Here are some comments and partial solutions for Homework 6 Problem 4. Please review this carefully as not only are finite fields important in many areas of mathematics, but these methods/ideas show up later. In particular, the idea of considering equivalence classes as elements of a set shows up literally everywhere in math (as quotient spaces/groups/rings/etc). So in particular, make sure you know how to check whether something “well-defined”. Some of this is more formal and with more details than necessary, but I wanted to make sure you understand the thinking.

(1), (2), (3) What does “well-defined” mean? For example, how do I show that

\[ A : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \]
\[ \overline{a} \times \overline{b} \mapsto \overline{a + b} \]

is well-defined?\(^1\)

**Comment:** Recall that \( \overline{a} = \{ a + kn \mid k \in \mathbb{Z} \} \), i.e. elements of \( \mathbb{Z}_n \) are subsets of \( \mathbb{Z} \). I could just as easily write \( \overline{a}' \), where \( a' \in \mathbb{Z} \) such that \( a' \in \overline{a} \), and then \( \overline{a} = \overline{a}' \) (here \( a \) and \( a' \) are called representatives of \( \overline{a} \)). Since there is nothing canonical about these choices and the definition of \( A \) depends on them, the definition of \( A \) could be ambiguous, i.e. different choices of representatives of \( \overline{a} \) and \( \overline{b} \) could give different images. So what needs to be checked is that if I choose different representatives, I will get the same image (i.e. that this really is a function!).

A correct solution: Let \( a' \in \overline{a} \) and \( b' \in \overline{b} \) be choices of representatives. That is, \( a - a' = k_1n \) and \( b - b' = k_2n \) for some \( k_1, k_2 \in \mathbb{Z} \). Then I want to make sure that \( A(\overline{a} \times \overline{b}) = A(\overline{a'} \times \overline{b'}) \), that is \( \overline{a + b} = \overline{a' + b'} \). This happens if \( n \) divides \( (a + b) - (a' + b') \). Well

\[
(a + b) - (a' + b') = a - a' + b - b' = k_1n + k_2n = (k_1 + k_2)n
\]

which implies that \( \overline{a + b} = \overline{a' + b'} \). We write \( \overline{a + b} \) for \( A(\overline{a} \times \overline{b}) \).

The situation for multiplication is almost exactly the same, only you need to consider \( a'b' - ab \) instead. Checking the associative, commutative and distributive properties does not require anything particularly difficult, but the idea is to simply reduce it to the properties in \( \mathbb{Z} \), for example:

\[
\overline{a + b} = \overline{a + b} = \overline{b + a} = \overline{b + a}
\]

\(^1\)This notation means \( A \) is a map from \( \mathbb{Z}_n \times \mathbb{Z}_n \) to \( \mathbb{Z}_n \) that takes the element \( \pi \times \overline{b} \in \mathbb{Z}_n \times \mathbb{Z}_n \) (also written \( (\pi, \overline{b}) \)) to the element \( a + b \in \mathbb{Z}_n \), that is \( A(\overline{a} \times \overline{b}) = \overline{a + b} \).

\(^2\)It is not correct to say \( \overline{a} = a + kn \) for some \( k \in \mathbb{Z} \)
(4) **A solution:** We will prove the contrapositive: Suppose that \( n = n_1 n_2 \). Then \( \overline{n_1 n_2} = \overline{0} \) in \( \mathbb{Z}_n \). Suppose \( \overline{n} \) has an inverse \( \overline{m} \). Then \( \overline{m} \overline{n_1 n_2} = \overline{m \overline{n_1 n_2}} = \overline{m \overline{0}} = \overline{0} \). So by definition, this means that \( n_2 = kn \) for some \( k \in \mathbb{Z} \). But then \( n = n_1 n_2 = n_1 kn \), which implies that \( n_1 k = 1 \), so since both \( n_1, k \in \mathbb{Z} \), this means \( n_1 = \pm 1 \). This shows that if every element of \( \mathbb{Z}_n \) has an inverse, then \( n \) is prime.

