Book Abstract Algebra An Introduction, Third Edition, Exercises

Jason Sass

May 19, 2025

Hungerford exercises 1.2

Exercise 1. Let $a, b, c \in \mathbb{Z}$.
Then $(a, (b, c)) = ((a, b), c)$.

Proof. Let $d = \gcd(a, b)$.
Let $e = \gcd(b, c)$.
To prove $\gcd(a, e) = \gcd(d, c)$, let $f = \gcd(a, e)$.
We must prove $f = \gcd(d, c)$.

We prove f is a common divisor of d and c.
Since $f = \gcd(a, e)$, then $f|a$ and $f|e$, and any common divisor of a and e divides f.
Since $e = \gcd(b, c)$, then $e|b$ and $e|c$, and any common divisor of b and c divides e.
Since $d = \gcd(a, b)$, then $d|a$ and $d|b$, and any common divisor of a and b divides d.
Since $f|e$ and $e|b$, then $f|b$.
Since $f|a$ and $f|b$, then f is a common divisor of a and b, so $f|d$.
Since $f|e$ and $e|c$, then $f|c$.
Since $f|d$ and $f|c$, then f is a common divisor of d and c.

Let g be any common divisor of d and c.
Then $g|d$ and $g|c$.
Since $g|d$ and $d|a$, then $g|a$.
Since $g|d$ and $d|b$, then $g|b$.
Since $g|b$ and $g|c$, then g is a common divisor of b and c, so $g|e$.
Since $g|a$ and $g|e$, then g is a common divisor of a and e, so $g|f$.
Thus, any common divisor of d and c divides f.

Since f is a common divisor of d and c, and any common divisor of d and c divides f, then $f = \gcd(d, c)$, as desired. $\square$

Exercise 2. Let $a, b, c \in \mathbb{Z}$.

Then $\gcd(a, c) = \gcd(b, c) = 1$ iff $\gcd(ab, c) = 1$.

Proof. Suppose $\gcd(a, c) = \gcd(b, c) = 1$.

Since $\gcd(a, c) = 1$, then $m_1 a + n_1 c = 1$ for some integers m_1 and n_1.

Since $\gcd(b, c) = 1$, then $m_2 b + n_2 c = 1$ for some integers m_2 and n_2.

Thus, $b = 1b = (m_1 a + n_1 c)b = m_1 ab + n_1 bc$, so $m_2(m_1 ab + n_1 bc) + n_2 c = 1$.

Hence, $1 = m_1 m_2 ab + m_2 n_1 bc + n_2 c = (m_1 m_2)(ab) + (m_2 n_1 b + n_2)c$.

Since there exist integers $m_1 m_2$ and $m_2 n_1 b + n_2$ such that $(m_1 m_2)(ab) + (m_2 n_1 b + n_2)c = 1$, then $\gcd(ab, c) = 1$. $\square$

Proof. Conversely, suppose $\gcd(ab, c) = 1$.

Then $xab + yc = 1$ for some integers x and y.

Hence, $1 = xab + yc = (xb)a + yc = (ax)b + yc$.

Since there exist integers xb and y such that $(xb)a + yc = 1$, then $\gcd(a, c) = 1$.

Since there exist integers ax and y such that $(ax)b + yc = 1$, then $\gcd(b, c) = 1$.

Therefore, $\gcd(a, c) = \gcd(b, c) = 1$. $\square$

oldstuff3

Exercise 3. Let $a, b, u, v \in \mathbb{Z}$.

If $au + bv = 1$, then $\gcd(a, b) = 1$.

Proof. Suppose $au + bv = 1$.

Let $d = \gcd(a, b)$.

Then $d \in \mathbb{Z}^+$, so $d > 0$.

Since $u, v \in \mathbb{Z}$ and $1 = ua + bv = ua + vb$, then 1 is a linear combination of a and b.

Thus, 1 is a multiple of d, so $d|1$.

Since $d \in \mathbb{Z}$ and $d > 0$ and $1 > 0$ and $d|1$, then $d \leq 1$.

Since $0 < d$ and $d \leq 1$, then $0 < d \leq 1$.

Since $d \in \mathbb{Z}$ and $0 < d \leq 1$, then $d = 1$.

Therefore, $1 = d = \gcd(a, b)$. $\square$

Exercise 4. Let $a, b, c, d \in \mathbb{Z}$.

If $a|c$ and $b|c$ and $\gcd(a, b) = d$, then $ab|cd$.

Proof. Suppose $a|c$ and $b|c$ and $\gcd(a, b) = d$.

Since $a|c$ and $b|c$, then $c = ar$ and $c = bs$ for some integers r and s.

Since $d = \gcd(a, b)$, then d is the least positive linear combination of a and b, so there exist integers m and n such that $d = ma + nb$.

Observe that

$$\begin{aligned} cd &= c(ma+nb) \\ &= cma+cnb \\ &= (bs)ma+(ar)nb \\ &= bsma+arnb \\ &= smab+rnab \\ &= ab(sm+rn). \end{aligned}$$

Since $sm+rn \in \mathbb{Z}$ and $cd = ab(sm+rn)$, then $ab|cd$. □

Exercise 5. Let $a, b, c, d \in \mathbb{Z}$.
If $c|ab$ and $\gcd(c, a) = d$, then $c|db$.

Proof. Suppose $c|ab$ and $\gcd(c, a) = d$.
Since $c|ab$, then $ab = ck$ for some integer k.
Since $d = \gcd(c, a)$, then d is the least positive linear combination of c and a, so there exist integers m and n such that $d = mc + na$.
Observe that

$$\begin{aligned} db &= (mc+na)b \\ &= mcb+nab \\ &= mcb+n(ck) \\ &= mcb+nck \\ &= c(mb+nk). \end{aligned}$$

Since $mb+nk \in \mathbb{Z}$ and $db = c(mb+nk)$, then $c|db$. □

Proof. Suppose $c|ab$ and $\gcd(c, a) = d$.
Since $\gcd(c, a) = d$, then $d = xc + ya$ for some integers x and y.
Hence, $db = (xc+ya)b = xcb+yab = (xb)c+yab$ is a linear combination of c and ab.
Since $c|c$ and $c|ab$, then c divides any linear combination of c and ab, so $c|db$. □

Exercise 6. A positive integer is divisible by 3 iff the sum of its digits is divisible by 3.

Proof. TODO □

Exercise 7. A positive integer is divisible by 9 iff the sum of its digits is divisible by 9.

Proof. TODO □

Exercise 8. gcd of a finite number of integers

Let $a_1, a_2, ..., a_n \in \mathbb{Z}$, not all zero.

The greatest common divisor of $a_1, a_2, ..., a_n$ is the largest integer d such that $d|a_i$ for every $i \in \{1, 2, ..., n\}$.

There exist integers u_i such that $d = a_1u_1 + a_2u_2 + ...a_nu_n$.

Proof. TODO $\square$