Homework 1 Solutions

For the problems themselves, see Dr. Pop's website.

1 (a) Associativity of Δ:

$$\begin{aligned}(A\Delta B)\Delta C &= (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A))) \\ &= ((A \setminus B) \setminus C) \cup ((B \setminus A) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A)))\end{aligned}$$

Now, $(A \setminus B) \setminus C = A \setminus (B \cup C)$, and so this becomes $(A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus ((A \setminus B) \cup (B \setminus A)))$. Also, $C \setminus (A\Delta B)$ is equal to the set of elements of C which are not in precisely one of A or B, and so $C \setminus (A\Delta B)$ is equal to $C \setminus (A \cup B)$ union with $A \cap B \cap C$. Thus, $(A\Delta B)\Delta C = (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B)) \cup (A \cap B \cap C)$. Working backwards, but changing the roles of the three sets, we obtain $(A\Delta B)\Delta C$.

Identity of Δ: We need a set such that $A\Delta x = A$ for all A. That is, that $(A \setminus x) \cup (x \setminus A) = A$. If $x = \emptyset$, then $A \setminus \emptyset = A$ and $\emptyset \setminus A = \emptyset$, so their union is A.

Commutativity of Δ: $A\Delta B = (A \setminus B) \cup (B \setminus A)$, and as $\cup$ is commutative, this is $(B \setminus A) \cup (A \setminus B) = B\Delta A$.

Associativity of $\cdot$: $(A \cdot B) \cdot C) = (A \cap B) \cap C = A \cap (B \cap C)$ by the associativity of intersection, and so we have $A \cdot (B \cdot C)$.

Identity of $\cdot$: We need a set such that $A \cdot x = A$ for all A. That is, $A \cap x = A$. So, in particular, $A \subset x$ for all A. The only option, then, is $x = X$. And then, $A \cap X$ does, in fact, equal A for all A.

Commutativity of $\cdot$:

(b) To show that it is a ring, we must still prove that Δ has inverses and that $A \cdot (B\Delta C) = A \cdot B\Delta A \cdot C$. So see that Δ has inverses, we just look at $A\Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset$. Seeing distributivity is a bit harder, we start with $A \cdot (B\Delta C)$. This is equal to $A \cap (B \setminus C \cup C \setminus B)$.

As a lemma, we prove that $A \cap (B \setminus C) = A \cap B \setminus (A \cap C)$. Let $x \in A \cap (B \setminus C)$. Then $x \in A$ and $x \in B \setminus C$. So $x \in A$ and $x \in B$ and $x \notin C$. Similarly, let $x \in A \cap B \setminus (A \cap C)$. Then $x \in (A \cap B)$ and $x \notin (A \cap C)$. So $x \in A$ and $x \in B$ and $x \notin A \cap C$. As $x \in A$ already, $x \notin A \cap C$ if and only if $x \notin C$, and so the two conditions are both $x \in A$, $x \in B$ and $x \notin C$. Thus, the lemma is proved.

Now, we have $A \cap (B \setminus C \cup C \setminus B)$. As $\cap$ distributes over $\cup$, we have $A \cap (B \setminus C) \cup A \cap (C \setminus B)$. This is equal to, by the lemma, $A \cap B \setminus (A \cap C) \cup (A \cap C) \setminus (A \cap B) = (A \cdot B) \setminus (A \cdot C) \cup (A \cdot C) \setminus (A \cdot B) = (A \cdot B) \Delta (A \cdot C)$.

(c) Fix $A \in \mathcal{P}(X)$. Then $A \cdot A = A \cap A = A$.

2 Let $x, y \in R$. Note that $(x + x)^2 = x^2 + 2x^2 + x^2 = 4x^2$, but, because R is boolean, we also have that $(x + x)^2 = x + x = 2x$ and $x^2 = x$, thus, $4x = 2x$, and so $2x = 0$, which implies that $x = -x$ for all elements of R. Now look at $(x + y)^2 = x + y$. The left hand side expands to $x^2 + xy + yx + y^2$, and as R is boolean, we have $x + xy + yx + y = x + y$, and so $xy + yx = 0$. thus, $xy = -yx = yx$, and so R is commutative.

