Abstract Algebra Herstein - Solutions Manual

Mingruifu Lin

September 2023

Contents

Chapter 1

Preliminary Notions

1.1 Set Theory

Problem 1

(a) We expand the definitions $A \subseteq B$ and $B \subseteq C$:

$$x \in A \Rightarrow x \in B$$

$$x \in B \Rightarrow x \in C$$

Suppose $x \in A$. Then by modus ponens, $x \in B$. Again by modus ponens, $x \in C$. Hence, by conditional proof, $x \in A \Rightarrow x \in C$. This is the definition of $A \subseteq C$.

(b) Suppose $x \in A \cup B$. We check two cases. If $x \in A$, then $x \in A$. If $x \in B$, then using $B \subseteq A$ and modus ponens, we get $x \in A$, hence $x \in A$. Thus $A \cup B \subseteq A$.

For the reverse direction, suppose $x \in A$. Then $x \in A \cup B$ by disjunction introduction. Thus $A \subseteq A \cup B$. Hence proven.

(c) Too lazy. Disjunctions are always tedious, as seen previously.

Problem 2

(a) For intersection:

$$x \in A \cap B$$

$$\Leftrightarrow x \in A \text{ and } x \in B$$

$$\Leftrightarrow x \in B \cap A$$

For union: Too lazy. Again, too many disjunctions.

(b) Same idea as (a). Simply apply conjunction elimination twice, then conjunction introduction twice.

Problem 3

Here we gooooo.

Suppose $x \in A \cup (B \cap C)$. If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$, hence $x \in (A \cup B) \cap (A \cup C)$. Otherwise, $x \in B \cap C$, so $x \in B$ and $x \in C$, thus $x \in B \cup A$ and $x \in C \cup A$, hence $x \in (A \cup B) \cap (A \cup C)$. Hence $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

For the reverse direction, suppose $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. If $x \in A$, then $x \in A \cup (B \cap C)$. If $x \in B$, then, in order to satisfy the second statement, either $x \in A$, which we've seen, or $x \in C$. In the latter case, we thus have $x \in B \cap C$, hence $x \in (B \cap C) \cup A$. In all cases, we have $x \in A \cup (B \cap C)$. Hence $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Hence proven.

Problem 4

(a)

$$x \in (A \cap B)'$$

$$\Rightarrow x \notin A \cap B$$

Using the fact $\neg(A \wedge B) = \neg A \vee \neg B$:

$$\Rightarrow x \notin A \text{ or } x \notin B$$

$$\Rightarrow x \in A' \text{ or } x \in B'$$

$$\Rightarrow x \in A' \cup B'$$

Too lazy to prove the reverse direction.
(b) Too lazy.

Problem 5

Idk what I'm allowed to do bro.

Problem 6

Include or exclude an element.

Problem 7

At least 39% like both. At most 63% like both.

Problems 8, 9

Too lazy, skipped.

Problem 10

(a) No. The common ancestor could be different for each pair.
(b) No. For example, one at far left, one in middle, one at far right.
(c) Yes.
(d) Yes.
(e) No. Equivalence relation must be reflexive.
(f) Yes.

Problem 11

(a) The reflexive property guarantees the existence of equivalence classes on non-empty sets, whereas the other properties do not.
(b) Idk. Maybe $a \in R \Rightarrow a \sim a$.

Problems 12 and 13

Too lazy.

1.2 Mappings

Problem 1

(a) Onto, but not one-to-one.
(b) Both onto and one-to-one. The inverse image is $t\sigma^{-1} = \sqrt{t}$.
(c) Neither onto nor one-to-one.
(d) One-to-one, but not onto.

Problem 2

Simply take $f(s \times t) = t \times s$.

Problem 3

Too lazy. Seems obvious.

Problem 4

(a) Any bijective function has an inverse, which is also a bijection.
(b) Simply take the composition of the bijection.

Problem 5

???

Problem 6

This is akin to Cantor's diagonal argument. In the original argument, we create a real number which differs from every listed real number by a single digit, hence it is not in the list. Here, the idea is similar.

Suppose I have a bijection $f : S \to S^*$, where each $s \in S$ is mapped to a subset $f(s) \in S^*$. Let me construct the set $B = \{s \in S \mid s \notin f(s)\}$. In other words, this is the set of elements which are not contained in the subset associated with them. As you see, B differs from $f(s)$ by the single element s for each $f(s)$. If $f(s)$ contains s, then B does not contain s, and if $f(s)$ does not contain s, then B contains s. Since for all bijections f, we can such a set B, hence there exists no bijection between S and S^*.

