Name:

Math 251W: Foundations of Advanced Mathematics

Solutions to Portfolio problems from Chapter 7 and Section 5.3

Problem 7.2.3

Let A be a set. Define the binary operation $\triangle$ on $\mathcal{P}(A)$ by $X \triangle Y = (X - Y) \cup (Y - X)$ for all $X, Y \in \mathcal{P}(A)$. This operation is called the symmetric difference.

proposition: The set $\mathcal{P}(A)$ with the operation $\triangle$ forms an abelian group.

proof Let A be a set and define the binary operation $\triangle$ on $\mathcal{P}(A)$ by $X \triangle Y = (X - Y) \cup (Y - X)$ for all $X, Y \in \mathcal{P}(A)$. By definition of the powerset, there is at least one element, namely the null set, thus $\mathcal{P}(A)$ is nonempty.

Let X and Y be arbitrary elements of $\mathcal{P}(A)$. Consider $X \triangle Y$. By definition of $\triangle$, $X \triangle Y = (X - Y) \cup (Y - X)$. It is easy to see that $X \triangle Y$ is in $\mathcal{P}(A)$. Since X and Y are arbitrary, $\mathcal{P}(A)$ is closed under A.

Let X, Y and Z be arbitrary elements of $\mathcal{P}(A)$. Consider $X \triangle (Y \triangle Z)$. By definition of $\triangle$,

$$X \triangle (Y \triangle Z) = X \triangle [(Y - Z) \cup (Z - Y) = (X - [(Y - Z) \cup (Z - Y)]) \cup ([(Y - Z) \cup (Z - Y)] - X) = (X \triangle Y) \triangle Z.$$

Since X, Y and Z are arbitrary elements in $\mathcal{P}(A)$, this applies to all elements, hence is associative on $\mathcal{P}(A)$.

Considser an arbitrary element $E \in \mathcal{P}(A)$. Consider $E \triangle \emptyset$. By definition of $\triangle$, $E \triangle \emptyset = (E - \emptyset) \cup (\emptyset - E) = E$. Furthermore, consider $\emptyset \triangle E = (\emptyset - E) \cup (E - \emptyset)$. Thus $E \triangle \emptyset = E = \emptyset \triangle E$. Thus, since E is arbitrary, $\emptyset$ is the -identity element and $\triangle$ on $\mathcal{P}(A)$ satisfies the identity law.

Let X be an arbitrary element of A. Consider $X \triangle X = (X - X) \cup (X - X) = \emptyset$. Since X is arbitrary, every element in $\mathcal{P}(A)$ is it's own inverse. Thus $\triangle$ on $\mathcal{P}(A)$ satisfies the inverse law.

Since the operation $\triangle$ on S satisfies the associative, identity, and inverse laws, $(\mathcal{P}(A), \triangle)$ is a group.

Let X and Y be arbitrary elements of $\mathcal{P}(A)$. Consider $X \triangle Y$. By definition of $\triangle$, $X \triangle Y = (X - Y) \cup (Y - X) = (Y - X) \cup (X - Y) = Y \triangle X$. Since X and Y are arbitrary, $X \triangle Y = Y \triangle X$ for all $X, Y \in \mathcal{P}(A)$. By definition of the commutative property, $\triangle$ on $\mathcal{P}(A)$ satisfies the commutative law.

Since the binary operation $\triangle$ on $\mathcal{P}(A)$ forms a group and satisfies the commutative law, it is therefore an abelian group.

Problem 7.2.6

proposition: Let $(G, *)$ be a group. For all g in G, the $*$-inverse of g is unique.

proof Let $(G, \star)$ be an arbitrary group, and let g be an arbitrary element in G. By definition of a group, there is exists at least one inverse, and also that there exists some identity element, let e be the $\star$-identity. Let x and y be $\star$-inverses of G. By definition of the $\star$-inverse, $g \star x = e$ and $g \star y = e$. By transitivity of equality, $g \star x = e = g \star y$. By definition of the $\star$ identity, $e \star x = x$. By substitution, $(g \star x) \star x \star (y \star e) = x = x \star (g \star y)$. By definition of a group, $(G, \star)$ satisfies the associative law, hence $x = (x \star g) \star y$. By the inverse law, it follows that $x = e \star y = y$. Thus $x = y$. Since x and y are arbitrary inverses of a, for all $g \in G$, the inverse is unique.

Problem Symmetries of Rectangle

a. What are all the symmetries of a rectangle? List them and then form the composition operation table for the set of symmetries.

