Math 309 – Intermediate Linear Algebra **Homework 1** **Xida Ren**

(Due Friday, February 2)

- **Justify your work. Do not skip steps!**
- You may cite the result of an earlier problem on this homework.
- Each problem will be graded out of 10 points.

1. Prove that congruence modulo n is an equivalence relation on the integers, where $n \in \mathbb{N}$.

We have proven in class that partitions induce equivalence relations.
Congruence modulo n is a partition of the integers into n equivalence classes: we put an integer i into the set numbered k if $i \mod n \equiv k$.
Each integer belongs to at least one class because every integer has a remainder $\mod n$.
Each integer belongs to no more than one class because there can't be two remainders.

Fix $n \in \mathbb{N}$ and define $\mathbb{Z}_n$ to be the set of equivalence classes of integers under congruence modulo n. For $[a], [b] \in \mathbb{Z}_n$, we define addition modulo n by $[a] \oplus [b] := [a + b]$, and we define multiplication modulo n by $[a] \odot [b] := [ab]$.

2. Prove that addition modulo n is well-defined, i.e., if $a_1 \equiv a_2 \pmod n$ and $b_1 \equiv b_2 \pmod n$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod n$. (In other words, addition modulo n does not depend on the choice of representative of the equivalence class.)

By definition of modular equilavence, $a_1 = a_2 + in$ and $b_1 = b_2 + jn$. So

$$(a_1 + b_1) - (a_2 + b_2) = in + jn = (i + j)n$$

which gives us the desired result after one more application of the definition.

3. Prove that multiplication modulo n is well-defined, i.e., if $a_1 \equiv a_2 \pmod n$ and $b_1 \equiv b_2 \pmod n$, then $a_1 b_1 \equiv a_2 b_2 \pmod n$. (In other words, multiplication modulo n does not depend on the choice of representative of the equivalence class.)

With the same setup as the last problem,

$$a_1 b_1 - a_2 b_2 = a_2 b_2 + a_2 jn + b_2 in + injn - a_2 b_2$$
$$= (a_2 j + b_2 i + ijn)n$$

which is what we need for the definition of modular equivalence.
Problems 2 and 3 show why it is acceptable to write $\mathbb{Z}_n = \{0, 1, \ldots, (n-1)\}$ *with operations* $+$ *and* $\cdot$.

4. Prove that function composition is associative; that is, if $f : A \to B$, $g : B \to C$, and $h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

To prove the composed functions are equal, we prove that for equal input they generate the same output. Indeed:
$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$.

5. Let $f : A \to B$ and $g : B \to C$ be functions.

(a) Prove that, if f and g are injective, then the composition of f and g (namely, $g \circ f$) is also injective.

let $h = g \circ f$. We prove that by the injectivity of f and g, h is also injective. Namely, two distinct elements x_1 and x_2 cannot be mapped to the same y.

Suppose that h is not injective, such that for some $x_1 \neq x_2$, $h(x_1) = h(x_2)$. That means that $g(f(x_1)) = g(f(x_2))$. Because f is injective, this implies that $g(x_1) = g(x_2)$. Because g is injective, we now have $x_1 = x_2$, a contradiction. So h must be injective.

(b) Prove that, if f and g are surjective, then the composition of f and g (namely, $g \circ f$) is also surjective.

Let $h = g \circ f$. We prove that surjectivity of f and g implies that for all y in the range of h, there exists an x such that $h(x) = y$. Choose any y in the range of h. Because g is surjective, there exists a z such that $g(z) = y$. Because f is surjective, there exists an x such that $f(x) = z$.

So $h(x) = g(f(x)) = y$.

Let $\mathrm{id}_A : A \to A$ be the *identity function* on A, that is, the function defined by $\mathrm{id}_A(a) = a$ for all $a \in A$. We define a *left inverse* of a function $f : A \to B$ to be a function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$. We define a *right inverse* of a function $f : A \to B$ to be a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$. An *inverse* (or a *two-sided inverse*) of f is a function that is both a left and a right inverse.

6. Let $f : A \to B$ be a function.

(a) Prove that f is injective if and only if it has a left inverse.

We first prove that having a left inverse implies injectiveness.

Suppose that f has a left inverse g. Since $g \circ f$ is the identity function, for all x_1, x_2, $f(x_1) = f(x_2)$ implies $g(f(x_1)) = g(f(x_2))$. But then because $g \circ f$ is the identity function, $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Hence having a left-inverse implies injectivity.

We then prove that injective functions all have left inverses.

"f injective" implies that for any y in the *codomain* (as distinct from *range*) of f, there is a unique x such that $y = f(x)$. From this fact we construct g, the inverse of f. For all y in the codomain of f, let $g(y) = x$ where x is the unique element of A such that $f(x) = y$.

(b) Prove that f is surjective if and only if it has a right inverse.

Suppose f has a right inverse g. We want to prove from this that the image of f covers every element of B. I.e. for any $b \in B$, there exists an $a \in A$ such that $f(a) = b$. This is accomplished by chosing $a = g(b)$. Since g is defined all over B, we can always find such an a. Hence, having a right inverse implies surjectivity.

Now, suppose f is surjective. We construct a right inverse for f. By surjectivity, for any $b \in B$ there exists at least one $a \in A$ such that $f(a) = b$. Define $g(b)$ by choosing any of these a for an input b. g covers its entire domain because f covers its entire range, and because for all b we chose $g(b) = a$ such that $f(a) = b$, we guarantee that $f(g(b) = f(a) = b$.

(c) Prove that f is bijective if and only if it has an inverse.

If f has an inverse, by (a) and (b) it would be bijective.

If f is bijective, by (a) and (b) it would have a left inverse g and a right inverse h. Calling in associativity, we see that g and h has to be the same:
$g = g \circ id = g \circ f \circ h = id \circ h = h$.

And hence $g = h$ is the double-sided inverse of f.