Problem 7

There are $n!$ ways to permute n objects.

Problem 8

(a) and (b) ??
(c) For (a), as we learned in real analysis, you can map $[0, 1)$ to $\mathbb{R}$, so you repeat the procedure for every $[n, n+1)$ for $n \in \mathbb{Z}$. This is onto, but not one-to-one. For (b), simply map $\mathbb{R}$ to $(0, 1)$, which is one-to-one, but not onto.

Problem 9

(a) Using the real numbers again, let $\sigma : \mathbb{R} \to \mathbb{R}$ and $\tau : (0, 1) \to \mathbb{R}$, but the range of σ is $(0, 1)$.
(b) Just some domain BS. The first function must be one-to-one, but its range may not cover the entire domain of the second function. So you can do whatever you want to the things outside of the domain.

Problem 10

Classic real analysis exercise. Skipped.

Problem 11

(a) Obvious?
(b) Too easy.
(c) Again, domain BS.

Problem 12

??

Problem 13

(a) Let $\sigma : n \mapsto 2n$.
(b) Let $\sigma : \mathbb{R} \to (0, 1)$, which is easily found if you know real analysis.
(c) A is infinite, so it has a map $f : A \to a$, where $a \subset A$. Then, we use the identity function on $S \setminus A$. Combining the two functions, we effectively get a bijection $g : S \to s$ where $s \subset S$:

$$g(x) = \begin{cases} f(x) & x \in A \\ i(x) & x \in S \setminus A \end{cases}$$

Problem 14

Classic exercise in real analysis.

Problems 15 and 16

Obvious.

1.3 The Integers

Problem 1

$$\begin{aligned} a \mid b \quad &\Rightarrow \quad b = k_1 a \\ b \mid a \quad &\Rightarrow \quad a = k_2 b \end{aligned}$$

Where k_1, k_2 are integers. But we know $k_2 = \frac{1}{k_1}$, and in order for k_2 to remain an integer, k_1 must be equal to 1 or -1 (this can be proved by induction). Hence, $b = (\pm 1)a = \pm a$.

Problem 2

$$b \mid g, \quad b \mid h \quad \Rightarrow \quad b \mid mg, \quad b \mid nh \quad \Rightarrow \quad b \mid mg + nh$$

Problem 3

Let $d = \frac{ab}{(a,b)} = \frac{a}{(a,b)} b$. Since $(a, b) \mid a$, then $\frac{a}{(a,b)}$ is an integer, hence $b \mid d$. The same procedure can be done for $a \mid d$. Hence, d satisfies the first property.

For the second property, first note that if $a = m(a, b)$ and $b = n(a, b)$, then $(m, n) = 1$. Suppose for contradiction that $k \mid m$ and $k \mid n$ for some $k > 1$. Then

$$k(a, b) \mid m(a, b) = a$$

and

$$k(a, b) \mid n(a, b) = b$$

hence $k(a, b) \mid a, b$ but $k(a, b) \nmid (a, b)$, contradicting the fact that (a, b) is the GCD. Hence $(m, n) = 1$.

SKIP.

Problem 4

$$am = bn$$

Since $(a, b) = 1$, and $a \mid bn$, then $a \mid n$. Hence $ab \mid nb = x$.

Problem 5

(a) Obviously, $p_1^{\delta_1} \dots p_k^{\delta_k}$ divides both a and b. Now, suppose $x \mid a, b$. We can develop its prime factorization. So $x = p_1^{\omega_1} \dots p_k^{\omega_k} \mid a, b$. Which means $p_i^{\omega_i} \mid a, b$, for each i. But $p_i^{\omega_i}$ is coprime with every other prime of a, b, so it must divide the non-coprime part, which only consists of the prime equal to him, hence $p_i^{\omega_i} \mid p_i^{\alpha_i}$ and $p_i^{\omega_i} \mid p_i^{\beta_i}$. Hence, it must divide the minumum power, so $\omega_i \mid \min(\alpha_i, \beta_i) = p_i^{\delta_i}$. Multiplying every $p_i^{\omega_i}$ together, we get $p_1^{\omega_1} \dots p_k^{\omega_k} \mid p_1^{\delta_1} \dots p_k^{\delta_k}$, which gives us our desired result.
(b) We use the formula proven in Problem 3.

$$[a, b] = \frac{ab}{(a, b)}$$

Let's concentrate on a single prime at a time. For prime i, we have

$$p_i^{\gamma_i} = \frac{p_i^{\alpha_i} p_i^{\beta_i}}{p_i^{min(\alpha_i, \beta_i)}}$$
$$= p_i^{\alpha_i + \beta_i - \min(\alpha_i, \beta_i)}$$
$$= p_i^{\max(\alpha_i, \beta_i)}$$

