Math 103B, Homework 2

Zonglin Jiang

April 11, 2019

Problem (1)(a) To show \((R, +)\) is an abelian group, note that \((R, +)\) is isomorphic to the direct product \((\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +)\) as abelian groups, and it is shown in Math 103A that the direct product of abelian groups is an abelian group. To show \(\cdot\) is associative, \([a, b](c, d)](e, f) = (ac - bd, ad + bc)(e, f) = ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e) = (ace - bde - adf - bef, acf - bdf + ade + bce), while \((a, b)[(c, d)(e, f)] = (a, b)(ce - df, cf + de) = (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) = (ace - adf - be - bde, acf + ade + bce - bdf) = [(a, b)(c, d)](e, f).

As for the distributive laws, first note that \((c, d)(a, b) = (ca - bd, cb + da) = (ac - bd, ad + bc) = (a, b)(c, d), thus the multiplication is commutative, it’s enough to show one of the distributive laws. \((a, b)((c, d) + (e, f)) = (a, b)(c + e, d + f) = (a(c + e) - b(d + f), a(d + f) + b(c + e)) = (ac + ae - bd - bf, ad + af + bc + be), and \((a, b)(c, d) + (a, b)(e, f) = (ac - bd, ad + bc) + (ae - bf, af + be) = (ac - bd + ae - bf, ad + bc + af + be) = (a, b)((c, d) + (e, f))\)

Problem (1)(b) \((1, 0)(a, b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a, b), and by commutativity of the multiplication, \((a, b)(1, 0) = (a, b)\) is also true.

Problem (1)(c) If \((a, b)\) is a solution, then \((a, b)^2 = (a, b)(a, b) = (a^2 - b^2, ab + ba) = (a^2 - b^2, 2ab) = -1_R = (-1, 0), a^2 - b^2 = -1, 2ab = 0. Since 3 is prime, \(\mathbb{Z}_3\) is a field in which the product of a bunch of nonzero elements cannot be zero, thus \(2ab = 0\) implies \(a = 0\) or \(b = 0\). If \(b = 0\), then \(a^2 = -1 = 2\) has no solution in \(\mathbb{Z}_3\) (as \(0^2 = 0 \neq 2, 1^2 = 1 \neq 2, 2^2 = 1 \neq 2\), hence \(b \neq 0\), there must be \(a = 0\), and \(-b^2 = -1 \iff b^2 = 1 \iff (b + 1)(b - 1) = 0 \iff b = \pm 1\). Thus the solutions can only be \((0, 1), (0, -1)\), and we can check they are indeed solutions.

Problem (1) Bonus Given \((a, b) \in R \setminus \{0\}\), following the hint, we first show that \(a^2 + b^2 \neq 0\). Since \((a, b) \neq (0, 0)\), if \(b = 0\), then \(a \neq 0 \Rightarrow a^2 \neq 0\) as \(\mathbb{Z}_3\) is a field, thus \(a^2 + b^2 = a^2 \neq 0\). Now if \(b \neq 0\), \(b^{-1}\) exists in \(\mathbb{Z}_3\), and if \(a^2 + b^2 = 0\), then \(a^2 = -b^2, a^2(b^{-1})^2 = -b^2(b^{-1})^2 = -1, (ab^{-1})^2 = -1\), but we already know that \(x^2 = -1\) has no solution in \(\mathbb{Z}_3\) in the last part by calculating \(0^2, 1^2, 2^2\).

Now we know that \(a^2 + b^2 \neq 0\), and again since \(\mathbb{Z}_3\) is a field, \((a^2 + b^2)^{-1}\) exists in \(\mathbb{Z}_3\), and we can check that \(((a^2 + b^2)^{-1}a)(a^2 + b^2)^{-1}(-b))(a, b) = ((a^2 + b^2)^{-1}a^2 - (a^2 + b^2)^{-1}(-b^2), (a^2 + b^2)^{-1}ab + (a^2 + b^2)^{-1}(-b)a) = (1, 0) = 1_R,\)
and since it’s a commutative ring, \((a, b)((a^2 + b^2)^{-1}a, (a^2 + b^2)^{-1}(-b)) = 1_R\) is also true.