   Symmetries The symmetries are: e, do nothing, r, rotation by 180 degrees (clockwise or counterclockwise brings the same result), v, a vertical reflection across the center, and h, a horizontal reflection across the center. Let $\circ$ be a binary operation on the set of these symmetries, defined as composition of two symmetric transformations. The table for the compositions is below.

$\circ$	e	r	v	h
e	e	r	v	h
r	r	e	h	v
v	v	h	e	r
h	h	v	r	e

b. Do the symmetries of the rectangle with composition form a group? You should explain your answer, but you do not need to give a formal proof.

   Explanation These do form a group. In fact, they form a abelian group. If any operation is carried out on the result of two operations, it is the same as the result of carrying out the result of the first two operations with the last, so the associative law is satisfied. Furthermore, the identity law is the do nothing, which is no surprise, and each symmetry is its own inverse. Obviously the set is not empty, so this forms a group. It also has the communative property, because the operations are symmetric along the diagonal on the table, which would make this an abelian group.

Problem 7.2.12(1)

proposition: Given $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group.

proof (Direct) Let n be an arbitrary natural number, and define $+$ as defined in class. To show that $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group, it is first necessary to show that it is a group, and then show that the operation $+$ is commutative on $\mathbb{Z}/n\mathbb{Z}$.

(Closure) Let $[x]$ and $[y]$ be arbitrary elements in $\mathbb{Z}/n\mathbb{Z}$. Consider $[x] + [y] = [x + y]$.

(Identity) Let $[x]$ be an arbitrary element in $\mathbb{Z}/n\mathbb{Z}$. Consider $[0]$. By definition of $\mathbb{Z}/n\mathbb{Z}$, $[0] \in \mathbb{Z}/n\mathbb{Z}$. Consider $[x] + [0] = [x + 0] = [x]$. Since $[x]$ is arbitrary, it follows that for all elements $[x] \in \mathbb{Z}/n\mathbb{Z}$, $[x] + [0] = [x]$. By definition of the identity law, $+$ satisfies the identity law on $\mathbb{Z}/n\mathbb{Z}$, and $[0]$ is the $+$-identity.

(Inverse) Let $[x]$ be an arbitrary element in $\mathbb{Z}/n\mathbb{Z}$. Consider $[-x]$. Somehow, $[-x] \in \mathbb{Z}/n\mathbb{Z}$. Consider $[x] + [-x] = [x + (-x)] = [0]$. Since $[0]$ is the $+$-identity, it follows that $[-x]$ is the $+$-inverse of $[x]$. Since $[x]$ is an arbitrary element in $\mathbb{Z}/n\mathbb{Z}$, it follows that $+$ satisfies the inverse law on $\mathbb{Z}/n\mathbb{Z}$.

(Associative Law) Let $[x], [y]$ and $[z]$ be arbtirary elements in $\mathbb{Z}/n\mathbb{Z}$. Consider

$$([x] + [y]) + [z] = [x + y] + [z] = [x + y + z] = [x] + [y + z] = [x] + ([y] + [z]).$$

Since $[x], [y]$ and $[z]$ are arbitrary, it follows that $+$ satisfies the associative law on $\mathbb{Z}/n\mathbb{Z}$. Since the operation $+$ satisfies closure and the identity, inverse, and associative laws on $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z}, +)$ is therefore a group.

(commutative Law) Let $[x]$ and $[y]$ be arbitrary elements in $\mathbb{Z}/n\mathbb{Z}$. Consider $[x]+[y] = [x+y] = [y+x] = [y]+[x]$. Since $[x]$ and $[y]$ arte arbitrary, it follows that for all $[x]$ and $[y]$ in $\mathbb{Z}/n\mathbb{Z}$, $[x]+[y] = [y]+[x]$. Hence the operation $+$ is commutative on $\mathbb{Z}/n\mathbb{Z}$. Since $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group, it follows that $(\mathbb{Z}/n\mathbb{Z}, +)$ is also an abelian group.