Problem 6

Proof by induction. Base case. r_{n-1} is divisible by r_n.

$$r_{n-1} = q_n r_n + r_{n+1} = q_n r_n + 0 = q_n r_n$$

And obviously, r_n is divisible by r_n.
Now, suppose r_{k-1} and r_k are divisible by r_k, then

$$r_{k-2} = q_{k-1} r_{k-1} + r_k$$

indicates that r_{k-2} is obviously divisible by r_k. Here, we thus proved:

$$r_k \mid r_k \text{ and } r_k \mid r_{k-1} \quad \Rightarrow \quad r_k \mid r_{k-1} \text{ and } r_k \mid r_{k-2}$$

which completes our induction step. (a and b are precisely $r_{(-1)}$ and r_0.)

Chapter 2

Group Theory

2.1 Some Preliminary Lemmas

Problem 1

(a) No. Not associative
(b) No. Missing inverse.
(c) Yes.
(d) Yes.

Problem 2

Just repeatedly swap.

Problem 3

For all a, b, we have

$$(a \cdot b)^2 = a^2 \cdot b^2$$

$$a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$$

Take inverse on each end.

$$\Rightarrow b \cdot a = a \cdot b$$

Problem 4

We are given (1)

$$(ab)^i = a^i b^i$$

and (2)

$$(ab)^{i+1} = a^{i+1} b^{i+1}$$

$$\Rightarrow (ba)^i = a^i b^i$$

and (3)

$$(ab)^{i+2} = a^{i+2}b^{i+2}$$

$$\Rightarrow (ba)^{i+1} = a^{i+1}b^{i+1}$$

We substitute (2) into (3), then regroup, giving the result (4)

$$\Rightarrow (ba)^{i+1} = a(ba)^i b$$

$$\Rightarrow ba(ba)^i = ab(ab)^i$$

Notice that we can equate $a^i b^i$ in (1) and (2), giving the result (5)

$$(ab)^i = a^i b^i = (ba)^i$$

Now, we substitute (5) into (4), which becomes

$$\Rightarrow ba(ba)^i = ab(ba)^i$$

Taking the inverse on each side gives the desired result.

Problem 5

??

Problem 6

Let $x = 1 \leftrightarrow 2$. Let $y = 2 \leftrightarrow 3$. Then $(xy)^2$ will cause $123 \to 312$, while x^2y^2 would be identity $123 \to 123$.

Problem 7

The identity operation, as well as the 2-element swaps, satisfy $x^2 = e$. The 3-element cycles satisfy $x^3 = e$. It's then easy to count.

Problem 8

Suppose for contradiction that $a^N \neq e$ for all $N \in \mathbb{N}$. We show that this implies $a^X \neq a^Y$ for all pairs $X \neq Y$. Suppose for (nested) contradiction that $a^X = a^Y$ for some pair $X > Y > 1$. Then taking the inverse on both sides yields $a^{X-Y} = e$, contradicting the fact that $a^N \neq e$ for all N. Hence, $a^X \neq a^Y$, i.e. the powers of a are pairwise distinct. However, we know our group is finite, but a^N creates infinite distinct elements. Hence, it must be false, so $a^N = e$ for some N.

Problem 9

(a)

$$G = \{e, x, y\}$$

Since identity e is unique, then $xy \neq x$. Because, otherwise, we would have $y = e$, which is false. Similarly, $xy \neq y$. So, using the fact that groups are closed, xy must have some result in G, the only one left being $xy = e$. Property of inverse implies that $yx = e$ as well. Hence x commutes with y. Finally, we know the identity commutes with every elements. Hence proven.
(b)

$$G = \{e, x, y, z\}$$

Suppose $xy = yx = e$, then xz cannot equal x nor z, because neither is equal to the unique e. It also cannot equal e, because x, y are already inverse pairs, and inverses are unique, so z cannot be another inverse. Hence xz can only equal y, by the closure property. This procedure is repeated for zx, yz, zy, which must equal y, x, x respectively. Hence, $xy = yx = e$ and $xz = zx = y$ and $yz = zy = x$, where e already commutes with everyone.

Now, suppose $x^2 = e$ and $y^2 = e$. Since inverses are unique, we have $z^2 = e$. And thus $xy = yx = z$ and $xz = zx = y$ and $yz = zy = x$ (same logic as before, none can be identity, and none is inverse pair). And e already commutes with everyone.

