Mathematics 1214: Introduction to Group Theory

Homework exercise sheet 7

Due 12:50pm, Friday 19th March 2010

1. Which of the following sets of real numbers contains a least element?
[Recall that if $S \subseteq \mathbb{R}$, then S contains a least element if there is an element $x \in S$ such that $x \leq y$ for all $y \in S$].

(a) $\mathbb{N}$ (b) $\{2, 4, 6, 8, 10, \dots\}$

(c) $(3, 5)$ (d) $[0, \infty) \setminus \mathbb{Q}$, that is, the set of non-negative irrational numbers

Solution (a), (b), have least elements by the Least Integer Principle, since they are non-empty subsets of $\mathbb{N}_0$.

(c) has no least element, since if $x \in (3, 5)$ then $x > 3$ so $x > \frac{1}{2}(3 + x) \in (3, 5)$, so x is not a least element of $(3, 5)$.

(d) There is no least element, since 0 is rational, so is not in $S = [0, \infty) \setminus \mathbb{Q}$. Hence $x \in S \implies x > 0, x \notin \mathbb{Q} \implies x > \frac{1}{2}x$ and $\frac{1}{2}x \in S$ so x is not a least element of S. So S does not contain a least element.

2. Let a, b be integers.
Prove that $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$

Solution Let $d = \gcd(a, b)$. The definition of $\gcd(a, b)$ is unchanged if we swap a and b, so $\gcd(a, b) = \gcd(b, a)$. Moreover, if $k \in \mathbb{Z}$ then $k|a \iff k|-a$ and $k|b \iff k|-b$, so the definition is also unchanged if we swap a with $-a$, or b with $-b$, or both. Hence $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.

3. Use the Euclidean algorithm to compute:

(a) $\gcd(1082, 361)$ (b) $\gcd(1680, 1841)$

(c) $\gcd(2001, -1173)$ (d) $\gcd(-1960, -2184)$

Solution

$$\begin{aligned} 1082 &= 361 \times 2 + 360 \\ 361 &= 360 \times 1 + 1 \\ 360 &= 1 \times 360 + 0 \end{aligned}$$

So $\gcd(1082, 361) = 1$.

(b)

$$\begin{aligned}
1841 &= 1680 \times 1 + 161 \\
1680 &= 161 \times 10 + 70 \\
161 &= 70 \times 2 + 21 \\
70 &= 21 \times 3 + 7 \\
21 &= 7 \times 3 + 0
\end{aligned}$$

So $\gcd(1680, 1841) = \gcd(1841, 1680) = 7$.

(c)

$$\begin{aligned}
2001 &= 1173 \times 1 + 828 \\
1173 &= 828 \times 1 + 345 \\
828 &= 345 \times 2 + 138 \\
345 &= 138 \times 2 + 69 \\
138 &= 69 \times 2 + 0
\end{aligned}$$

So $\gcd(2001, 1173) = \gcd(2001, -1173) = 69$.

(d)

$$\begin{aligned}
2184 &= 1960 \times 1 + 224 \\
1960 &= 224 \times 8 + 168 \\
224 &= 168 \times 1 + 56 \\
168 &= 56 \times 3 + 0
\end{aligned}$$

So $\gcd(-2184, -1960) = \gcd(2184, 1960) = 56$.

4. Compute $\gcd(808, 253)$ using the Euclidean algorithm. Then carefully examine your working, and use it to find integers s, t such that $808s + 253t = 1$.

Solution

$$\begin{aligned}
808 &= 253 \times 3 + 49 \\
253 &= 49 \times 5 + 8 \\
49 &= 8 \times 6 + 1 \\
8 &= 1 \times 8 + 0
\end{aligned}$$

So $\gcd(808, 253) = 1$. Rearranging these equations from bottom to top gives

$$\begin{aligned}
1 &= 49 - 8 \times 6 \\
8 &= 253 - 49 \times 5 \implies 1 = 49 - (253 - 49 \times 5) \times 6 = 49 \times 31 - 253 \times 6 \\
49 &= 808 - 253 \times 3 \implies 1 = (808 - 253 \times 3) \times 31 - 253 \times 6 = 808 \times 31 - 253 \times 99.
\end{aligned}$$

So $s = 31$ and $t = -99$ do the job.

5. Let a, b be integers. Prove that $a = \gcd(a, b) \iff a|b$.

Solution $\Rightarrow$: we always have $\gcd(a,b)|a$. Hence if $a = \gcd(a,b)$, then $a|b$.

$\Leftarrow$: suppose that $a|b$. Then

- $a|a$ and $a|b$, and
- if $c \in \mathbb{Z}$ with $c|a$ and $c|b$, then $c|a$.

Hence $a = \gcd(a,b)$.

6. Let a, b, c be integers with $c \geq 1$.

   (a) Prove that $a|b \iff ac|bc$.

   (b) Prove that $\gcd(ac, bc) = c\gcd(a,b)$.
   [Suggestion: let $D = \gcd(ac, bc)$, and argue that $d = D/c$ is equal to $\gcd(a,b)$.]

(a) $a|b \iff \exists m \in \mathbb{Z} \colon b = am \iff \exists m \in \mathbb{Z} \colon bc = acm \iff bc|ac$.

[To justify the second $\iff$, observe that since $c \neq 0$, the statements $b = am$ and $bc = acm$ are equivalent.]

(b) Let $D = \gcd(ac, bc)$. Since $c|ac$ and $c|bc$, we have $c|D$. Hence $d = D/c$ is an integer. We will show that $d = \gcd(a,b)$.

We have $D = dc|ac$, so $d|a$, and $D = dc|bc$, so $d|b$. Moreover, if $e \in \mathbb{Z}$ with $e|a$ and $e|b$ then $ce|ac$ and $ce|bc$, so $ce|D = cd$ (since ce is a common divisor of ac and bc, and D is the gcd of ac and bc) so $e|d$.

In summary:

- $d|a$ and $d|b$
- if $e \in \mathbb{Z}$ with $e|a$ and $e|b$, then $e|d$.

Hence $d = \gcd(a,b)$. Now $d = D/c = \gcd(ac,bc)/c$ by definition, so $\gcd(ac,bc) = c\gcd(a,b)$.