

Tutorial 4

1. Show that any non-zero homomorphism from a field F to a field E must be injective.

Solution.

Let $\phi: F \rightarrow E$ be a homomorphism, where E and F are fields. Suppose also that ϕ is not the zero map. If there exists a nonzero $c \in F$ with $\phi(c) = 0$ then for all $a \in F$ we have

$$\phi(a) = \phi(ac^{-1}c) = \phi(ac^{-1})\phi(c) = \phi(ac^{-1})0 = 0,$$

contrary to the assumption that ϕ is nonzero. So for all $c \in F$, if $\phi(c) = 0$ then $c = 0$. Now let $a, b \in F$ with $\phi(a) = \phi(b)$. Then

$$\phi(a - b) = \phi(a) - \phi(b) = 0,$$

and so by the result just proved it follows that $a - b = 0$. We have thus shown that $\phi(a) = \phi(b)$ implies $a = b$; that is, ϕ is injective.

Alternatively, we deduce $\ker \phi \neq F$ since ϕ is nonzero. So $\ker \phi$ is an ideal in the field F and so, $\ker \phi = \{0\}$, which implies that ϕ is injective.

2. (Euclidean Algorithm) Let $a_1, a_2 \in \mathbb{Z}$ with $a_1 > a_2 \geq 0$ or $a_1 = a_2 > 0$, and whenever $a_i \neq 0$ define a_{i+1} by the conditions

$$a_{i-1} = q_i a_i + a_{i+1}, \text{ and } 0 \leq a_{i+1} < a_i.$$

That is, a_{i+1} is the remainder when a_{i-1} is divided by a_i . Let k be the largest integer such that $a_k \neq 0$ (so that $a_1 \geq a_2 > \dots > a_{k+1} = 0$).

- (i) Calculate k and a_k in the case $a_1 = 117$ and $a_2 = 51$.
- (ii) Show that if $e \in \mathbb{Z}$ satisfies $e|a_1$ and $e|a_2$ then $e|a_i$ for all i from 1 to k .
- (iii) Show that a_k is a divisor of all of $a_{k-1}, a_{k-2}, \dots, a_2, a_1$.
- (iv) Deduce that $a_k = \gcd(a_1, a_2)$.

Solution.

- (i) 117, 51, 15, 6, 3, 0. The 5th a_i is the last nonzero one; so $k = 5$ and $a_5 = 3$ (which must be the g.c.d. of 117 and 51, in view of part (iv) below).
- (ii) Suppose that $e|a_1$ and $e|a_2$. We use induction on j to show that if $1 \leq j \leq k$ then $e|a_i$ for all $i \in \{1, 2, \dots, j\}$. By hypothesis this holds for $j = 1$ and

$j = 2$. Suppose now that $2 < j \leq k$, and assume inductively that $e|a_i$ for all i from 1 to $j - 1$. In particular there exist integers r and s such that $a_{j-2} = re$ and $a_{j-1} = se$, and since $j \leq k$ we have

$$a_j = a_{j-2} - q_{j-1}a_{j-1} = re - q_{j-1}se = (r - q_{j-1}s)e.$$

Thus $e|a_j$ as well as all the earlier a_i , and this establishes our induction. In particular, $e|a_i$ for all i from 1 to k .

- (iii) We use induction on j to show that if $j \in \{0, 1, \dots, k - 1\}$ then $a_k|a_i$ for all $i \in \{k - j, k - j + 1, \dots, k, k + 1\}$. For $j = 0$ this says that $a_k|a_k$ and $a_k|a_{k+1}$, which is clearly true since $a_{k+1} = 0$. Suppose now that $0 < j \leq k - 1$, and assume inductively that $a_k|a_i$ for all i from $k - j + 1$ to $k + 1$. Then in particular there exist integers r and s with $a_{k-j+1} = ra_k$ and $a_{k-j+2} = sa_k$, and now

$$a_{k-j} = q_{k-j+1}a_{k-j+1} + a_{k-j+2} = q_{k-j+1}ra_k + sa_k = (q_{k-j+1}r + s)a_k,$$

showing that $a_k|a_{k-j}$ as well as all the subsequent a_i . This completes the induction, and the case $j = k - 1$ yields that $a_k|a_i$ for all i from 1 to $k + 1$.

- (iv) By construction a_k is a positive integer; part (iii) shows that it is a common divisor of a_1 and a_2 ; part (ii) shows that any other common divisor of a_1 and a_2 is a divisor of a_k . By definition therefore a_k is the g.c.d. of a_1 and a_2 .

3. In this question assume a, b, c are integers.

- (i) Show that if $(a, b) = 1$ then $a|c$ and $b|c$ imply $ab|c$.
- (ii) Show that if $(a, b) = d$, then $(a/d, b/d) = 1$.
- (iii) An integer $h > 0$ is called the lowest common multiple of integers a and b if $a|h$ and $b|h$ and if $a|k$ and $b|k$, then k is a multiple of h . So if a lowest common multiple exist it is unique.

