Tugas Abstract Algebra

Dari Buku Randall B. Maddox

Exercise 2.7

6 . Prove Theorem 2.7.7:

Suppose $x, y \in Z$ and $n \in N$. Then $x \equiv_n y$ if and only if x and y have the same remainder when divided by n according to the division algorithm.

Proof :

($\rightarrow$) $x \equiv_n y$ means that $\exists k \in Z \ni x - y = n.k$

$$x = n.k + y$$

If $y = n.p + r$, $p, r \in Z, 0 \leq r < n$,

we can rewrite $x = n.k + y$ as $x = n.k + n.p + r$

$$x = n.(k + p) + r$$

So, x and y have the same remainder r.

($\leftarrow$)x and y have the same remainder when divided by n according to the division algorithm. We can write x and y as

$x = n.k + r.\ \ k.r \in Z. 0 \leq r < n$
$y = n.q + r,\ \ q, r \in Z, 0 \leq r < n$

We get $x - y = n(k - q) + (r - r)$

$$x - y = n\ (k - q) + 0$$

$$x - y = n\ (k - q)$$

So, $x \equiv_n y$ (Q.E.D)

15. Prove the following parts of Theorem 2.7.13

(a) If $g = m_0 a + n_0 b$ is the smallest element of S as defined in Eq (2.84), then $g|a$. (The proof that $g|b$ is identical)

(b) If h is any positive integer with the properties that $h|a$ and $h|b$, then it must be that $h|g$

(c) If g_1 and g_2 both have properties D1-D2, then $g_1 = g_2$

Proof:

(a) Proof:

Let $g \nmid a$ means that $a = kg + r, k, r \in Z, 0 < r < g$

$a = kg + r$

$$
\begin{aligned}
r &= a - kg \\
&= a - k(m_0 a + n_0 b\,) \\
&= a - km_0 a - kn_0 b \\
&= (1 - km_0)a + (-kn_0)b
\end{aligned}
$$

Notice that $r \in S$ and $r < g$. It contradicts with g is the smallest element of S.

(b) Proof:

$h|a$ means that $\exists k_1 \in Z \ni\ a = k_1 h$

$h|b$ means that $\exists k_2 \in Z \ni\ b = k_2 h$

Consider that

$g = m_0 a + n_0 b$

$g = m_0(k_1 h) + n_0(k_2 h)$

$g = (m_0 k_1 + n_0 k_2)h$

So, $h|g$

(c) Proof:

(1) A. $g_1|a$, $g_1|b$

B. If h any positive integers with properties $h|a$ and $h|b$, then $h|g_1$

(2) A. $g_2|a$, $g_2|b$

B. If k any positive integers with properties $k|a$ and $k|b$, then $k|g_2$

From (1 A), we have $g_1|a$, $g_1|b$

We can choose $k = g_1$ for (2 B) then we get $g_1|g_2$

From (2 A), we have $g_2|a$, $g_2|b$

We can choose $h = g_2$ for (1 B) then we get $g_2|g_1$

According to Theorem 2.7.11 :

If $a|b$ and $b|a$ then $a = \pm b$

We can say that

$$g_1 = \pm g_2$$

Because of $g_1, g_2 > 0$ so $g_1 = g_2$

By: Cecyl