SOLUTION KEY
Produced by: Kyle Dahlin

Problem 0.58. Let S be the set of real numbers. If $a, b \in S$, define $a \sim b$ if $a - b$ is an integer. Show that $\sim$ is an equivalence relation on S. Describe the equivalence classes of S.

Solution: We must show that the relation defined by $\sim$ is **reflexive**, **symmetric**, and **transitive**. Let $a, b, c \in S$.

Reflexivity:

Clearly $a - a = 0$ is an integer, hence $a \sim a$ and $\sim$ is reflexive.

Symmetricity:

Suppose that $a \sim b$. Then there is an integer n such that $a - b = n$. Since $b - a = -(a - b) = -n$ is also an integer, $b \sim a$. Hence $\sim$ is symmetric.

Transitivity:

Suppose that $a \sim b$ and $b \sim c$. There are integers m and n such that $a - b = m$ and $b - c = n$. Since $a - c = (a - b) + (b - c) = m + n$ is also an integer, $a \sim c$. Hence $\sim$ is transitive.

An equivalence class, A, of S under $\sim$ is a set of real numbers with the property that if $a, b \in A$, then $10^n(a - b) \bmod 10^n = 0$ for all $n \in \mathbb{N}$. Loosely speaking, a and b have the same digits after the decimal point. ■

Problem 0.59. Let S be the set of integers. If $a, b \in S$, define aRb if $ab \geq 0$. Is R an equivalence relation on S?

Solution: No, because R is not transitive. For example, if $a = 1$, $b = 0$, and $c = -1$ then aRb and bRc since $ab = bc = 0$. However, $ac = -1 < 0$, so that $a \not R c$. ■

Problem 2.6. In each case, perform the indicated operation:

a. In $\mathbb{C}^*$, $(7 + 5i)(-3 + 2i)$

b. in $GL(2, Z_{13})$, $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$

c. In $GL(2, \mathbb{R})$, $\begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}^{-1}$

d. In $GL(2, Z_{13})$, $\begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}^{-1}$

Solution:

a. In $\mathbb{C}^*$, $(7 + 5i)(-3 + 2i) = -21 + 14i - 15i + 10i^2 = -31 - i$

b. in $GL(2, Z_{13})$, $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix} = 35 - 4 \bmod 13 = 31 \bmod 13 = 5 \bmod 13$

c. In $GL(2, \mathbb{R})$, $\begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}^{-1} = \dfrac{1}{31} \begin{bmatrix} 5 & -4 \\ -1 & 7 \end{bmatrix}$

d. In $GL(2, Z_{13})$, $\begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}^{-1} = 8 \begin{bmatrix} 5 & 9 \\ 12 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 7 \\ 5 & 4 \end{bmatrix}$

■

Problem 2.16. Show that the set 5, 15, 25, 35 is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?

Solution: We must show first that the set $S = \{5, 15, 25, 35\}$ is **closed** under multiplication modulo 40, that the group G of S with multiplication modulo 40 is **associative**, has an **identity**, and each element has an **inverse**.

A Cayley table will help us to illustrate that G has all of these properties.

mod 40	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

S is closed under multiplication modulo 40 because each element of the table belongs to S. We see that the identity element is 25. Since 25 shows up in each row, each element has an inverse. It remains to show that the operation of G is associative.

By Problem 0.9, we know that for any integers a, b, n:

$$ab \bmod n = (a \bmod n)(b \bmod n).$$

Hence, since regular multiplication is associative:

$$\begin{aligned}(ab \bmod 40)(c \bmod 40) &= (ab)c \bmod 40 \\ &= a(bc) \bmod 40 \\ &= (a \bmod 40)(bc \bmod 40)\end{aligned}$$

for any $a, b, c \in S$. ■

Problem 2.18. List the members of $H = \{x^2 | x \in D_4\}$ and $K = \{x \in D_4 | x^2 = e\}$

Solution: A Cayley table of D_4 can be found on page 33 of your textbook. We can read off the diagonal of this table to find that: $H = \{R_0, R_{180}\}$ and $K = \{R_0, R_{180}, H, V, D, D'\}$
■

Problem 2.31. Prove that every group table is a Latin square; that is, each element of the group appears exactly once in each row and each column.