Problem 7.3.7

proposition: Let G, H, and K be groups, and let $f : G \to H$ and $j : H \to K$ be homomorphisms. Then the map $j \circ f : G \to K$ is a homomorphism.

proof

Let G, H and K be arbitrary groups, and let $f : G \to H$ and $j : H \to K$ be arbitrary homomorphisms. Let $\star, \diamond, \oplus$ be the operations which G, H and K are defined under respectively. By definition of a homomorhpism, $f(x \star y) = f(x) \diamond f(y)$. Consider the map $f \circ j$. Since H is the codomain of j and the domain of f, this map is well defined. Let x and y be arbtirary elements in G. By composition and by definition of a homomorphism,

$$j \circ f(x \star y) = j(f(x \star y)) = j(f(x) \diamond f(y)) = j(f(x)) \oplus j(f(y)) = (j \circ f(x)) \oplus (j \circ f(y)).$$

Thus, for all x and y, $j \circ f(x \star y) = (j \circ f(x)) \oplus (j \circ f(y))$. By definition of a homomorphism, $j \circ f : G \to K$ is a homomorhpism

Problem 7.Awesome

proposition: Define a relation $\mathcal{I}$ on the set of all groups by saying two groups are related (or isomorphic) if there exists an isomorphism from one to the other. Prove this is an equivalence relation on the set of all groups.

proof (Proof by Length)

Let $\mathcal{I}$ be the relation on the set of all groups defined $(G, F) \in \mathcal{I}$ iff G and F are isomorphic, for all groups G and F.

Let X be an arbitrary group, and let $\oplus$ be the operation for X. Consider the identity map $1_X : X \to X$ defined $1_X(X) : X \to X$. Let x and y be arbitrary elements in X. Consider $1_X(x \oplus y)$. By definition of the identity map, $1_X(x \oplus y) = x \oplus y$. Since x and y are arbitrary, this applies to all elements in X. Thus, by definition of a homomorphism, $1_X : X \to X$ is a homomorphism from X to X. By definition, the identity map is its own inverse. By theorem, this means that 1_X is bijective. Thus, $1_X : X \to X$ is an isomorhpism, hence X is isomorphic to itself. Thus, $(X, X) \in \mathcal{I}$. Since X is an arbitrary group, this applies to all groups, thus $\mathcal{I}$ is reflexive.

Let Q and R be arbitrary isomorphic groups, and let $\star$ and $\diamond$ be their respective operations. By definition of an isomorphism, there exists some map $m : Q \to R$ such that $m(a \star b) = m(a) \diamond m(b)$. By definition of an isomorhpism, m is bijective. By theorem, there exists an inverse $m^{-1} : R \to Q$. Let c and d be arbitrary elements in R. Consider $m^{-1}(c \diamond d)$. Since m is bijective, it is therefore surjective. Thus, by definition of surjectivity, there exists elements $v, w \in Q$ such that $c = m(v)$ and $d = m(w)$. Substituting, $m^{-1}(c \diamond d) = m^{-1}(m(v) \diamond m(w))$. Since m is a homomorhpism, $m^{-1}(m(v) \diamond m(w)) = m^{-1}(m(v \star w))$. By definition of composition, $m^{-1}(m(v \star w)) = m^{-1} \circ m(v \star w)$. By definition of inverses, $m^{-1} \circ m : Q \to Q$ is the identity map $1_Q : Q \to Q$. Thus, by definition of the idenity map, $m^{-1} \circ m(v \star w) = v \star w$. By substitution, $m^{-1}(c \diamond d) = v \star w$. Since $c = m(v)$ and $d = m(w)$, $v = m^{-1}(c)$ and $w = m^{-1}(d)$. Substituting, $m^{-1}(c \diamond d) = m^{-1}(c) \star m^{-1}(d)$. Since c and d are arbitrary, this applies to all pairs of elements in the domain, thus $m^{-1} : R \to Q$ is an isomorphism, and R is isomorhpic to Q. By definnition of $\mathcal{I}$, $(R, Q) \in \mathcal{I}$. Since R and Q are arbitrary groups, $\mathcal{I}$ is symmetric.

Let A, B and C be arbitrary groups, defined under operations $\cdot$, $\oplus$, $\otimes$ respectively, such that $(A, B) \in \mathcal{I}$ and $(B, C) \in \mathcal{I}$. By definition of $\mathcal{I}$, A is isomorphic to B and B is isomorphic to D. By definition of an isomorophism, there exits bijective maps $f : A \to B$ and $g : B \to C$ such that $f(a \cdot b) = f(a) \oplus f(b)$ and $g(c \oplus d) = g(c) \otimes g(d)$ for all elements $a, b \in A$ and $c, d \in B$. Let a and b be arbitrary elements in A. Consider $g \circ f : A \to C$, which is well defined because the codomain of f is the domain of g. By composition, and since f and g are homomorhpisms, $g \circ f(a \cdot b) = g(f(a \cdot b)) = g(f(a) \oplus f(b)) = g(f(a)) \otimes g(f(b)) = (g \circ f(a)) \oplus (g \circ f(b))$. Since a and b are arbitrary, and by definition of a homomorphism, $g \circ f : A \to C$ is a homomorphism. Furthermore, by theorem, since f and g are bijective, so is $g \circ f$. By definition of an isomorphism, $g \circ f : A \to C$ is an isomorphism, hence A and C are isomorphic. By definition of $\mathcal{I}$, $(A, C) \in \mathcal{I}$. Since A, B and C are arbitrary groups, $\mathcal{I}$ is transitive.