Show that if $a, b \in \mathbb{N}$ are not both zero then $h = ab/(a, b)$ is the lowest common multiple of a and b .

Solution.

Note you might like to verify that for $x, y, z \in \mathbb{Z}$ with $x \neq 0$, $y|z$ if and only if $xy|xz$. So if a and b are both divisible by e then $a|b$ if and only if a/e divides b/e .

- (i) Since $a|c$, $c = am$, for some $m \in \mathbb{Z}$. Hence $(a, b) = 1$ and $b|am$. So $b|m$, i.e. $m = bn$ for some $n \in \mathbb{Z}$. Thus $c = abn$, i.e. $ab|c$.
- (ii) Both a/d and b/d are integers. If e divides a/d and e divides b/d then $ed|a$ and $ed|b$. Hence $ed|(a, b) = d$. So $e|1$. Hence $e = 1$.
- (iii) Put $d = (a, b)$. Then b/d and a/d are positive integers. So we see from

$$h = \frac{ab}{d} = a \frac{b}{d} = \frac{a}{d} b,$$

that h is a positive multiple of both a and b .

Now suppose k is a common multiple of a and b . Then $a|k$ and $b|k$. Hence the positive integers a/d and b/d divide k/d . From (ii) they are relatively prime. So by (i), their product ab/d^2 divides k/d . Multiplying through by d we find $h = ab/d$ divides k . So any common multiple of a and b is divisible by h . So h is the lowest common multiple.

4. (i) Show that $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $x \mapsto (x \bmod 2, x \bmod 3)$ is a ring homomorphism and determine $\ker \phi$.
(ii) Use the first isomorphism theorem to deduce that

$$x \bmod 6 \mapsto (x \bmod 2, x \bmod 3)$$

defines a ring isomorphism from $\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Solution.

- (i) The domain of this map is a ring with an identity. So it suffices to show ϕ respects addition and multiplication.

For all $a, b \in \mathbb{Z}$, by the definition of ϕ and of addition and multiplication in products of rings,

$$\begin{aligned} \phi(a+b) &= (a+b \bmod 2, a+b \bmod 3) \\ &= (a \bmod 2, a \bmod 3) + (b \bmod 2, b \bmod 3) \\ &= \phi(a) + \phi(b), \end{aligned}$$

and

$$\begin{aligned} \phi(ab) &= (ab \bmod 2, ab \bmod 3) \\ &= (a \bmod 2, a \bmod 3)(b \bmod 2, b \bmod 3) \\ &= \phi(a)\phi(b). \end{aligned}$$

So ϕ is a homomorphism.

Given $x \in \mathbb{Z}$, $x \in \ker \phi$ if and only if $x = 0 \bmod 2$ and $x = 0 \bmod 3$, i.e both 2 and 3 divide x which is the case if and only if $6|x$. So $\ker \phi = 6\mathbb{Z}$.

- (ii) The given map is the natural isomorphism,

$$\bar{x} = x \bmod 6 \mapsto (x \bmod 2, x \bmod 3)$$

from $\mathbb{Z}/\ker \phi = \mathbb{Z}/6\mathbb{Z}$ to $\text{im } \phi$. It remains to show $\text{im } \phi = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Well, $\mathbb{Z}/6\mathbb{Z}$ has 6 elements. So its isomorphic image $\text{im } \phi$ has 6 elements. But the image is a subset of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and this has only $2 \times 3 = 6$ elements. Hence $\text{im } \phi = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

5. (Chinese Remainder Theorem) Suppose m_1, m_2, \dots, m_n are pair-wise relatively prime integers, all greater than 1. Then any set of simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots \quad x \equiv a_n \pmod{m_n},$$

has a solution, and it is uniquely determined $\pmod{m_1 m_2 \cdots m_n}$.

Solution.

Put $m = m_1 m_2 \cdots m_n$.

You could generalise the above result and show that

$$x \mapsto (x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots \quad x \equiv a_n \pmod{m_n})$$

defines an isomorphism

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}.$$

The result follows immediately from that.

Alternatively put $M_i = m/m_i$. The condition that the m_i are pair-wise relatively prime implies for each i , $(m_i, M_i) = 1$. Hence we can find integers a_i, e_i such that $a_i m_i + e_i M_i = 1$. Then $e_i \equiv 1 \pmod{m_i}$, and $e_i \equiv 0 \pmod{m_j}$, for $i \neq j$. So the integer

$$x = a_1 M_1 + a_2 M_2 + \cdots + a_n M_n$$

solves the simultaneous congruences.

Further check integers x and y are solutions if and only if if and only if $x \equiv y \pmod{m_i}$ for each i . But $x \equiv y \pmod{m_i}$ for each i if and only if $x - y$ is divisible by each of the pair-wise prime integers m_i , and this is the case if and only if their product m divides $x - y$, i.e $x \equiv y \pmod{m}$. This shows the solution is uniquely determined modulo m .