Solution: Suppose that G is a group whose Cayley table is not a Latin square. Then there is at least one row or column where an element appears more than once. That is, there must be *distinct* elements $a, b, c \in G$ such that $ab = ac$. However, by **Theorem 2.2**, cancellation implies that $b = c$, which is impossible since b and c were distinct. Hence there is no such group G and every group table must be a Latin square. ■

Problem 2.32. Construct a Cayley table for $U(12)$.

Solution: $U(12)$ is the group comprised of the set $\{1, 5, 7, 11\}$ together with the operation of multiplication modulo 12.

mod12	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

■

Problem 2.33. Suppose the table below is a group table. Fill in the blank entries.

	e	a	b	c	d
e	e	–	–	–	–
a	–	b	–	–	e
b	–	c	d	e	–
c	–	d	–	a	b
d	–	–	–	–	–

Solution:

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

■

Problem 2.42. Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n such that $F_1F_2 = F_2F_1$. Prove that $F_1F_2 = R_{180}$.

Solution: As described in **Table 2.1** of the textbook, elements of D_n are made up of rotations, R_i, and a reflection, L. Here R_i corresponds to a rotation of $\frac{360i}{n}$ degrees for $0 \le i \le n$. Note also that $L^2 = R_0$, the identity.

Lemma 1. *$LR_iL = R_i^{-1}$ for all i.*

Proof. Any reflection has the form LR_i for some i. Since if we apply the same reflection twice, we return to the original orientation, we know that $(LR_i)(LR_i) = R_0$. Hence $LR_iL = R_i^{-1}$. ■

Let F_1 and F_2 be distinct reflections in D_n. Then $F_1 = R_iL$ and $F_2 = R_jL$ for some $i \neq j$. Suppose now that $F_1F_2 = F_2F_1$. Then

$$\begin{aligned} R_iLR_jL &= R_jLR_iL \\ R_iR_j^{-1} &= R_jR_i^{-1} \\ (R_j^{-1}R_i)(R_j^{-1}R_i) &= R_0 \\ R_\gamma^2 &= R_0 \end{aligned}$$

where $R_\gamma = R_j^{-1}R_i$ and we have used that $LR_iL = R_i^{-1}$ by **Lemma 1**. The only rotations that may square to the original configuration are R_0 or $R_{n/2} = R_180$ (see **Problem 2.18**). Note that $R_{n/2}$ is only a proper rotation in D_n is n is even.

Now we show that $F_2F_1 = R_\gamma$

$$\begin{aligned}
F_2F_1 &= F_1F_2 \\
R_jLF_1 &= R_iLF_2 \\
LF_1 &= R_\gamma LF_2 \\
F_1 &= LR_\gamma LF_2 \\
F_1 &= R_\gamma^{-1}F_2 \\
F_1F_2 &= R_\gamma F_2^2 \\
F_1F_2 &= R_\gamma
\end{aligned}$$

Now if $R_\gamma = R_0$, then $F_1 = F_2$, which cannot happen since we assumed they are distinct. Hence $R_\gamma = R_{180}$, as desired. ■

Problem 2.45. In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write each of the following products in the form R^i or R^iF, where $0 \leq i < n$.

a. In D_4, $FR^{-2}FR^5$

b. In D_5, $R^{-3}FR^4FR^{-2}$

c. In D_6, $FR^5FR^{-2}F$

Solution: We will apply **Lemma 1** throughout this problem.

a. In D_4, $FR^{-2}FR^5$

$$\begin{aligned}
FR^{-2}FR^5 &= R^2R^5 \\
&= R^7 \\
&= R^3
\end{aligned}$$

since $7 \equiv 3 \bmod 4$.

b. In D_5, $R^{-3}FR^4FR^{-2}$

$$\begin{aligned}
R^{-3}FR^4FR^{-2} &= R^{-3}R^{-4}R^{-2} \\
&= R^{-9} \\
&= R
\end{aligned}$$

since $-9 \equiv 1 \bmod 5$.

c. In D_6, $FR^5FR^{-2}F$

$$\begin{aligned}
FR^5FR^{-2}F &= R^{-5}R^{-2}F \\
&= R^{-7}F \\
&= R^5F
\end{aligned}$$

since $-7 \equiv 5 \bmod 6$.

■