4 (a) Let A, B be finite and nonempty. Then, $A \times B = \{(a, b) | a \in A, b \in B\}$. It will be finite, as there are only finitely many possibilities to go into the coordinate a and also only finitely many for b. Conversely, assume that $A \times B$ is finite. Then there are natural functions $A \times B \to A$ and $A \times B \to B$ given by $(a, b) \mapsto a$ and $(a, b) \mapsto b$. These are both surjective, by definition, and so A and B must be finite, as no finite set can surject onto an infinite set. This does not hold if A or B is empty. For instance, $A = \emptyset$, $B = \mathbb{Z}$, then $A \times B = \emptyset$, and so is finite, but is a product of an infinite set and a finite (empty) set.

(b) Let A and B be finite. If either is empty, then $A \times B$ is, and so $|A \times B| = |A||B| = 0$. So we may assume that they are nonempty. Then A is in bijection with $\{1, \ldots, n\}$ and B with $\{0, \ldots, m\}$, so we label the elements $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$. Now, the product is $A \times B = \{(a, b) | a \in A, b \in B\}$, and we can label $(a_i, b_j) = c_{ij}$. So then $A \times B = \{c_{ij} | i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$. Thus, there are nm possibilities for c_{ij}, and so $|A \times B| = nm = |A||B|$.

(c) First we see that $|X| \leq |\mathcal{P}(X)|$. This is because there is always an injection $a \mapsto \{a\}$ from X to $\mathcal{P}(X)$. All that remains is to show that this inequalitiy is strict. Assume that it isn't, that is, that there exists a bijection $f : X \to \mathcal{P}(X)$. Then there is a set in the image defined by $B = \{x \in X | x \notin f(x)\}$. As f is a bijection, and hence surjective, there exists $x_0 \in X$ such that $f(x_0) = B$. Now, if $x_0 \in B$, then $x_0 \in f(x_0)$, but that contradicts the definition of B, that is that $x \notin f(x_0)$. Similarly, if $x_0 \notin B$, then $x_0 \notin f(x_0)$, and so x_0 must be in B, another contradiction. Thus, assuming the existence of a bijection leads to a contradiction, so one must not exist, and so the statemnet is proved.

7 (a) As $*$ is associative on M, it must be on G. So we must check that G has a neutral element, inverses, and is closed under $*$. The neutral element is in G, as $e * e = e$, and so it has an inverse. Similarly, if $x \in G$ then $x^{-1} \in G$, as x is an inverse for x^{-1}. All that remains is closure. Let $x, y \in G$, we must show $xy \in G$. That amounts to

providing an inverse. An inverse for xy is $y^{-1}x^{-1}$, and so G is closed under $*$, and so is a group.

(b) Let $x' \in M$. It has left inverse $x \in M$. Similarly, x has left inverse x''. So $xx' = e$ and $x''x = e$. So we look at $(x''x)x' = x'$, but as M is associative, $(x''x)x' = x''(xx') = x''$ and so $x' = x''$, and so x has a two-sided inverse.

(c) Here we must classify all groups of order less than or equal to seven.

m=1 The only group of order one is the trivial group.

m=2 By Fermat's Little Theorem (Corollary 4 and 5 on page 44 of Herstein), any group of prime order is a cyclic group. Thus, the only group of order 2 is C_2.

m=3 Similar to $m = 2$, we have the only group being C_3.

m=4 Here is the first interesting case. As $m = 4$ it is not prime. Now, the order of any element must be a divisor of four, so we get two cases. If there exists an element of order four, then we have C_4. So now let us assume that there is no element of order 4. Then every element other than the identity must be of order 2. So we can posit the existence of two elements of order two, a and b, which give the group the description as $\{e, a, b, ab\}$. Now, the group must be abelian, because ba cannot be the identity, as then $ab = e$ as well, nor can $ab = a$ or $ab = b$, as then $b = e$ or $a = e$, so this group is abelian. The whole multiplication is determined, then, and so the group is $C_2 \times C_2$.