Because the relation $\mathcal{I}$ is reflexive, symmetric, and transitive, $\mathcal{I}$ is therefore an equivalence relation. ■

Problem 5.3.6

Let A be a non-empty set, and let $\sim$ be an equivalence relation on A.
proposition: Let $x, y \in A$.

a If $x \sim y$, then $[x] = [y]$

b If $x \not\sim y$ then $[x] \cap [y] = \emptyset$

c $\bigcup_{[x]\in A/\sim}[x] = A$

a $\boxed{\text{proof}}$ Let A be an arbitrary non-empty set, and let $\sim$ be an arbitrary equivalence relation on A. Let x and y be arbitrary elements in A such that $x \sim y$.

Let a be an arbitrary element of $[x]$. By definition of the relation class, $x \sim a$. Furthermore, since equivalence relations are symmetric, $y \sim x$. Since equivalence relations are transitive, $y \sim a$. By definition of a relation class, $a \in [y]$. Since a is an arbitrary element of $[x]$, $[x] \subseteq [y]$.

Let b be an arbitrary element of $[y]$. By definition of the relation class, $y \sim b$. Since equivalence relations are transitive and $x \sim y$, $x \sim b$, hence $b \in [x]$. Since b is an arbitrary element of $[y]$, $[y] \subseteq [x]$.

By definition of set equality, $[x] = [y]$.

b $\boxed{\text{proof}}$ Using the same instantiations used in the previous proof for $\sim$, and A. Let x and y be arbitrary elements in A. Suppose by way of contrapositive that $[x] \cap [y] \neq \emptyset$, that is, there exists some element a which is in $[x]$ and $[y]$. By definition of the relation class, $x \sim a$ and $y \sim a$. Since equivalence relations are symmetric, $a \sim x$. Since equivalence relations are transitive, $x \sim y$.

By way of contrapositive, if $x \not\sim y$, then $[x] \cap [y] = \emptyset$.

c $\boxed{\text{proof}}$ Let x be an arbitrary element in A. Since $\sim$ is reflexive, $(x, x) \in\sim$. Furthermore, by definition of the relation class, $x \in [x]$. Thus, by definition of the union of an indexed family of sets, $x \in \bigcup_{[x]\in A/\sim}[x]$.
Since x is arbitrary, $A \subseteq \bigcup_{[x]\in A/\sim}[x]$.
Let y be an arbitrary element in $\bigcup_{[x]\in A/\sim}[x]$. By definition of the union of an indexed family of sets, there exists some $[y]$ such that $y \in [y]$. By definition of the relation class, $(y, y) \in\sim$. Furthermore, since $\sim$ is a relation on A, $y \in A$. Since y is arbitrary, $A \subseteq \bigcup_{[x]\in A/\sim}[x]$.

By set equality, $\bigcup_{[x]\in A/\sim}[x] = A$.

Problem 5.3.14

Let A be a non-empty set, and let E_1 and E_2 be equivalence relations on A with associated partitions $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively. Let E be the equivalence relation on A defined by $E = E_1 \cap E_2$, and $\mathcal{D}$ its associated partition. Let $\mathcal{D}$ denote the partition of A corresponding to E. Define $\mathcal{D}$ in terms of $\mathcal{D}_1$ and $\mathcal{D}_2$ and prove your result.

proposition: $\mathcal{D} = \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset$.

proof (Proof by Determination) Let A be an arbitrary non-empty set, and let E_1 and E_2 be arbitrary equivalence relations on A, with associated partitions $\mathcal{D}_1 = A/E_1$ and $\mathcal{D}_2 = A/E_2$. Define the relation $E = E_1 \cap E_2$, and its associated partition $\mathcal{D} = A/E$.

- Let $[x]_E$ be an arbitrary element in $\mathcal{D}$. Because, E is a relation on A, it follows that $x \in A$ By definition of partitions, there exists some unique $P \in \mathcal{D}_1$ and $Q \in \mathcal{D}_2$ such that $x \in P$ and $x \in Q$. Let P and Q be elements of $\mathcal{D}_1$ and $\mathcal{D}_2$ respectively such that $x \in P$ and $x \in Q$. We now need to verify that $[x]_E = P \cap Q$.

