MA1214

Introduction to group theory

Prof. Zaitsev

Solutions to Sheet 5

leitner@stp.dias.ie

1. Equivalence relation: We must check that $\sim$ is reflexive, symmetric and transitive.

   (a) true: We have $y = y$; $y_1 = y_2 \Rightarrow y_2 = y_1$; if $y_1 = y_2$ and $y_2 = y_3$ then $y_1 = y_3$.

   (b) not true.
   Explanation: Transitivity does not hold. We give an example. Suppose $(x_1, y_1) \sim (x_2, y_2)$ because $x_1 = x_2$, while $y_1 \neq y_2$. Suppose moreover $(x_2, y_2) \sim (x_3, y_3)$ because $y_2 = y_3$, while $x_2 \neq x_3$. Then $(x_2, y_2) \nsim (x_3, y_3)$ because $x_1 = x_2 \neq x_3$, and at the same time $y_1 \neq y_2 = y_3$.

   (c) true: $x - x = 0$ is an integer. When $y_1 - y_2 \in \mathbb{Z}$ then $y_2 - y_1 = -(y_1 - y_2) \in \mathbb{Z}$. Suppose $x_1 - x_2 \in \mathbb{Z}$ and $x_2 - x_3 \in \mathbb{Z}$. Then $x_1 - x_3 = (x_1 - x_2) + (x_2 - x_3) \in \mathbb{Z}$.

   The question does not make precise which and how many equivalence classes we are to determine. For brevity, we shall give one example for each. An answer assigning a specific real number to any of the variables occurring with a star is correct as well.

   (a) An equivalence class is $[(x, y_*)]_\sim = \{(x, y) \in \mathbb{R}^2 | \, y = y_*\}$, where $y_* \in \mathbb{R}$ is fixed.

   (b) An equivalence class is $[(x_*, y_*)]_\sim = \{(x, y) \in \mathbb{R}^2 | \, x = x_*\} \cup \{(x, y) \in \mathbb{R}^2 | \, y = y_*\}$, where $x_*, y_* \in \mathbb{R}$ are fixed.

   (c) An equivalence class is $[(x_*, y)]_\sim = \{(x, y) \in \mathbb{R}^2 | \, x - x_* \in \mathbb{Z}\}$, where $x_* \in \mathbb{R}$ is fixed.

2. (a) Suppose $a|b$ (i.e. $\exists\, n \in \mathbb{Z}$ s.t. $an = b$) and $b|c$ ($\exists\, m \in \mathbb{Z}$ s.t. $bm = c$). Then

   $$c = bm = (an)m = a(nm)\,,$$

   where $nm \in \mathbb{Z}$. Thus $a|c$.

   (b) Since $a|b$, $\exists n \in \mathbb{Z}$ s.t. $an = b$. On the other hand, $b|a$ so $\exists m \in \mathbb{Z}$ s.t. $bm = a$. So

   $$a = bm = (an)m = a(nm)$$

   whence $nm = 1$. Since both $n, m \in \mathbb{Z}$, we must have $n = m = -1$ or $n = m = 1$. Thus $a = \pm b$.

3. (a)

   $$a : b = 19 : 5 = (15 + 4) : 5 = 3 + \frac{4}{5} \quad \overset{\cdot b}{\Rightarrow} \quad a = 3 \cdot b + 4\,.$$

   $$a : b = (-7) : 5 = (-5 - 2) : 5 = -1 - \frac{2}{5} \quad \overset{\cdot b}{\Rightarrow} \quad a = -b - 2\,.$$

There is a *mathematical convention* to choose for the remainder the same sign as for the divisor b. (This should be mentioned in your lecture notes.) With this convention, the answer for the second pair $(a, b) = (-7, 5)$ reads

$$a : b = (-7) : 5 = (-10 + 3) : 5 = -2 + \frac{3}{5} \quad \overset{\cdot b}{\Rightarrow} \quad a = -2b + 3\,.$$

Note that the absolute value of the remainder is larger than in the first answer.

(b) Since $m|n$, $\exists\, k \in \mathbb{Z}$ s.t. $mk = n$. Now

$$a \equiv b \mod n \quad :\Leftrightarrow \quad a - b \in n\mathbb{Z}$$

(Here $x \in n\mathbb{Z}$ means that $\exists\, \ell \in \mathbb{Z}$ s.t. $x = n\ell$.) We have to show that $a \equiv b \mod m$. But

$$a - b \in n\mathbb{Z} = (mk)\mathbb{Z} \subseteq m\mathbb{Z}\,.$$

(The statement is that if $a - b$ is an integer multiple of $n = mk$ then it is in particular an integer multiple of m, since $k \in \mathbb{Z}$.) This shows that $a - b \in m\mathbb{Z}$ and thus $a \equiv b \mod m$.

(c) Since $25 = 4 + 21$, we have

$$25 = 4 \mod 21\,,$$

so by the preceding part of the problem, since $21 = 3 \cdot 7$, we also have

$$25 = 4 \mod 3\,, \quad 25 = 4 \mod 7\,.$$

Since $3, 7$ are prime, the argument does not apply again, and the procedure stops here.
Note: The above mentioned *mathematical convention* for the division with remainder applies: We have

$$25 \equiv 4 \mod n \quad \Leftrightarrow \quad n|(25 - 4) \quad \Leftrightarrow \quad \exists\, k \in \mathbb{Z} \text{ s.t.} \quad 25 = k \cdot n + 4\,.$$

Only non-negative n is admissible since since the remainder has positive sign $(4 > 0)$.