Math 103B, Homework 4

Zonglin Jiang

April 24, 2019

Problem (1) For any $y \in \mathbb{R}$, $xy = x^2 y = x(xy)$ by $x = x^2$ and associativity of the multiplication, and further by the left distributive law

$$xy - x(xy) = x(y - xy) = 0$$

As $R$ has no zero divisor and $x$ is nonzero, $y - xy = 0$, $xy = y$. Similarly we can show $yx = y$ too.

Exercises 18, 52 In Example 18.15, it was established that the map $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ defined by $\phi(n \cdot 1) = n \cdot (1, 1)$ is a ring isomorphism, whenever $\gcd(r, s) = 1$. In particular, the map $\phi$ is surjective.

Thus for any $m, n \in \mathbb{Z}$, there is an $x$ in $\mathbb{Z}_{rs}$ such that

$$\phi(x) = (m \cdot 1, n \cdot 1)$$

that is,

$$x \cdot (1, 1) = (x \cdot 1, x \cdot 1) = (m \cdot 1, n \cdot 1)$$

$$\Rightarrow x \cdot 1 = m \cdot 1 \text{ in } \mathbb{Z}_r \text{ and } x \cdot 1 = n \cdot 1 \text{ in } \mathbb{Z}_s$$

$$\Rightarrow (x - m) \cdot 1 = 0 \text{ in } \mathbb{Z}_r \text{ and } (x - n) \cdot 1 = 0 \text{ in } \mathbb{Z}_s$$

$$\Rightarrow r | x - m \text{ and } s | x - n$$

and the last row is equivalent to

$$x \equiv m \text{ mod } r, x \equiv n \text{ mod } s$$

Exercises 18, 53(a)

Theorem 1 (Chinese Remainder Theorem). Let $r_1, \cdots, r_n$ be positive integers which are pairwise coprime (i.e. $\gcd(r_i, r_j) = 1$ for any $1 \leq i < j \leq n$)\footnote{It’s not enough to assume $\gcd(r_1, \cdots, r_n) = 1$.} Then $\phi_n : \mathbb{Z}_{r_1 r_2 \cdots r_n} \to \prod_{i=1}^{n} \mathbb{Z}_{r_i}$ defined by $\phi(x) = x \cdot (1, 1, \cdots, 1)$ is an isomorphism.
Proof. To show $\phi$ is an isomorphism, it’s enough to show $\phi$ is a homomorphism and bijection. To show $\phi$ is a homomorphism is similar to what’s done in Example 18.15. To show $\phi$ is injective, it’s enough to show $\ker(\phi) = \{0\}$. And indeed if $\phi(x) = 0$, then $x \cdot (1, \cdots, 1) = (x \cdot 1, \cdots, x \cdot 1) = (0, \cdots, 0)$, thus $r_1|\cdots,r_n|x$, $x$ is a common multiple of $r_1,\cdots,r_n$. Note that since $r_i$’s are pairwise prime, their least common multiple is $r_1r_2\cdots r_n$, hence $r_1r_2\cdots r_n|x$, and since $x \in \mathbb{Z}_{r_1r_2\cdots r_n} = \{0, 1, \cdots, r_1r_2\cdots r_n-1\}$, $x = 0$.

Because $\mathbb{Z}_{r_1r_2\cdots r_n}$ and $\prod_{i=1}^n \mathbb{Z}_{r_i}$ are both finite sets of size $r_1r_2\cdots r_n$, an injective map between them must be also surjective, thus $\phi$ is also surjective.

Here is a second proof based on induction.

Proof. We prove this by induction on $n$. When $n = 2$, this is already proved in Example 18.15. For the inductive step, given general $n \geq 3$, by the induction hypothesis $f: \mathbb{Z}_{r_1r_2\cdots r_n} \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_{n-2}} \times \mathbb{Z}_{r_{n-1}r_n}$

$$f(x) = x \cdot \underbrace{(1,1,\cdots,1)}_{n-1 \text{ components}}$$

is an isomorphism. And by the $n = 2$ case,

$$g: \mathbb{Z}_{r_{n-1}r_n} \to \mathbb{Z}_{r_{n-1}} \times \mathbb{Z}_{r_n}$$

g($y$) = $y \cdot (1,1)$

is also an isomorphism, hence

$$h: \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_{n-2}} \times \mathbb{Z}_{r_{n-1}r_n} \to \prod_{i=1}^n \mathbb{Z}_{r_i}$$

$$h = \text{id}_{\mathbb{Z}_{r_1}} \times \cdots \times \text{id}_{\mathbb{Z}_{r_{n-2}}} \times g$$

$$h(x_1,\cdots,x_{n-2},y) = (x_1,\cdots,x_{n-2},g(y))$$

is also an isomorphism.