  This leads to a set equality proof.

  - Let a be an arbitrary element in $[x]_E$. By of equivalence relations, $(x, a) \in E$. Furthermore, by definition of E, $(x, a) \in E_1$ and $(x, a) \in E_2$. By definition of the relation class, $a \in [x]_{E_1}$ and $[x]_{E_2}$. Since P and Q are unique, it follows that $[x]_{E_1} = P$ and $[x]_{E_2} = Q$. It follows that $a \in P$ and $a \in Q$. By intersection, $a \in P \cap Q$. Since a is arbitrary, for all $a \in [x]_E$, $a \in P \cap Q$. Hence, $[x]_E \subseteq P \cap Q$.
  - Let p be an arbitrary element in $P \cap Q$. By intersection, it follows that $p \in P$ and $p \in Q$. Furthermore, since $P \in \mathcal{D}_1$ and $x \in P$, $P = [x]_{E_1}$. Similarly, since $P \in \mathcal{D}_2$ and $x \in P$, $P = [x]_{E_2}$. Since $p \in P$ and $p \in Q$, it follows that $p \in [x]_{E_1}$ and $p \in [x]_{E_2}$. By definition of the relation class, $(p, x) \in E_1$ and $(p, x) \in E_2$. By definition of the intersection, $(p, x) \in E_1 \cap E_2$. Thus, by definition of E, $(p, x) \in E$. Furthermore, by definition of the relation class, $p \in [x]_E$. Since p is arbitrary, for all $p \in P \cap Q$, $p \in [x]_E$. Hence $P \cap Q \subseteq [x]_E$.

  Since $P \cap Q \subseteq [x]_E$ and $[x]_E \subseteq P \cap Q$, it follows by definition of set equality that $[x]_E$. Furthermore, since $[x]_E$ is an arbitrary element in $\mathcal{D}$, it follows that for all $X \in \mathcal{D}$, $X \in \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset$. Hence, $\mathcal{D} \subseteq \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset$.

- Let S be an arbitrary element in $\{P \cap Q | P \in \mathcal{D}_1, Q \in \mathcal{D}_2\} - \emptyset$. By set difference, $S \neq \emptyset$, hence there exists some element $a \in S$.Furthermore, $S = P \cap Q$ for some $P \in \mathcal{D}_1$ and some $Q \in \mathcal{D}_2$. By intersection, $a \in P$ and $a \in Q$. Since P and Q are elements of $\mathcal{D}_1$ and $\mathcal{D}_2$ respectively, it follows that $a \in [a]_{E_1}$ and $a \in [a]_{E_2}$.

  - Let x be an arbitrary element in S. Since $S = P \cap Q$, by intersection it follows that $x \in P$ and $x \in Q$, hence $x \in [a]_{E_1}$ and $x \in [a]_{E_2}$. By definition of the equivalence class, $(x, a) \in E_1$ and $(x, a) \in E_2$. Hence, by the intersection, $(x, a) \in E$. By definition of the equivalence class, $x \in [a]_E$. Since x is arbitrary, it follows that $S \subseteq [a]_E$.
  - Let y be an arbitrary element in $[a]_E$. By definition of the equivalence class, $(a, y) \in E = E_1 \cap E_2$. Furthermore, by definition of E and intersection, $(a, y) \in E_1$ and $(a, y) \in E_2$. By definition of the equivalence class, $y \in [a]_{E_1}$ and $y \in [a]_{E_2}$. By substitution, $y \in P$ and $y \in Q$. By the intersection, $y \in P \cap Q = S$. Since y is arbitrary, $[a]_E \subseteq S$.

  Since $S \subseteq [a]_E$ and $[a]_E \subseteq S$, it follows by set equality that $S = [a]_E$. By definition of the quotient set, $[a]_E \in A/E$. By substitution and by definition of $\mathcal{D}$, $S \in \mathcal{D}$. Since S is an arbitrary element in $\mathcal{D} \subseteq \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset$, by definition of a subset, $\mathcal{D} \subseteq \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset \subseteq \mathcal{D}$.

Having shown that $\mathcal{D} \subseteq \mathcal{D} \subseteq \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset \subseteq \mathcal{D}$, and $\mathcal{D} \subseteq \mathcal{D} \subseteq \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset \supseteq \mathcal{D}$, it follows by definition of set equality that $\mathcal{D} \subseteq \mathcal{D} \subseteq \{P \cap Q | P \in \mathcal{D}_1, Q \in D_2\} - \emptyset = \mathcal{D}$

■