All cases have been gone over. Hence proven.
(c) Too lazy. We know every group of prime order must be cyclic, therefore abelian.

Problem 10

For every pair x, y, we have

$$(xy)^2 = e = ee = x^2y^2$$

$$\Rightarrow xyxy = xxyy$$

Taking inverse on both extremities of each side yields

$$yx = xy$$

Problem 11

Inverses come in pairs. But e is paired with itself. So if the group order is even, then there is an odd number of non-e elements. Hence, another element must be paired with itself.

Problem 12

Inverse is commutative:

$$ay = e$$

$$yay = ye$$

$$yay = y$$

$$yayy^{-1} = yy^{-1}$$

$$ya = e$$

We use this result to prove identity is commutative:

$$ae = a$$

$$aya = a$$

$$ea = a$$

Problem 13

??

Problem 14

Since the group is finite, for every a, there exists m such that $a^m = a$. Let $e_a = a^{m-1}$ be an identity of a. It's clear by associativity that it's both left and right identity of a.

Let $a^{-1} = a^{m-2}$ be an inverse of a. It's also clear by associativity that it's both left and right inverse of a.

Suppose $ab = e_a$. Recall that $a \cdot a^{m-2} = a^{m-1} = e_a$. Hence,

$$ab = e_a = a \cdot a^{m-2}$$

$$\Rightarrow b = a^{m-2}$$

by left cancellation law. Thus, each element's inverse is unique. The same procedure also shows that each element's identity is unique.

Suppose $ae_a = a$. Then

$$ae_a c = ac$$

$$\Rightarrow e_a c = c$$

by left cancellation law. Hence, every element shares an identity pairwise. Since every element also only has a single identity, then all identities are equal.

Problem 15

(a) It's already finite, closed, and associative. Suppose for contradiction that $ab \equiv ac \mod p$, but $b \not\equiv c \mod p$, where $a, b, c \in \{1, \dots, p-1\}$. Then $ab - ac = a(b-c) \equiv 0 \mod p$. Hence $p \mid a(b-c) = am$ where clearly $m < p$. Now, since p is prime, it must divide one of the factors a or m. But $a < p$ and $m < p$, thus we have a contradiction. Hence, it must be that $b \equiv c \mod p$. Hence, by Problem 14, this is a group.
(b) Skip

Problem 16

??

Problem 17

Consider the naturals $\mathbb{N} = \{1, 2, \dots\}$ under addition. It's associative and closed, and the cancellation laws work. However, the latter still don't allow us to dip lower than 1. Hence, we don't have access to the identity element.

Problem 18

Since inverses are organized in pairs, we have

$$e \quad \begin{matrix} a_1 & a_2 & \cdots & a_{n-1} \\ b_1 & b_2 & \cdots & b_{n-1} \end{matrix} \quad c$$

Let us define the product as follows:

$$a_i b_i = b_i a_i = e$$

$$c^2 = e$$

Idk...

Problem 19

Nah.

Problem 20

It is closed. Suppose $\det(A), \det(B) \in \mathbb{Q}$. Then,

$$\det(AB) = \det(A)\det(B) \in \mathbb{Q}$$

It is associative, because matrix multiplication is inherently associative. There exists the identity matrix which has determinant 1, and clearly $1 \in \mathbb{Q}$. And since determinant is nonzero, then there exists an inverse for each matrix.

Problem 21

It is closed:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} e & f \\ 0 & h \end{pmatrix} = \begin{pmatrix} ae & af+bh \\ 0 & dh \end{pmatrix}$$

and since $ad, eh \neq 0$, then $adeh = (ae)(dh) \neq 0$. Matrix multiplication is inherently associative. The identity matrix satisfies the conditions. And since ad is the determinant, which is nonzero, then every matrix has an inverse. Finally,

$$\begin{pmatrix} e & f \\ 0 & h \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} ae & be+df \\ 0 & dh \end{pmatrix}$$

so it is not abelian.

Problem 22

Clearly closed and associative. The identity satisfies the conditions also. Next, since a is nonzero, then a^{-1} exists and is also nonzero. Therefore their product is nonzero. And $aa^{-1} = 1$ is precisely their determinant, which is nonzero, hence the inverse exists. Finally, diagonal matrices are commutative, hence the group is abelian.

Problem 23

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Problem 24

We can simply make an exhaustive list:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

It contains 6 elements. The identity is present. If you check all cases, you will see that it is closed and each element has an inverse. Matrix multiplication is already associative.

Problem 25

Too lazy.

Problem 26

Too lazy.