Thus $h \circ f$ must be an isomorphism too. Note that

$$(h \circ f)(x) = h(f(\underbrace{1,1,\cdots,1}_{n-2 \text{ components}}, 1\underbrace{\mathbb{Z}_{r_{n-1}r_n}}_{n-1 \text{ components}}))$$

$$= h(x \cdot 1, x \cdot 1, \cdots, x \cdot 1, x \cdot 1\underbrace{\mathbb{Z}_{r_{n-1}r_n}}_{n-2 \text{ components}})$$

$$= (x \cdot 1, x \cdot 1, \cdots, x \cdot 1, g(x \cdot 1\underbrace{\mathbb{Z}_{r_{n-1}r_n}}_{n-2 \text{ components}}))$$

$$= (x \cdot 1, x \cdot 1, \cdots, x \cdot 1)$$

$$= \phi_n(x)$$

And this implies $\phi_n$ is an isomorphism.

\qed
Exercises 18, 53(b)  
Use the same argument as in Exercise 18, 52, with the help of Part (a).

Exercises 20, 19  
Exercise 28 states that if \( p \) is a prime, \( (p-1)! \equiv -1 \mod p \). Note that \( (p-1)! = (p-2)! \cdot (p-1) \), \( (p-1)! \equiv (p-2)! \cdot (-1) \mod p \), thus \( (p-2)! \cdot (-1) \equiv -1 \mod p \), \( p | (p-2)! \cdot (-1) - (-1) = (-1>((p-2)! - 1) \), and since \( p \nmid -1 \), \( p | (p-2)! - 1 \), thus \( (p-2)! \equiv 1 \mod p \).

Exercises 20, 23

a. False. E.g. when \( a = 0 \), the equality is obviously false. In fact, this is only true when \( \gcd(a, p) = 1 \).

b. True. This is Fermat’s little theorem.

c. True. According to the definition of the Euler phi-function on Page 104, \( \phi(n) \) is the number of positive integers less than or equal to \( n \) that are relatively prime to \( n \). The number of such integers is at most \( n \).

d. True if \( n \geq 2 \), as \( \gcd(n, n) = n \neq 1 \), thus the set of positive integers less than or equal to \( n \) that are relatively prime to \( n \) is a subset of \( \{1, 2, \ldots, n-1\} \). Hence \( \phi(n) \) is at most \( n-1 \).

False if \( n \) is allowed to be 1, as \( \phi(1) = 1 \) according to the definition.

e. True when \( n \geq 2 \). 0 is not a unit in \( \mathbb{Z}_n \) if \( n \geq 2 \). For integer \( a \) such that \( 1 \leq a \leq n-1 \), if \( \gcd(a, n) \neq 1 \), then \( a \) is a zero divisor, thus not a unit. If \( \gcd(a, n) = 1 \), \( a \) is a unit in \( \mathbb{Z}_n \) by Theorem 20.6.

False if \( n \) is allowed to be 1, because when \( n = 1 \), \( \mathbb{Z}_n = \{0\} \) has no positive integer, but 0 is a unit as it’s the identity element of the multiplication.

f. True. The product of two units in any ring is always a unit as we have seen in Homework 1 that the set of units form a group, in particular it’s closed under multiplication.

g. False. In a commutative ring \( R \), if \( a \) is not a unit, then for any \( b \), \( ab = ba \) is not a unit. Otherwise, there is \( c \) such that \( (ab)c = 1 \), and hence \( a(bc) = 1 \).

Because \( R \) is commutative, \( (bc)a = 1 \), thus \( bc \) is the multiplicative inverse of \( a \), but \( a \) is not a unit by assumption. (Even if \( b \) is a unit, \( ab \) can’t be a unit as no special property of \( b \) is required in the proof.)

h. True. See the Part (g) for explanation.

i. False. For example, \( 0 \cdot x \equiv 1 \mod 2 \) has no solution.

If \( \gcd(p, a) = 1 \), then \( ax \equiv b \mod p \) always has a unique solution.

j. True. This is just a paraphrase of Theorem 20.12.

\[2\] This statement fails for general non-commutative rings. In fact, one can find an example of a noncommutative ring \( R \) where there are \( x, y \) such that \( xy = 1 \), but none of \( x, y, yx \) is invertible. Such an example can be found in operator algebras over Hilbert spaces.