**Remark** You may have noticed that the multiplication in \(R\) is very similar to the multiplication of complex numbers — if you think of \((a, b)\) as \(a + bi\), and indeed this is how we find the inverse of \((a, b)\) in \(R\) (we “guess” the same formula for complex numbers shall work for \(R\) too, and then we prove it is indeed the case).

**Problem (2)(a)(b)** By the given condition, \((x + x)^2 = x + x\), and on the other hand \((x + x)^2 = (x + x)(x + x) = x^2 + x^2 + x^2 = x + x + x + x\), thus \(x + x = x + x + x + x\), hence \((x + x)^2 = 0\).

**Problem (2)(c)** \(x + y = (x + y)^2 = (x + y)(x + y) = x^2 + x y + y x + y^2 = x + x y + y x + y\), hence \(x y + y x = 0\). We have shown in (b) that \(\forall x \in R, x + x = 0\), in particular \(x y + y x = 0\), thus \(x y + y x = x y + y x, y x = y x\).

**Problem (3)** For \(Z_5 \times Z_6, n \cdot 1 = 0 \Leftrightarrow n \cdot (1, 1) = (n \cdot 1, n \cdot 1) = (0, 0) \Leftrightarrow 5|n\) and \(6|n \Leftrightarrow 30|n\). The minimal positive integer that is divisible by 30 is 30 itself. Thus the characteristic of \(Z_5 \times Z_6\) is 30.

Here \(5|n\) and \(6|n \Leftrightarrow 30|n\) is because 5 and 6 are coprime to each other.

For \(Z_6 \times Z_8 \times Z_9\), by a similar argument, we can show that \(n \cdot 1 = 0 \Leftrightarrow 6|n, 8|n, 9|n\). Thus \(n\) is a common multiple of 6, 8, 9, and the least of them is \(\text{lcm}(6, 8, 9) = 72\). Thus 72 is the characteristic of \(Z_6 \times Z_8 \times Z_9\).

**Remark** The same method can be used to show in general the characteristic of \(Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_m}\) is \(\text{lcm}(n_1, \cdots, n_m)\).

**Exercise 19, 2** In \(Z_7, 3^{-1} = 5\), thus \(3x = 2 \Leftrightarrow 3^{-1} \cdot 3x = 3^{-1} \cdot 2 \Leftrightarrow x = 5 \cdot 2 = 3\). Similarly, in \(Z_{23}, 3^{-1} = 8\), thus \(x = 8 \cdot 2 = 16\). Note that the way we solve the equations has promised there is no other solution than the unique one we found.

**Exercise 19, 10** Using the same method as in Problem (3), the characteristic of \(Z_6 \times Z_{15}\) is \(\text{lcm}(6, 15) = 30\).

**Exercise 19, 12** For any \(x, y\) in the ring, \((x + y)^3 = (x + y)(x + y)(x + y) = (x^2 + xy + yx + y^2)(x + y) = (x^2 + 2xy + y^2)(x + y) = x^3 + x^2y + 2xyx + 2xy^2 + y^2x + y^3 = x^3 + 3x^2y + 3xy^2 + y^3 = x^3 + y^3\). That is \((x + y)^3 = x^3 + y^3\) for any \(x, y\).

Thus \((a + b)^3 = ((a + b)^3)^3 = (a^3 + b^3)^3 = (a^3)^3 + (b^3)^3 = a^9 + b^9\).
Remark  It can be proved that the binomial theorem

\[(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\]

holds as long as \(ab = ba\) in any given ring, but may fail if \(ab \neq ba\).

Exercise 19, 14  To show an element \(a \neq 0\) from a ring is a zero divisor, we only need to find \(b \neq 0\) from the ring such that \(ab = 0\) or \(ba = 0\) (they don’t have to be true at the same time). In this particular case, we can check for example, \(\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} -2 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\).