**Note on rings (not required material):** If \( R \) is a ring,\(^3\) the set of elements with multiplicative inverses in \( R \) are called **units**. This uses that the units of \( \mathbb{Z} \) are precisely \( \pm 1 \). It also uses the fact that if \( a \neq 0 \) and \( ab = ac \) in \( \mathbb{Z} \), then \( b = c \) (I’m going to call this property **♠**). Some rings have elements such that \( ab = 0 \) but \( a, b \) are both nonzero. An element \( a \) such that there exists such a \( b \) is called a **zero divisor**. A ring with no zero divisors is called a **division ring** and has property **♠** (why?). This solution shows that if \( n \) is not prime, then \( \mathbb{Z}_n \) has zero divisors. Another example of a ring with zero divisors is \( M_{n \times n}(k) \), the matrix ring over a field \( k \). Can you find zero divisors of \( M_{n \times n}(k) \)? (Note that while \( M_{n \times n} \) is a ring, it is not a commutative ring since multiplication is not commutative.)

(5) Suppose \( p \) is prime. Suppose that \( \overline{m} \in \mathbb{Z}_p \) such that \( \overline{m} \neq 0 \). That means that \( p \nmid m \), since the only positive divisors of \( p \) are 1 and \( p \), this means that \( gcd(m, p) = 1 \). On a previous homework, you proved that this means that there are \( a, b \in \mathbb{Z} \) such that \( am + bp = 1 \). So, if we take \( \overline{am} = \overline{am} = \overline{1} = \overline{-bp} = \overline{1} \). So \( \overline{m} \) is the multiplicative inverse of \( \overline{a} \).

(6) There are a few steps that need to be checked in this proof and I leave as an exercise to you.

Let \( F \) be a field with \( p \) elements. Since it is a field there are elements \( 0_F \) and \( 1_F \in F \) which act as additive and multiplicative identities. For \( k > 0 \), let \( k_F \) denote the sum of \( 1_F \) with itself \( k \) times (that is \( n_F = \underbrace{1_F + \cdots + 1_F}_k \)). Define a map:

\[
\phi : \mathbb{Z}_p \to F \\
\overline{k} \mapsto k_F
\]

where if \( k < 0 \), we can use the division algorithm to choose a nonnegative representative (i.e. there are \( q, r \in \mathbb{Z} \) such that \( 0 \leq r < p \) and \( k = qp + r \), then define \( \phi(\overline{k}) = r_F \)). We need to check that this is well-defined. If \( \overline{k} = \overline{k'} \in \mathbb{Z}_p \) (\( k > k' \geq 0 \)), then there is an \( m \in \mathbb{Z} \) such that \( k - k' = mp \) and \( m \geq 0 \). So \( \phi(k) - \phi(k') = k_F - k'_F = \underbrace{1_F + \cdots + 1_F}_{k} - \underbrace{1_F + \cdots + 1_F}_{k'} = \underbrace{1_F + \cdots + 1_F}_{m} = (mp)_F \). So to show that \( \phi \) is well-defined, it suffices to show that in \( F \) any multiple of \( p \) is zero.

Let \( f \) be the characteristic of \( F \). Note it can’t be 0 since \( F \) is finite. Then consider the elements \( \{0_F, 1_F, \ldots, (f - 1)_F\} \). This is a division ring (you should check this!). Since this is a field and \( F \) is a field containing it, \( F \) is a vector space over \( \mathbb{F} \). So we can fix a basis \( \{x_1, \ldots, x_d\} \), where \( d \) is the dimension of \( F \) as a vector space over \( \mathbb{F} \), and note that this implies that \( p = |F| = f^d \). But the only positive integers dividing \( p \) are 1 and \( p \). Since \( 0 \neq 1 \) in any field, the characteristic of a field is never 1, so this means that \( f = p \). As a result of this, \( \phi \) is well-defined.\(^4\)

You should check that \( \phi \) is a field isomorphism (i.e. preserved multiplication and addition) but this is not difficult. Additionally, note that this implies that \( \phi \) is injective, since if \( \phi(\overline{k}) = \phi(\overline{k'}) \), so \( k_F = k'_F \). Since the characteristic of \( F \) is \( p \), this implies that \( p \) divides \( k - k' \), and so \( \overline{k} = \overline{k'} \). Since we have an injective field isomorphism between two finite fields of the same cardinality, this implies that \( \phi \) is a field isomorphism.

---

\(^3\)If you don’t know what a ring is, you can find a definition on wikipedia under “Ring (mathematics)”.

\(^4\)This proof in fact shows that any finite field is of the form \( p^d \) where \( p \) is the characteristic of the field. It can be shown that for every prime \( p \) and \( d > 0 \), there is a unique field of characteristic \( p \) and size \( p^d \), which completely classifies all finite fields. The proof above shows that this is exhaustive and uniqueness of addition, but showing existence and uniqueness of multiplication uses some algebra that is a little more advanced.