 (Exercise 2.16)**.** *Let $f : X \to Y$ be a function. If $B_i \subseteq Y$ is a family of subsets of Y then the following are true:*

i $f^{-1}\left(\bigcup_{i \in I} B_i\right) = \bigcup_{i \in I} f^{-1}(B_i)$ and $f^{-1}\left(\bigcap_{i \in I} B_i\right) = \bigcap_{i \in I} f^{-1}(B_i)$, and

ii If $B \subseteq Y$, then $f^{-1}(B') = f^{-1}(B)'$, where B' denotes the complement of B.

Proof. (i) Let $x \in f^{-1}\left(\bigcup_{i \in I} B_i\right)$. Thus, $f(x) \in \bigcup_{i \in I} B_i$, by the definition of a preimage. So, $f(x) \in B_i$ for some $i \in I$, by definition of a union. It follows then that $x \in f^{-1}(B_i)$. Thus, $x \in \bigcup_{i \in I} f^{-1}(B_i)$. Then we can conclude that

$$f^{-1}\left(\bigcup_{i \in I} B_i\right) \subseteq \bigcup_{i \in I} f^{-1}(B_i).$$

For the opposite inclusion, let $x \in \bigcup_{i \in I} f^{-1}(B_i)$. Then $x \in f^{-1}(B_i)$ for some $i \in I$. Thus, $f(x) \in B_i$. So, $f(x) \in \bigcup_{i \in I} B_i$. Thus, we have that $x \in f^{-1}\left(\bigcup_{i \in I} B_i\right)$. This shows that the opposite inclusion holds. Therefore, set equality holds.

(ii) Let $x \in f^{-1}(B')$. Thus, $f(x) \in B'$. Since B' is the complement of B, $f(x) \notin B$. So, $x \notin f^{-1}(B)$. It follows by the definition of a complement that $x \in f^{-1}(B)'$. ■

Proposition 8 (Exercise 2.17)**.** *Let $f : X \to Y$ be a function. Define a relation on X by $x \equiv x'$ if $f(x) = f(x')$. Then $\equiv$ is an equivalence relation.*

Proof. For reflexivity, let $x \in X$. It's clear that $f(x) = f(x)$. Thus, we see that $x \equiv x$.

For symmetry, we assume that $x \equiv x'$. Thus, $f(x) = f(x')$. By the symmetry of equality, $f(x') = f(x)$. So, $x' \equiv x$.

For transitivity, let $x_1, x_2, x_3 \in X$ such that

$$x_1 \equiv x_2 \qquad \text{and} \qquad x_2 \equiv x_3.$$

It follows that $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$. By the transitivity of equality, $f(x_1) = f(x_3)$. So, $x_1 \equiv x_3$. We conclude that $\equiv$ is an equivalence relation. ■