So far we’ve introduced the notion of a group $G$, a ring $R$, and a field $F$ and given examples of them. One very important idea is to use equivalence relations to produce new examples from old examples or, most critically, to construct new examples. Let’s begin with the notion of equivalence relation in complete generality - notice how we keep stripping all the structure from examples of mathematical objects except for the structure we want to isolate!

**Definition 1.** An EQUIVALENCE RELATION on a set $S$ is a subset $E$ of $S \times S$ such that

1. **(Reflexitivity)** $(a, a) \in E$,
2. **(Symmetry)** $(a, b) \in E \implies (b, a) \in E$,
3. **(Transitivity)** $(a, b), (b, c) \in E \implies (a, c) \in E$

hold for all $a, b$ and $c$ in $S$.

This looks more familiar perhaps if we write $a \equiv b$ instead of $(a, b) \in E$.

**Problem 1.** Define $\equiv_n$, $n$ a fixed positive integer, $\equiv_\leq$, and $\equiv_<$ respectively on integers $a, b$ by

1. $a \equiv_n b$ when $a - b = mn$ for some integer $m$;
2. $a \equiv_\leq b$ when $a \leq b$;
3. $a \equiv_< b$ when $a < b$.

Which of these define an equivalence relation on $\mathbb{Z}$? For those that fail, point out which of the properties in Definition 1 do not hold.

To proceed more generally than in class, suppose $\equiv$ is an equivalence relation on a set $S$ and set

$$[a] = \{ b \in S : a \equiv b \}.$$ 

We call $[a]$ the Equivalence Class of $a$. These equivalence classes have some crucial properties.
**Problem 2.** If $\equiv$ is an equivalence relation on a set $S$, then

1. $a \in [a]$,
2. $a \in [b] \implies [a] = [b]$;
3. $[a] = [b]$ if and only if $a \equiv b$;
4. either $[a] = [b]$, or $[a], [b]$ are disjoint.

By property (4), therefore, an equivalence relation $\equiv$ on a set $S$ partitions the set $S$ into **mutually disjoint** equivalence classes. For convenience, we shall denote this family of equivalence classes by $S/\equiv$ for reasons that will become clearer when we get to the case when $S$ is a group.

Now suppose that $\circ$ is a binary operation on $S$. A fundamental question is whether we can use $\circ$ to introduce an associated binary operation on the set $S/\equiv$. An obvious approach suggests itself: given equivalence classes $[a], [b]$ define $[a] \circ [b]$ by

$$[a] \circ [b] = [a \circ b].$$

The right hand side makes sense because $a \in [a]$ and $b \in [b]$. For (2.1) to make good sense though, we have to show that the equivalence class $[a \circ b]$ does not depend on the choice of $a$ in $[a]$ and $b$ in $[b]$. Under a simple property of $\equiv$ this is true (see Lemma 1.7.5 in the text for the special case of $\equiv_n$).

**Problem 3.** Suppose that $\circ$ is a binary operation on $S$ and that $\equiv$ is an equivalence relation on $S$. Show that if

$$a \equiv x, \ b \equiv y \implies a \circ b \equiv x \circ y,$$

then

$$x \in [a], \ y \in [b] \implies [x \circ y] = [a \circ b];$$

in other words, under condition (‡) the equivalence class $[a \circ b]$ does not depend on the choice of $x \in [a]$ and $y \in [b]$, so

$$[a] \circ [b] = [a \circ b]$$

defines a binary operation on $S/\equiv$.

Armed with Lemma 1.7.5 in the text we can investigate the algebraic structure on the set $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$ for each fixed positive integer $n$. The standard addition and multiplication on $\mathbb{Z}$ passes to $\mathbb{Z}_n$ setting

$$[m] + [n] = [m + n], \quad [m] \times [n] = [m \times n].$$
Proposition 1.7.7 in the text now shows not surprisingly that \((\mathbb{Z}_n, +, \times)\) is a ring in which \([0]\) is the additive identity and \([1]\) is the multiplicative identity. The notation \([a]\) for elements of \(\mathbb{Z}_n\) is clumsy - for instance, we surely don’t want to think of the equivalence classes \([99]\) or \([2045]\) as elements of the binary arithmetic system \(\mathbb{Z}_2\) or of the hexadecimal system \(\mathbb{Z}_{16}\).

Lemma 1.7.3 and Corollary 1.7.4 show how to simplify this labelling problem: for each \(a \in \mathbb{Z}\), there is a unique integer \(r\), such that

\[ 0 \leq r < n, \quad a = mn + r, \]

for some integer \(m\); in other words, \(r/n\) is the fractional remainder after dividing \(a\) by \(n\). Thus each

\[ [a] \sim r, \quad 0 \leq r < n, \]

uniquely labels the elements of \(\mathbb{Z}_n\) and

\[ [a] = [r], \quad [a] + [b] = [s], \quad [a] \times [b] = [t] \]

with

\[ s = r_a + r_b \pmod{n}, \quad t = r_a \times r_b \pmod{n} \]

is standard arithmetic modulo \(n\). Example 1.7.8 and some of the problems in Exercises 1.7 illustrate these ideas numerically.

**Problem 4.** (1) Show that \(a^7 \equiv a \pmod{7}\) holds for every integer \(a\);

(2) Compute \([4^{437}]\) in \(\mathbb{Z}_{12}\).

Now comes the first pay-off for studying these ideas as generally as we did. Notice that everything we’ve done for \((\mathbb{Z}, +, \times)\) applies equally well to the ring \(\mathcal{P}(\mathbb{R})\) of all polynomials

\[ P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \]

of arbitrary degree \(n\) having coefficients \(a_0, a_1, a_2, \ldots, a_n\) in the ring \(\mathbb{R}\). Indeed, given polynomials \(P, Q\) with realcoefficients, we can add and multiply them to form new polynomials \(P + Q\) and \(PQ\) because all this requires is the ability to *add and multiply the coefficients*. But \(\mathbb{R}\) is also a field, so we can also divide coefficients. This is all that’s needed to carry out LONG DIVISION of polynomials having real coefficients.

**Problem 5.** Set \(Q(x) = 1 + x^2\).

(1) Determine unique polynomials \(S\) and \(R\) so that

\[ P(x) = S(x)Q(x) + R(x), \quad \deg(R) < 2, \]

when \(P(x) = 5x^3 + 2x^2 + 3x + 7\).
(2) More generally, show that
\[ P_1 \equiv_Q P_2 \text{ when } P_1(x) - P_2(x) = S(x)Q(x) \]
for some \( S \in \mathcal{P}(\mathbb{R}) \) defines an equivalence relation on \( \mathcal{P}(\mathbb{R}) \).

(3) Show that \( \equiv_Q \) has property (†) in Problem 3.

Granted Problem 5, the usual addition and multiplication of polynomials passes to the set \( \mathcal{P}(\mathbb{R})/\equiv_Q \) of equivalence classes of polynomials. Consequently, under the notation
\[
(\mathbb{C}, + , \times) = \left( \mathcal{P}(\mathbb{R})/\equiv_Q, + , \times \right),
\]
\( \mathbb{C} \) becomes a ring under addition and multiplication.

**Exploration.** (1) Devise a labelling of elements in \( \mathbb{C} \).

(2) Identify \( \mathbb{C} \) with a familiar ring in mathematics.