m=5 As before, we have C_5

m=6 Here we have the only other nonprime number. First we look at the case where there is an element of order 6. Then $G \cong C_6$, and so we can assume that there are no elements of order six. By Cauchy's Theorem (2.11.4 on page 87), there exist elements a of order 3 and b of order two. The group can be described, as a set, by $\{e, a, a^2, b, ab, a^2b\}$. The claim is that this uniquely determines the multiplication table. To check this, we will derive the rows. The first row is left multiplication of elements by e, which is just the identity. The second is left multiplication by a, which is also dictated by the form of the elements and the fact that $a^3 = e$. Similarly for the third row, left multiplication by a^2. The only products left to determine are $ba, ba^2, bab, ba^2b, aba, aba^2, abab, aba^2b, a^2ba, a^2ba^2, a^2bab, a^2ba^2b$. Now, $abab$ and a^2ba^2b are really $(ab)^2$ and $(a^2b)^2$, which must be the identity. This is because ab and a^2b must be of order two, as if there were two distinct elements a, b of order three, without $a^2 = b$, then the group would have order at least nine. Now, as $abab = e$, we right multiply by b to obtain $aba = b$, and left multiply by a^2 to get $ba = a^2b$. Now, with $ba = a^2b$ in hand, we have that $ba^2 = a^2ba = a^2(a^2b) = ab$, that $bab = (a^2b)b = a^2$, that

$ba^2b = (ab)b = a$, $aba^2 = a(ba)a = a(a^2b)a = a^3ba = ba = a^2b$, $aba^2b = a(ba)ab = a(a^2b)(ab) = bab = a^2$, $a^2ba = a^2(a^2b) = ab$, $a^2ba^2 = aba = b$, and finally that $a^2bab = a^2(a^2b)b = a^4b^2 = a$, forcing the whole multiplication table. So there is a unique non-abelian group of order six, and it must by S_3, with an isomorphism obtained by $a \mapsto (123)$ and $b \mapsto (12)$.

m=7 As before, we have C_7.

(d) As $\sigma^5 = (134)$ is of order three, we can cube both sides to obtain $\sigma^{15} = e$. Thus, σ has order dividing 15, and must be 1,3,5 or 15. Now, it can't be 1, as then $\sigma = e$, and it can't be 5 or 15, as no element of S_4 has either of those orders (nor any order greater than 4), and so $\sigma^3 = e$. Thus, $\sigma^5 = \sigma^2\sigma^3 = \sigma^2 = (134)$. As σ is order three, $\sigma^2 = \sigma^{-1}$, and so there is a unique permutation whose fifth power is (134), and it is the inverse of (134), which is (143). Now for $\tau^2 = (1432)$, we note that this has order four. So we take each side to the fourth power to obtain $\tau^8 = e$. Then τ has order 1,2,4 or 8. It cannot be 1, as then $\tau = e$, nor 2, as then $\tau^2 = e \neq (1432)$, nor can it be 8, as no elements have order 8. Thus, τ must have order four. However, if τ has order four, then τ^2 has order two, and so τ cannot have order 4 either. There is no allowable order, and thus no such τ can exist.

8 (a) We rewrite the system of linear equations as an equation of matrices $\begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} b \\ c \end{pmatrix}$. Thus, the condition is that $\begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix}$ has an inverse over our ring R. Now, if there is an inverse, we can write it as $\frac{1}{a^2-1}\begin{pmatrix} a & -1 \\ -1 & a \end{pmatrix}$, and so the condition is that $a^2 - 1$ has to be invertible, as everything else always makes sense. Thus, $a^2 - 1$ must be in the list 5,7,11,13,17,19,23,25,29,31,35 which are invertible (because they are relatively prime to 36. And so, a^2 must be in the list $6, 8, 12, 14, 18, 20, 24, 26, 30, 32, 36 = 0$. So now we must merely determine which of these are squares modulo 36. The list of squares is $1, 4, 9, 16, 25, 0, 13, 28$. The only number on both lists is 0. So $a^2 = 0$. Thus, a is on the list $0, 6, 12, 18, 24, 30$, as all square to zero, modulo 36.

(b) Here, however, every element other than 0 is coprime to 37 and so is invertible, thus $a^2 - 1 \neq 0$, and so $a^2 \neq 1$, so $a \neq \pm 1$, thus, we just need $a \neq 1, 36$ in order to have a unique solution.

(c) The difference between the two cases is that 37 is a prime number, and so $\mathbb{Z}/37\mathbb{Z}$ is a field, whereas $\mathbb{Z}/36\mathbb{Z}$ is not, and has a lot of noninvertible elements and zerodivisors.